

09/12/2019

1

TABLE OF CONTENTS 1.

INTRODUCTION.....2

1.1. Definitions2

1.2. Purpose and Scope of the Personal Data Protection Policy.....3

2. PROCESSING OF PERSONAL DATA.....4

2.1. General Principles Regarding the Processing of Personal Data4

2.2. Conditions for the Processing of Personal Data5

2.3. Purposes of Processing Personal Data6

2.4. Method of Collecting Personal Data7

3. TRANSFER OF PERSONAL DATA.....7 4.

STORAGE AND DESTRUCTION OF PERSONAL DATA.....8

5. TECHNICAL AND ADMINISTRATIVE MEASURES FOR DATA

SECURITY..... 9 6. RIGHTS OF DATA SUBJECTS OVER THEIR

PERSONAL DATA..... 10 7. AMENDMENTS TO THE PERSONAL DATA

PROTECTION POLICY.....11

2

1. INTRODUCTION

The protection of personal data is a matter of significant importance for Uğur Teneke Ambalaj ve Plastik Sanayi A.Ş. (hereinafter referred to as "Uğur Teneke" or the "Company"). Since its founding, Uğur Teneke has kept confidential the personal data it has obtained from natural persons in the course of its activities and has taken all manner of technical and administrative measures to ensure the protection of personal data and data security. Even before 7 April 2016, the date on which Law No. 6698 on the Protection of Personal Data (the "KVKK", hereinafter referred to as the Personal Data Protection Law (KVKK)) entered into force, Uğur Teneke had adopted and applied the confidentiality of personal data as a working principle.

In order to conduct all of its activities in a manner compliant with both the Constitution of the Republic of Turkey and the KVKK and its related secondary legislation, the Company adopts all of the principles set out in the KVKK and fulfills its obligations relating to the processing, deletion, destruction, and anonymization of personal data, the transfer of such

data, the informing of data subjects, and the provision of data security. This Personal Data Protection Policy ("KVKK Policy"), prepared within this scope, is made available to the natural persons whose personal data is processed.

1.1. DEFINITIONS

"Explicit Consent" Consent relating to a specific matter, based on information, and expressed by free will "Employee" A natural person who has an employer-employee-type relationship with Uğur Teneke based on an employment contract or a service agreement "KVKK" or "the Law" Law No. 6698 on the Protection of Personal Data "Personal Data" Any information relating to an identified or identifiable natural person "Anonymization of Personal Data" The process of rendering personal data incapable, under any circumstances, of being associated with an identified or identifiable natural person, even by matching it with other data "Processing of Personal Data" Any operation performed on personal data, such as obtaining, recording, storing, preserving, altering, reorganizing, disclosing, transferring, taking over, making retrievable, classifying, or preventing the use of such data, whether wholly or partly by automated means, or by non-automated means provided that it forms part of a data recording system "Deletion of Personal Data" The process of rendering personal data inaccessible and unusable by the relevant users in any way whatsoever

3 "Destruction of Personal Data" The process of rendering personal data inaccessible, irretrievable, and unusable by anyone, in any way whatsoever "Board" The Personal Data Protection Board (KVKK Board) "Authority" The Personal Data Protection Authority "Special Categories of Personal Data" Data relating to a person's race, ethnic origin, political opinion, philosophical belief, religion, sect, or other beliefs, appearance and dress, membership of an association, foundation, or trade union, health, sexual life, criminal conviction and security measures, as well as biometric and genetic data "KVKK Policy" Uğur Teneke Personal Data Protection Policy "Uğur Teneke" or "the Company" Uğur Teneke Ambalaj ve Plastik Sanayi A.Ş. "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 "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

1.2. PURPOSE AND SCOPE OF THE KVKK POLICY

This KVKK Policy explains matters relating to the obtaining, use, transfer, destruction, and other forms of processing of personal data by Uğur Teneke, as well as the technical and administrative measures taken by the Company to protect personal data and the rights of data subjects. This KVKK Policy applies to the personal data of: • Employees, • Job applicants, • Company shareholders, • Company officers, • Visitors, • Employees of institutions with which the Company cooperates, • Persons who access any type of application or service offered by the Company, and • Third parties, processed within the scope of the KVKK. Personal data obtained through the explicit consent of the data subjects, or under any of the other lawful bases set out in the KVKK, is processed for the purpose of fulfilling Uğur Teneke's legal obligations, providing its services

4 appropriately, increasing the quality of the services provided, improving quality policy, and for the other purposes specified in this KVKK Policy.

