

TABLE OF CONTENTS

1. PURPOSE 1

**2. RECORDING MEDIA IN WHICH PERSONAL DATA ARE STORED
.... 1**

**3. EXPLANATIONS REGARDING THE REASONS REQUIRING
RETENTION 1**

**4. MEASURES TAKEN FOR THE PROTECTION OF PERSONAL DATA
.... 2**

4.1 Technical Measures 2

4.2 Administrative Measures 3

**5. MEASURES TAKEN FOR THE DESTRUCTION OF PERSONAL
DATA 4**

**5.1 Methods Regarding the Deletion, Destruction and Anonymization of
Personal Data 4**

5.1.1 Deletion of Personal Data 4 5.1.2 Destruction of Personal Data 4 5.1.3
Anonymization of Personal Data 5

**6. PERSONAL DATA RETENTION AND DESTRUCTION PERIODS
5**

7. PERIODIC DESTRUCTION PERIODS 6

8. REVISION AND REPEAL 6

9. ENTRY INTO FORCE 6

ANNEX 1 – Data Retention and Destruction Periods 7

1. PURPOSE

UĞUR TENKEKE AMBALAJ VE PLASTİK SANAYİ ANONİM ŞİRKETİ ("the Company") issues this Personal Data Retention and Destruction Policy ("Retention and Destruction Policy") for the purpose of regulating the technical and administrative protection of personal data in

accordance with Law No. 6698 on the Protection of Personal Data ("the Personal Data Protection Law (KVKK)" or "the Law"), and the implementation of the provisions of the Regulation on the Deletion, Destruction or Anonymization of Personal Data ("the Regulation"), published in the Official Gazette dated 28/10/2017, in the event that the conditions requiring the processing of personal data cease to exist.

2. RECORDING MEDIA IN WHICH PERSONAL DATA ARE STORED

Personal data belonging to data subjects are securely stored by UĞUR TENEKE AMBALAJ VE PLASTİK SANAYİ ANONİM ŞİRKETİ in the media listed below, in compliance with the provisions of the Law in particular and other applicable legislation:

Electronic media: - CRM - MS SQL Server - E-mail inbox - Microsoft Office programs - Image recording devices (CCTV/video recorders) - Software applications - Personal computers

Physical media: - Unit cabinets - Folders/binders - Archive - Paper

3. EXPLANATIONS REGARDING THE REASONS REQUIRING RETENTION

Personal data belonging to data subjects are stored securely by UĞUR TENEKE AMBALAJ VE PLASTİK SANAYİ ANONİM ŞİRKETİ in the physical or electronic media listed above, within the limits set out in the Law and other applicable legislation, in particular for the following purposes: a. Ensuring the continuity of operations, b. Fulfilling legal obligations, c. Planning and executing employee rights and fringe benefits, d. Managing business relationships.

Reasons requiring retention: a. The personal data being directly related to the establishment and performance of a contract, b. The personal data being necessary for the establishment, exercise or protection of a right, c. The personal data being processed for the legitimate interest of UĞUR TENEKE AMBALAJ VE PLASTİK SANAYİ ANONİM ŞİRKETİ, provided that this does not harm the fundamental rights and freedoms of the data subject, d. The personal data being necessary for UĞUR TENEKE AMBALAJ VE PLASTİK SANAYİ ANONİM ŞİRKETİ to fulfil a legal obligation, e. The retention of personal data being expressly provided for by legislation,

Page 2 f. In respect of retention activities requiring the explicit consent of data subjects, the existence of the explicit consent of the data subjects.

Pursuant to the Regulation, in the cases listed below, personal data belonging to data subjects shall be deleted, destroyed or anonymized by UĞUR TENEKE AMBALAJ VE PLASTİK SANAYİ ANONİM ŞİRKETİ, either ex officio or upon request:

a. The amendment or repeal of the relevant legislative provisions constituting the basis for the processing or retention of the personal data, b. The purpose requiring the processing or retention of the personal data ceasing to exist, c. The conditions requiring the processing of personal data under Articles 5 and 6 of the Law ceasing to exist, d. In cases where the processing of personal data is based solely on explicit consent, the data subject withdrawing such consent, e. The data controller accepting the application made by the data subject, within the scope of the rights set out in Article 11(2)(e) and (f) of the Law, requesting the deletion, destruction or anonymization of his/her personal data, f. In cases

where the data controller rejects the application made by the data subject requesting the deletion, destruction or anonymization of his/her personal data, finds its response to be insufficient, or fails to respond within the period stipulated by the Law, and the data subject files a complaint with the Board, and the Board finds the request justified, g. Despite the expiry of the maximum period requiring the retention of personal data, the absence of any condition that would justify retaining the personal data for a longer period.

