**KiralikYonetimi.com**
**PERSONAL DATA STORAGE AND DESTRUCTION POLICY**

## 1. PURPOSE OF THE POLICY

This Personal Data Storage and Destruction Policy **("Policy")** of Aytaç MESTÇİ **("Individual Company" / "Company")** is issued in order to regulate the technical and administrative protection of personal data in accordance with the Personal Data Protection Law No. 6698 **("Law"),** and to regulate the implementation of the provisions of the Regulation on Deletion, Destruction or Anonymization of Personal Data **("Regulation")** published in the Official Gazette dated 28/10/2017 in case the conditions for processing personal data disappear.

## 2. REGULATED RECORDING MEDIA

Personal data belonging to data subjects are securely stored by **the Company** in the environments listed below in accordance with the relevant legislation, especially the provisions of the Law:

**Electronic media:**
- E-Mail Box
- Microsoft Office Programs

**Non-electronic media:**
- Unit Cabinets
- Folders
- Archive

## 3. 3. EXPLANATIONS ON THE REASONS FOR RETENTION

**Personal data belonging to data subjects, in particular by the Company:**

a. a. Sustainability of activities,
b. b. Fulfillment of legal obligations,
c. c. Planning and performance of employee rights and benefits,
d. d. Ability to manage business relationships,

it is stored securely in the above-mentioned physical or electronic media within the limits specified in the Law and other relevant legislation.

**Reasons for storage:**

a. a. Personal data is directly related to the establishment and performance of contracts,
b. b. The use of personal data for the establishment, exercise or protection of a right,
c. c. Provided that personal data does not harm the fundamental rights and freedoms of individuals, **the Company** has a legitimate interest,
d. d. Personal data fulfillment of any legal obligation of **the Company**,
e. e. Legislation clearly stipulates the retention of personal data,
f. f. Explicit consent of data subjects in terms of storage activities that require the explicit consent of data subjects.

Pursuant to the Regulation, in the cases listed below, personal data belonging to data subjects shall be deleted, destroyed or anonymized by **the Company** ex officio or upon request:

a. a. Amendment or abolition of the provisions of the relevant legislation that constitute the basis for the processing or storage of personal data,

b. b. The purpose requiring the processing or storage of personal data disappears,

c. c. The disappearance of the conditions requiring the processing of personal data under Articles 5 and 6 of the Law,

d. d. In cases where the processing of personal data takes place only in accordance with the explicit consent condition, the relevant person's withdrawal of his/her consent,

e. e. Acceptance by the data controller of the application made by the data subject for the deletion, destruction or anonymization of his/her personal data within the framework of his/her rights under paragraphs 2 (e) and (f) of Article 11 of the Law,

f. f. In cases where the data controller rejects the application made by the data subject with the request for the deletion, destruction or anonymization of his/her personal data, his/her response is found insufficient or he/she does not respond within the period stipulated in the Law; filing a complaint to the Board and this request is approved by the Board,

g. g. Although the maximum period for retaining personal data has elapsed, there are no circumstances that justify retaining personal data for a longer period.

## 4. MEASURES TAKEN FOR THE PROTECTION OF PERSONAL DATA

In accordance with Article 12 of the Law, **the Company** takes the necessary technical and administrative measures to ensure the appropriate level of security in order to prevent unlawful processing of the personal data it processes, to prevent unlawful access to the data and to ensure the preservation of the data, and to carry out or have the necessary audits carried out within this scope. Although all technical and administrative measures have been taken, in the event that the processed personal data is illegally obtained by third parties, **the Company** shall notify the relevant units as soon as possible.

### 4.1. Technical Measures

- Network security and application security are ensured.
- Closed system network is used for personal data transfers through the network.
- Security measures are taken within the scope of procurement, development and maintenance of information technology systems.
- There are disciplinary regulations for employees that include data security provisions.
- Training and awareness raising activities on data security are carried out for employees at regular intervals.
- Authorization matrix has been created for employees.
- Corporate policies on access, information security, use, storage and disposal have been prepared and implemented.
- Confidentiality commitments are made.
- Employees who are reassigned or leave their jobs are de-authorized in this area.
- Up-to-date anti-virus systems are used.
- Firewalls are used.
- The signed contracts contain data security provisions.
- 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 environments containing personal data is ensured.
- Internal periodic and/or random audits are conducted and commissioned.
- Existing risks and threats have been identified.
- Protocols and procedures for the security of sensitive personal data have been determined and implemented.
- Cyber security measures have been taken and their implementation is constantly monitored.
- Enciphering is performed.
- Data processing service providers are periodically audited on data security.
- Awareness of data processing service providers on data security is ensured.