2. PROCESSING OF PERSONAL DATA

2.1. GENERAL PRINCIPLES REGARDING THE PROCESSING OF PERSONAL DATA

Uğur Teneke complies with the principles set out in Article 4 of the KVKK when carrying out personal data processing activities.

- Lawfulness and compliance with the rules of good faith: Uğur Teneke inquires into the source of the personal data it obtains from the data subject or from third parties, and attaches importance to the lawful and good-faith acquisition and processing of such data. In this context, the Company issues the necessary warnings and notifications to the third parties to whom it transfers personal data, for the purpose of protecting such data.
- Being accurate and, where necessary, up to date: Uğur Teneke attaches importance to ensuring that all data held within its legal entity is accurate, does not contain incorrect information, and, in the event of any change to personal data, is updated where such changes are communicated to it. The Company exercises reasonable care and attention regarding the accuracy and currency of the personal data declared by its customers or by third parties who make contact with it.
- Being processed for specified, explicit, and legitimate purposes: Uğur Teneke sets out its legitimate and lawful data processing purposes in a specific and explicit manner before commencing personal data processing activities. Personal data is not processed for purposes other than those so determined.
- Being relevant, limited, and proportionate to the purposes for which they are processed: Uğur Teneke carries out personal data processing activities strictly limited to the purpose of processing. Personal data that is not relevant to the specified purpose is not processed by Uğur Teneke.
- Being retained for the period stipulated by the relevant legislation or required for the purpose for which they are processed:

5 Uğur Teneke retains personal data for the period stipulated by legislation or required by the purpose of processing. However, once the period stipulated by legislation has expired or all purposes of processing have ceased to exist, it deletes, destroys, or anonymizes the personal data.

These principles apply regardless of whether the Company has processed personal data based on explicit consent or in accordance with the other data processing conditions. In this respect, Uğur Teneke processes personal data in accordance with the data processing conditions and general principles, and also fulfills its obligation to inform data subjects.

2.2. CONDITIONS FOR THE PROCESSING OF PERSONAL DATA

Uğur Teneke processes personal data based on explicit consent or in accordance with the following conditions set out for the other data processing bases: • It is expressly provided for by law. • It is mandatory for the protection of the life or physical integrity of the person

concerned or of another person, where the person concerned is unable to give consent due to actual impossibility or where consent is not legally valid. • Processing is directly related to the establishment or performance of a contract, provided that it concerns the personal data of the parties to the contract. • It is mandatory for the data controller to fulfill its legal obligation. • The data has been made public by the data subject themselves. • Data processing is mandatory for the establishment, exercise, or protection of a right. • Data processing is mandatory for the legitimate interests of the data controller, provided that this does not harm the fundamental rights and freedoms of the data subject.

Under the KVKK, data relating to a person's race, ethnic origin, political opinion, philosophical belief, religion, sect, or other beliefs, appearance and dress, membership of an association, foundation, or trade union, health, sexual life, criminal conviction and security measures, as well as biometric and genetic data, constitute special categories of personal data.

Uğur Teneke takes the additional measures stipulated by the KVKK and by the Personal Data Protection Board (KVKK Board) when processing special categories of personal data.

In processing special categories of personal data, the data processing conditions set out in Article 6 of the KVKK and the additional measures announced by the Personal Data Protection Board (KVKK Board) are complied with. Within this scope, special categories of personal data are processed in the following cases: • Where the explicit consent of the data subject has been obtained,

6 • Where the processing of special categories of personal data other than health and sexual life data is expressly provided for by law. • Where data relating to health and sexual life is processed for the purposes of protection of public health, preventive medicine, medical diagnosis, treatment, and care services, or the planning and management of health services and their financing, by persons subject to a confidentiality obligation.