4. MEASURES TAKEN FOR THE PROTECTION OF PERSONAL DATA

In accordance with Article 12 of the Law, UĞUR TENKEKE AMBALAJ VE PLASTİK SANAYİ ANONİM ŞİRKETİ takes the necessary technical and administrative measures to provide an appropriate level of security in order to prevent the unlawful processing of the personal data it processes, to prevent unlawful access to such data, and to ensure the safekeeping of the data, and carries out or has carried out the necessary audits within this scope. In the event that the personal data processed is obtained by third parties through unlawful means despite all technical and administrative measures having been taken, UĞUR TENKEKE AMBALAJ VE PLASTİK SANAYİ ANONİM ŞİRKETİ shall notify the relevant units of this situation as soon as possible.

4.1 Technical Measures

- Network security and application security are ensured. - A closed-circuit network is used for personal data transfers over the network. - Key management is applied. - Security measures are taken within the scope of the procurement, development and maintenance of information technology systems. - The security of personal data stored in the cloud is ensured. - Disciplinary regulations containing data security provisions are in place for employees. - Training and awareness activities on data security are conducted for employees at regular intervals. - An authorization matrix has been established for employees. - Access logs are kept regularly. - Data masking measures are applied where necessary. - Corporate policies on access, information security, use, retention and destruction have been prepared and put into practice.

Page 3 - Confidentiality undertakings are obtained. - The authorizations of employees who change duties or leave employment are revoked in this area. - Up-to-date anti-virus systems are used. - Firewalls are used. - Signed agreements contain data security provisions. - Personal data security policies and procedures have been established. - Personal data security issues are reported promptly. - Personal data security is monitored. - Necessary security measures are taken regarding entry to and exit from 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 minimized as much as possible. - Personal data is backed up, and the security of the backed-up personal data is also ensured. - A user account management and authorization control system is applied, and these are monitored. - Periodic and/or random internal audits are conducted or had conducted. - Log records are kept in a manner that precludes user intervention. - Existing risks and threats have been identified. - Protocols and procedures for the security of special categories of personal data have been established and are implemented. - If special categories of personal data are to be sent by e-mail, they are sent encrypted and using a registered e-mail (KEP) or corporate e-mail account. - Intrusion detection and prevention

systems are used. - Cyber security measures have been taken and their implementation is continuously monitored. - Encryption is applied. - Special categories of personal data transferred via removable media, CDs, or DVDs are transferred in encrypted form. - Data processors are periodically audited with respect to data security. - Data processors are made aware of data security matters. - Data loss prevention software is used.

4.2 Administrative Measures

- Employees are trained on the technical measures to be taken to prevent unlawful access to personal data. - Access and authorization processes for personal data within UĞUR TENEKE AMBALAJ VE PLASTİK SANAYİ ANONİM ŞİRKETİ are designed and implemented at the business-unit level in accordance with legal compliance requirements for the processing of personal data. Whether the data is of a special category and its degree of importance are also taken into account when limiting access. - UĞUR TENEKE AMBALAJ VE PLASTİK SANAYİ ANONİM ŞİRKETİ has added provisions to all documents governing its relationship with its personnel and containing personal data, stating that the obligations set out in the Law must be complied with in order to process personal data lawfully, that personal data must not be disclosed, that personal data must not be used unlawfully, and that the confidentiality obligation regarding personal data continues even after the termination of the employment relationship with UĞUR TENEKE AMBALAJ VE PLASTİK SANAYİ ANONİM ŞİRKETİ. - Employees are informed that they may not disclose to others, in violation of the provisions of the Law, the personal data they have learned, and may not use it for purposes other than the purpose of processing, and that this obligation continues even after they leave their duties; and the necessary undertakings are obtained from them in this regard.

Page 4 - Provisions are added to agreements concluded by UĞUR TENEKE AMBALAJ VE PLASTİK SANAYİ ANONİM ŞİRKETİ with persons to whom personal data are lawfully transferred, stating that such persons will take the necessary security measures for the protection of personal data and will ensure compliance with these measures within their own organizations. - In the event that personal data being processed is obtained by others through unlawful means, this is notified to the data subject and to the Board as soon as possible. - Where necessary, personnel who are knowledgeable and experienced in the processing of personal data are employed, and personnel are provided with training on personal data protection legislation and data security. - UĞUR TENEKE AMBALAJ VE PLASTİK SANAYİ ANONİM ŞİRKETİ carries out or has carried out the necessary audits to ensure the implementation of the provisions of the Law. It remedies any confidentiality and security deficiencies revealed as a result of such audits.