### 4.2. Administrative Measures

- Employees are trained on the technical measures to be taken to prevent unlawful access to personal data.
- Access to personal data and authorization processes are designed and implemented within **the Company** in accordance with the legal compliance requirements for processing personal data on a business unit basis. In limiting access, whether the data is of special nature and the degree of importance are also taken into account.
- **The Company** has added records to all kinds of documents that regulate the relationship between the Company and its personnel and contain personal data, stating that in order to process personal data in accordance with the law, the obligations stipulated by the Law must be complied with, personal data must not be disclosed, personal data must not be used unlawfully and the confidentiality obligation regarding personal data continues even after the termination of the employment contract with **the Company**.
- Employees are informed that they cannot disclose the personal data they have learned to anyone else in violation of the provisions of the Law and cannot use it for purposes other than processing, and that this obligation will continue after their resignation and necessary commitments are taken from them in this direction.
- Provisions are added to the contracts concluded by **the Company** with the persons to whom personal data are transferred in accordance with the law; that the persons to whom personal data are transferred will take the necessary security measures to protect personal data and ensure that these measures are complied with in their own organizations.
- In the event that the processed personal data is obtained by others through unlawful means, it shall notify the relevant person and the Board as soon as possible.
- When necessary, it employs personnel who are knowledgeable and experienced in the processing of personal data and provides training to its personnel within the scope of personal data protection legislation and data security.
- **The Company** shall conduct and have conducted the necessary audits to ensure the implementation of the provisions of the Law. It addresses privacy and security weaknesses revealed as a result of audits.

## 5. 5. MEASURES TAKEN REGARDING THE DESTRUCTION OF PERSONAL DATA

Although **the Company** has been processed in accordance with the provisions of the relevant law, it may delete or destroy personal data based on its own decision or upon the request of the personal data owner if the reasons requiring its processing disappear. Following the deletion of personal data, the persons concerned will not be able to access and use the deleted data again in any way. An effective data tracking process will be managed by **the Company** to define and monitor the destruction processes of personal data. The process carried out will be the identification of the data to be deleted, the

identification of the relevant persons, the identification of the access methods of the persons and the deletion of the data immediately afterwards.

**The Company** may use one or more of the following methods to destroy, delete or anonymize personal data, depending on the medium in which the data is recorded:

### 5.1 5.1 Methods for Deletion, Destruction and Anonymization of Personal Data

#### 5.1.1 5.1.1 Deletion of Personal Data

Deletion of personal data is the process of making personal data inaccessible and non-reusable in any way for the relevant users. As a method of deleting personal data, **the Company** may use one or more of the following methods:

- ✓ Personal data in paper media will be processed by drawing, painting, cutting or erasing with the blackout method.
- ✓ The access right(s) of the user(s) for office files located in the central file will be eliminated.
- ✓ The rows or columns containing personal information in the databases will be deleted with the 'Delete' command.

When necessary, it will be safely deleted with the help of an expert.

#### 5.1.2 5.1.2 Destruction of Personal Data

Destruction of personal data is the process of making personal data inaccessible, unrecoverable and unusable by anyone in any way by the following methods.

Physical Destruction

Destruction with Paper Shredder

De-magnetization: It is the method of passing magnetic media through special devices where it will be exposed to high magnetic fields, distorting the data on it in an unreadable way.

#### 5.1.3 5.1.3 Anonymization of Personal Data

Anonymization of personal data refers to making personal data impossible to be associated with an identified or identifiable natural person under any circumstances, even by matching it with other data. **The Company** may use one or more of the following methods to anonymize personal data:

**Masking:** Data masking is a method of anonymizing personal data by removing the basic identifying information of personal data from the data set.

**Record Extraction:** In the de-recording method, the stored data is anonymized by removing the row of data that contains a singularity among the data from the records.

**Territorial Hiding:** In the territorial hiding method, anonymization is achieved by hiding the relevant data if it is determinative because a single data creates a combination that is very rare.

**Global Coding:** With the data derivation method, a more general content is created from the content of personal data and it is ensured that personal data cannot be associated with any person. For example, specifying ages instead of dates of birth; specifying the region of residence instead of the street address.

**Adding Noise:** The method of adding noise to the data, especially in a data set where numerical data is predominant, anonymizes the data by adding some deviations in the plus or minus direction to the existing data at a determined rate. For example, in a dataset with weight values, a deviation of (+/-) 3 kg is used to prevent the display of actual values and anonymize the data. The deviation is applied equally to each value.

In accordance with Article 28 of the Law; anonymized personal data may be processed for purposes such as research, planning and statistics. Such processing is outside the scope of the Law and the explicit consent of the personal data owner will not be sought.

**The Company** may take ex officio decisions regarding the deletion, destruction or anonymization of personal data and may freely determine the method to be used according to the category it has chosen. In addition, within the scope of Article 13 of the Regulation, if the data subject chooses one of the categories of deletion, destruction or anonymization of his/her personal data during the application, **the Company** will be at liberty regarding the methods to be used in the relevant category.

## 6. 6. PERSONAL DATA STORAGE AND DESTRUCTION PERIODS

**The Company** retains personal data for the purposes for which they are processed for the periods specified in Annex-1. If a period of time is stipulated in the legislation regarding the storage of the personal data in question, this period shall be observed. In the absence of a period stipulated in the legislation, personal data will be retained for the maximum period for the retention of personal data in the table in Annex-1. These periods have been determined by evaluating **the Company**'s data categories and data subject groups; the data obtained as a result of this evaluation will ensure the fulfillment of the obligations stipulated in the laws and by observing the maximum statute of limitations (10 years) in the Turkish Code of Obligations.