The procedures and principles regarding the processing, destruction, and protection of special categories of personal data are regulated by the Uğur Teneke Policy on the Protection and Processing of Special Categories of Personal Data.

2.3. PURPOSES OF PROCESSING PERSONAL DATA

Uğur Teneke processes personal data, within the framework of the legal grounds set out in Articles 5 and 6 of the KVKK, for the purposes listed below:

Within the scope of the planning and execution of human resources activities: the personal data of job applicants is processed for the purposes of evaluating suitability for the position and carrying out recruitment processes; the personal data of employees is processed for the purposes of performing the employment contract, establishing fringe benefits, carrying out promotion/bonus/salary-increase processes, fulfilling obligations arising from the legislation to which the Company is subject (in particular the Labor Law), carrying out social insurance processes, evaluating employee performance, and similar purposes.

In addition, the Company processes personal data within the scope of its ordinary business activities and the services it provides to its customers, for purposes including: the planning and execution of corporate sustainability activities; event management; the management of relationships with business partners or suppliers; the execution/monitoring of financial

reporting and risk management transactions; the execution/monitoring of legal affairs; the planning and execution of corporate communication activities; the execution of corporate governance activities; carrying out company and partnership law transactions; the management of requests and complaints; the management of investor relations; ensuring the security of Uğur Teneke's buildings and facilities; the creation and monitoring of visitor records; the determination and implementation of the Company's commercial and business strategies; resolving the problems and complaints of data subjects, ensuring their satisfaction, and providing effective service; responding to requests for information from administrative and judicial authorities; ensuring compliance with legal processes and legislation; ensuring information and transaction security and preventing malicious use; and similar purposes.

Where a processing activity carried out for the aforementioned purposes does not satisfy any of the other data processing conditions set out under the KVKK, Uğur Teneke obtains the explicit consent of the data subject in respect of the relevant data processing process.

7

2.4. METHOD OF COLLECTING PERSONAL DATA

Uğur Teneke collects personal data through contracts, digital media, notifications from administrative and judicial authorities, electronic mail, and other communication channels, verbally, electronically, or in writing, in physical and electronic environments, in accordance with the personal data processing conditions specified in the KVKK and in line with the legal grounds set out in this KVKK Policy. Such personal data is processed, primarily, within the scope of this KVKK Policy, for the purpose of establishing a contract and providing better service to data subjects.

In this context, personal data may be obtained when the services offered by the Company are used, when a legal relationship is established with the Company (purchase, intermediation, employment, etc.), or when contact is made with the Company in relation to services (by post, e-mail, etc.).

Uğur Teneke adopts the principle of acting lawfully when obtaining personal data from both its business partners and its solution partners. Data is collected from business partners and solution partners subject to a data confidentiality undertaking and only to the extent required by the service, and measures are taken at this point to ensure data security.

Uğur Teneke processes the personal data of its employees to the extent necessary for the employment relationship and, in other cases permitted by the relevant legislation, without obtaining consent, while ensuring the confidentiality and protection of the personal data belonging to its employees.

3. TRANSFER OF PERSONAL DATA

The Company transfers personal data to third parties only for the purposes specified in this KVKK Policy and in accordance with Articles 8 and 9 of the KVKK. In this context, the Company may transfer the personal data it collects to the following persons and institutions for specific purposes: • To the Company's business partners, limited to ensuring the fulfillment of the purposes for which the business partnership was established, • To the Company's suppliers, limited to ensuring that the services outsourced from the supplier and

necessary for the Company to carry out its commercial activities are provided to the Company, • To the Company's customers, • To authorized public institutions and organizations, upon request, • To the Company's solution partners,

8 The Company's purpose in sharing personal data is to provide access to services, to fulfill its legal obligations, to ensure the performance of the contract it has entered into with the data subject, to carry out purchase and sale transactions, to prevent and detect fraudulent or unlawful activities related to the services, and to carry out its other commercial activities in a lawful manner.