5. MEASURES TAKEN FOR THE DESTRUCTION OF PERSONAL DATA

Although processed in accordance with the relevant legal provisions, UĞUR TENEKE AMBALAJ VE PLASTİK SANAYİ ANONİM ŞİRKETİ may delete or destroy personal data, upon its own decision or upon the request of the personal data subject, in the event that the reasons requiring processing cease to exist. Following the deletion of personal data, the data subjects will in no way be able to access or use the deleted data again. Our Company will manage an effective data-tracking process for the identification and monitoring of personal data destruction processes. The process to be carried out will consist, in order, of identifying the data to be deleted, identifying the relevant persons, identifying the persons'

access methods, and then immediately deleting the data.

Depending on the medium in which the data is recorded, our Company may use one or more of the methods specified below to destroy, delete or anonymize personal data:

5.1 Methods Regarding the Deletion, Destruction and Anonymization of Personal Data

5.1.1 Deletion of Personal Data Deletion of personal data is the process of rendering personal data completely inaccessible and unusable again by the relevant users. Our Company may use one or more of the following methods for the deletion of personal data:

- Personal data on paper media will be processed using the blackout method, by scratching out, painting over, cutting out, or erasing. - For office files located in a central file/directory, the access right(s) of the user(s) will be revoked. - Rows or columns containing personal information in databases will be deleted using the "Delete" command. Where necessary, deletion will be carried out securely with the assistance of an expert.

5.1.2 Destruction of Personal Data Destruction of personal data is the process of rendering personal data completely inaccessible, unrecoverable and unusable again by anyone, through the methods set out below. **Physical Destruction** Destruction by paper shredder **Demagnetization:** The method whereby magnetic media is passed through special devices that expose it to strong magnetic fields, thereby corrupting the data on it in an unreadable manner.

Page 5 **5.1.3 Anonymization of Personal Data** Anonymization of personal data means rendering personal data incapable of being associated, under any circumstances, with an identified or identifiable natural person, even when matched with other data. UĞUR TENEKE AMBALAJ VE PLASTİK SANAYİ ANONİM ŞİRKETİ may use one or more of the methods specified below to anonymize personal data:

Masking: A method of anonymizing personal data by removing the primary identifying information of the data from the data set.

Removing records: In the record-removal method, the row(s) of data containing a distinguishing feature are removed from among the records, thereby anonymizing the retained data.

Regional concealment: In the regional-concealment method, if a single piece of data has a distinguishing quality because it creates a rarely-occurring combination, the concealment of that data provides anonymization.

Global coding (generalization): Through the data-derivation method, more general content is created from the content of the personal data, rendering the personal data incapable of being associated with any individual. For example, stating ages instead of dates of birth; stating the region of residence instead of the full address.

Adding noise: The noise-addition method, used particularly in data sets dominated by numerical data, anonymizes the data by adding certain deviations, in a determined proportion, in a positive or negative direction to the existing data. For example, in a data set containing weight values, using a deviation of (+/-) 3 kg prevents the display of the real values, thereby anonymizing 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 falls outside the scope of the Law, and the explicit consent of the personal data subject will not be required.

Our Company may decide ex officio on the deletion, destruction or anonymization of personal data, and may freely determine the method to be used according to the category it has selected. Furthermore, pursuant to Article 13 of the Regulation, where the data subject chooses one of the categories of deletion, destruction or anonymization of his/her personal data at the time of application, UĞUR TENKEKE AMBALAJ VE PLASTİK ANONİM ŞİRKETİ will also be free to determine the methods to be used within that category.

6. PERSONAL DATA RETENTION AND DESTRUCTION PERIODS

Our Company retains personal data, for the purposes for which they are processed, for the periods specified in Annex 1. Where the legislation stipulates a period for the retention of the personal data in question, that period shall be observed. Where no period is stipulated by the legislation, personal data will be retained for the maximum period specified in the table in Annex 1 for the retention of the personal data. These periods have been determined by evaluating the data categories and the data subject groups of UĞUR TENKEKE AMBALAJ VE PLASTİK SANAYİ ANONİM ŞİRKETİ; taking into account the fulfilment of the obligations set out in the laws with respect to the data obtained as a result of this evaluation, and taking into account, as a maximum, the statute-of-limitations period (10 years) set out in the Turkish Code of Obligations.