In the event that the obligation to delete, destroy or anonymize arises due to the expiration of these periods, **the Company** deletes, destroys or anonymizes personal data in the first periodic destruction process following this date.

All transactions regarding the deletion, destruction and anonymization of personal data are recorded and such records are kept for at least three years, excluding other legal obligations.

## 7. 7. PERIODIC DESTRUCTION PERIODS

Pursuant to Article 11 of the Regulation, the periodic destruction period is set as 6 months. Accordingly, periodic destruction is carried out in June and December each year. In the said systems, the information will be erased in such a way that the information will not be retrieved again and will not be recycled from the tools such as documents, files, CDs, floppy disks, hard disks, if any, where the data is recorded.

## 8. PERSONNEL

Within the scope of the Law, the titles, units and job descriptions of the personnel whose obligations will be fulfilled in terms of the implementation of the data retention and destruction process of the Law, based on paragraph 1 of Article 11 of the Regulation, as the data controller of **the Company**, are determined by the table in Annex-2 of the Retention and Destruction Policy.

## 9. 9. REVISION AND REPEAL

If the Retention and Disposal Policy is amended or repealed, the new regulation will be announced on **the Company**'s website.

## 10.10. ENFORCEMENT

This Retention and Disposal Policy enters into force on the date of its publication.

**ANNEXES**
**ANNEX-1 PERSONAL DATA STORAGE AND DESTRUCTION PERIODS**
**Annex 2- Personal Data Retention and Disposal Personnel Table**

## ANNEX-1 PERSONAL DATA STORAGE AND DESTRUCTION PERIODS

| Data Category | Storage Period | Disposal Period |
|---|---|---|
| Identity | 10 years from the date of the transaction or termination of the legal relationship | At the first periodic destruction following the end of the storage period |
| Contact | 10 years from the date of the transaction or termination of the legal relationship | At the first periodic destruction following the end of the storage period |
| Location | 10 years from the date of the transaction or termination of the legal relationship | At the first periodic destruction following the end of the storage period |
| Compendiousness | 10 years from the end of employment | At the first periodic destruction following the end of the storage period |
| Legal Action | 5 years from the finalization of the judgment | At the first periodic destruction following the end of the storage period |
| | 10 years from the date of the transaction or termination of the legal relationship | At the first periodic destruction following the end of the storage period |
| Customer Transaction | 10 years from the date of the transaction or termination of the legal relationship | At the first periodic destruction following the end of the storage period |
| Physical Space Security | 30 days | At the first periodic destruction following the end of the storage period |
| Process Security | 10 years from the date of the transaction or termination of the legal relationship | At the first periodic destruction following the end of the storage period |
| Risk Management | 10 years from the date of the transaction or termination of the legal relationship | At the first periodic destruction following the end of the storage period |
| Finance | 10 years from the date of the transaction or termination of the legal relationship | At the first periodic destruction following the end of the storage period |
| Professional Experience | 10 years from the end of employment | At the first periodic destruction following the end of the storage period |
| Marketing | 10 years from the date of the transaction or termination of the legal relationship | At the first periodic destruction following the end of the storage period |
| Audiovisual Records | 10 years from the date of the transaction or termination of the legal relationship | At the first periodic destruction following the end of the storage period |
| Health Information | 15 Years | At the first periodic destruction following the end of the storage period |
| Criminal Conviction and Security Measures | 10 years from the end of employment | At the first periodic destruction following the end of the storage period |
| Biometric Data | Transaction date and 2 months from the termination of the legal | At the first periodic destruction following the end of the storage |

| | relationship | period |
|---|---|---|
| Family Information | 10 years from the end of employment | At the first periodic destruction following the end of the storage period |
| Professional experience | 10 years from the end of employment | At the first periodic destruction following the end of the storage period |
| Website Usage Data | 2 years | At the first periodic destruction following the end of the storage period |
| Reputation Management Information | 2 years | At the first periodic destruction following the end of the storage period |
| Incident Management Information | 10 years | At the first periodic destruction following the end of the storage period |
| Signature Information | 10 years | At the first periodic destruction following the end of the storage period |
| Insurance Information | 10 years from the end of employment | At the first periodic destruction following the end of the storage period |
| Vehicle Details | 10 years | At the first periodic destruction following the end of the storage period |
| Compliance Information | 10 years | At the first periodic destruction following the end of the storage period |
| Audit and Inspection | 10 years | At the first periodic destruction following the end of the storage period |

## Annex 2- Personal Data Retention and Disposal Personnel Table

| PERSONNEL | TITLE | RESPONSIBILITY |
|---|---|---|
| AYTAÇ MESTÇİ | IMPLEMENTATION RESPONSIBLE | Management of the personal data destruction process in accordance with the periodic destruction period by ensuring the compliance of the processes within the task with the retention period |