Uğur Teneke adopts the principle of acting lawfully in its data-sharing activities. Data is shared with the third parties to whom personal data is transferred only to the extent required by the service. Utmost care is taken to ensure that these parties adopt measures relating to data security.

The personal data subject to the domestic and international transfers referred to above is protected legally, through data transfer agreements, in addition to the technical measures that ensure data security.

The Company may share the personal data it processes with public institutions and organizations that are legally authorized to request such information, for the purpose of fulfilling its legal obligations (including, but not limited to, combating crime, threats to state and public security, and similar situations where the Company has a legal or administrative obligation to notify or provide information).

4. STORAGE AND DESTRUCTION OF PERSONAL DATA

Pursuant to the KVKK, personal data is kept accurate and up to date and is retained for the period stipulated by the relevant legislation or required for the purpose for which it is processed. This period is determined separately for each category of personal data, and upon expiry of this period, the relevant personal data is deleted, destroyed, or anonymized at the end of the periodic destruction periods determined in accordance with the Regulation on the Deletion, Destruction, or Anonymization of Personal Data.

Deletion of personal data refers to the process of rendering personal data inaccessible and unusable by the relevant users in any way whatsoever; destruction of personal data refers to the process of rendering personal data inaccessible, irretrievable, and unusable by anyone in any way whatsoever; anonymization of personal data refers to the process of rendering personal data incapable, under any circumstances, of being associated with an identified or identifiable natural person, even if matched with other data.

In this context, Uğur Teneke has determined the necessary periodic destruction periods and has established a Personal Data Retention and Destruction Policy. The Company records all transactions carried out in relation to the deletion, destruction, and anonymization of personal data, and retains such records for a period of at least three years, except where other legal obligations apply.

9 When a data subject applies to the Company requesting the deletion or destruction of their personal data, Uğur Teneke: • Where all of the conditions for processing the personal data have ceased to exist, deletes, destroys, or anonymizes the personal data subject to

the request. It finalizes the data subject's request within thirty days at the latest and informs the data subject. • Where all of the conditions for processing the personal data have ceased to exist and the personal data subject to the request has been transferred to third parties, notifies the third party of this situation and ensures that the necessary action is taken by the third party. • Where not all of the conditions for processing the personal data have ceased to exist, may reject this request by explaining its justification pursuant to the third paragraph of Article 13 of the KVKK, and communicates its rejection response to the data subject in writing or electronically within thirty days at the latest.

5. TECHNICAL AND ADMINISTRATIVE MEASURES TAKEN TO ENSURE THE SECURITY OF PERSONAL DATA Uğur Teneke takes technical and administrative measures, in line with technological possibilities and the cost of implementation, in order to ensure that personal data is processed lawfully. The technical and administrative measures taken to protect personal data are applied with particular care and additional measures with respect to special categories of personal data, and the necessary audits are carried out periodically within the Company at the highest level.

Uğur Teneke has taken every appropriate security measure to ensure that personal data is processed only for the purposes specified in this KVKK Policy and to reduce risks such as malicious use, unauthorized access to personal data, unauthorized sharing, destruction, or alteration of personal data. These security measures also cover other precautions taken with respect to matters such as the transfer of personal data to countries that may not provide an adequate level of data protection.

Personal data is confidential, and Uğur Teneke observes this confidentiality. Personal data can only be accessed by persons who have been authorized within the Company. In this context, it is ensured that software complies with standards, that third parties are chosen with care, and that the data protection policy is observed within the Company.

Within the scope of the technical and administrative measures taken by Uğur Teneke to ensure data security, the Company: • Organizes regular training and awareness programs for its employees on the protection of personal data. • Establishes policies based on the Company's personal data processing inventory and structures the processes necessary for the implementation of these policies.