Where the obligation to delete, destroy or anonymize the data arises upon the expiry of these periods, our Company shall delete, destroy or anonymize the personal data at the first periodic destruction process following that date.

Page 6 All actions taken with respect to the deletion, destruction and anonymization of personal data are recorded, and such records are retained for at least three years, except for other legal obligations.

7. PERIODIC DESTRUCTION PERIODS

Pursuant to Article 11 of the Regulation, the periodic destruction period has been determined as 6 months. Accordingly, the periodic destruction process is carried out in February and August of each year. In the relevant systems, information will be anonymized and/or deleted in such a way that it cannot be recovered again, and, where applicable, in such a way that documents, files, CDs, diskettes, hard disks or other media on which the data is recorded cannot be reconstituted.

8. REVISION AND REPEAL

In the event that the Retention and Destruction Policy is amended or repealed, the new version will be announced on the website of UĞUR TENKEKE AMBALAJ VE PLASTİK SANAYİ ANONİM ŞİRKETİ (<https://www.ugurteneke.com.tr/>).

9. ENTRY INTO FORCE

This Retention and Destruction Policy shall enter into force on the date of its publication.

ANNEXES ANNEX 1 – Data Retention and Destruction Periods

Page 7 ANNEX 1 – Data Retention and Destruction Periods

Data Category: Identity Retention Period: 15 years from the transaction date or the termination of the legal relationship Destruction Period: At the first periodic destruction period following the expiry of the retention period

Data Category: Contact Retention Period: 15 years from the transaction date or the termination of the legal relationship Destruction Period: At the first periodic destruction period following the expiry of the retention period

Data Category: Location Retention Period: 10 years from the transaction date or the termination of the legal relationship Destruction Period: At the first periodic destruction period following the expiry of the retention period

Data Category: Personnel Records Retention Period: 15 years from the termination of employment Destruction Period: At the first periodic destruction period following the expiry of the retention period

Data Category: Customer Transaction Retention Period: 10 years from the transaction date or the termination of the legal relationship Destruction Period: At the first periodic destruction period following the expiry of the retention period

Data Category: Legal Transaction Retention Period: 15 years from the transaction date or the termination of the legal relationship Destruction Period: At the first periodic destruction period following the expiry of the retention period

Data Category: Physical Premises Security Retention Period: 1 year from the transaction date or the termination of the legal relationship Destruction Period: At the first periodic destruction period following the expiry of the retention period

Data Category: Transaction Security Retention Period: 10 years from the transaction date or the termination of the legal relationship Destruction Period: At the first periodic destruction period following the expiry of the retention period

Data Category: Risk Management Retention Period: 10 years from the transaction date or the termination of the legal relationship Destruction Period: At the first periodic destruction period following the expiry of the retention period

Data Category: Finance Retention Period: 10 years from the transaction date or the termination of the legal relationship Destruction Period: At the first periodic destruction period following the expiry of the retention period

Data Category: Professional Experience Retention Period: 15 years from the termination of employment Destruction Period: At the first periodic destruction period following the expiry of the retention period

Data Category: Marketing Retention Period: 1 year Destruction Period: At the first periodic destruction period following the expiry of the retention period

Data Category: Audio and Visual Records Retention Period: Other: 2 weeks Destruction Period: At the first periodic destruction period following the expiry of the retention period

Data Category: Philosophical Belief, Religion, Sect and Other Beliefs Retention Period: 15 years from the transaction date or the termination of the legal relationship Destruction Period: At the first periodic destruction period following the expiry of the retention period

Data Category: Dress and Appearance Retention Period: Other: 2 weeks Destruction Period: At the first periodic destruction period following the expiry of the retention period

Data Category: Association Membership Retention Period: 15 years from the transaction date or the termination of the legal relationship Destruction Period: At the first periodic destruction period following the expiry of the retention period

Data Category: Foundation Membership Retention Period: 15 years from the transaction date or the termination of the legal relationship Destruction Period: At the first periodic destruction period following the expiry of the retention period

Data Category: Trade Union Membership Retention Period: 15 years from the transaction date or the termination of the legal relationship Destruction Period: At the first periodic destruction period following the expiry of the retention period

Data Category: Health Information Retention Period: 15 years from the transaction date or the termination of the legal relationship Destruction Period: At the first periodic destruction period following the expiry of the retention period

Data Category: Criminal Conviction and Security Measures Retention Period: 15 years from the transaction date or the termination of the legal relationship Destruction Period: At the first periodic destruction period following the expiry of the retention period