10 • Identifies the risks within the scope of personal data protection law faced by the Company and carries out work aimed at eliminating such risks with due care. In this context, it creates active channels for providing information notices and obtaining explicit consent. • Carries out periodic internal audits within the Company in order to fulfill obligations relating to personal data protection law. • Continuously obtains legal advisory services regarding compliance with updated legislation. • Establishes a separate policy for the protection of special categories of personal data and implements the additional measures determined by the Board. • Implements the necessary measures, such as data-sharing agreements, for managing relationships with data processors. • Establishes secure technical infrastructure to ensure the security of the databases in which personal data will be stored. • Determines procedures for reporting on the technical measures taken and audit processes. • Security measures are periodically renewed and improved. • Network security and application security are ensured. • A closed-system network is used for the transfer of personal data over networks. • Key management is implemented. • 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. • An authorization matrix has been established for employees. • Access logs are kept regularly. • Corporate policies on access, information security, use, storage, and destruction have been prepared and put into practice. • Data masking measures are applied where necessary. • The authorizations of employees who change roles or leave the Company in this area are revoked. • Up-to-date anti-virus systems are used. • Firewalls are used. • Personal data security issues are reported promptly. • Personal data security is monitored. • The security of media containing personal data is ensured. • Personal data is backed up, and the security of the backed-up personal data is also ensured.

11 • A user account management and authorization control system is implemented, and these are also monitored. • Log records are kept in a manner that cannot be interfered with by users. • Intrusion detection and prevention systems are used. • Cybersecurity measures have been taken, and their implementation is continuously monitored. • Encryption is applied. • Penetration testing is applied. • Data loss prevention software is used.

Notwithstanding that Uğur Teneke takes the necessary information security measures, in the event that personal data is damaged or falls into the hands of unauthorized third parties as a result of attacks on the platforms operated by Uğur Teneke or on the Company's systems, Uğur Teneke immediately takes action to remedy such breach and minimizes the harm to the data subject. Uğur Teneke immediately notifies this situation to the relevant data subjects and to the Board, and takes the necessary measures.

6. RIGHTS OF DATA SUBJECTS OVER THEIR PERSONAL DATA

Under the Constitution of the Republic of Turkey, everyone has the right to request the protection of their personal data. In this context, the rights of the data subject over their personal data are set out in Article 11 of the KVKK as follows: • To learn whether or not their personal data has been processed, • To request information regarding such processing, if their personal data has been processed, • To learn the purpose of processing personal data and whether such data is used in accordance with its purpose, • To know the third parties, domestic or foreign, to whom their personal data has been transferred, • To request the correction of their personal data if it has been processed incompletely or incorrectly, • To request the deletion or destruction of their personal data within the framework of the conditions set out in Article 7 of the KVKK, • To request that the deletion, destruction, or correction transactions be notified to the third parties to whom the personal data has been transferred, • To object to the emergence of a result to their detriment through the exclusive analysis of their processed data via automated systems, • To claim compensation for damages in the event that they suffer harm due to the unlawful processing of their personal data under the KVKK.

12 Where data subjects submit requests relating to the rights listed above to the Company in accordance with the application procedures set out in the Communiqué on the Procedures and Principles Regarding Applications to the Data Controller, Uğur Teneke will conclude such requests free of charge, as soon as possible according to their nature and within thirty (30) days at the latest. However, where the transaction requires an additional cost, Uğur Teneke may charge the fee set out in the tariff determined by the Board.

The data subject may submit their requests relating to the rights set out above in writing, or by using a registered electronic mail (KEP) address, secure electronic signature, mobile signature, or the electronic mail address previously notified by the data subject to the Company and registered in Uğur Teneke's system. The application submitted must include:

- Name, surname, and, if the application is in writing, signature,
- For citizens of the Republic of Turkey, their Turkish ID number; for foreign nationals, their nationality, passport number, or, if any, identification number,
- Residential or business address for service of notice,
- Electronic mail address, telephone, and fax number, if any, to be used for notification,
- The subject matter of the request, and the information and documents relating to the matter must be attached to the application.

Applications will only be considered for evaluation if submitted in Turkish. In order for a third party to submit an application request on behalf of a data subject, a special power of attorney issued by a notary public on behalf of the person submitting the application must be provided by the data subject.

7. AMENDMENTS TO THE KVKK POLICY

Uğur Teneke may amend this KVKK Policy at any time. Such amendments take effect on the date the amended new KVKK Policy is published. Data subjects will be provided with the necessary notifications in order to be informed of amendments to this KVKK Policy.