Personal Data Storage and Destruction Policy

EYS.PO.30 Relase Date: 10.01.2023

CONTENTS

1- SCOPE

1. This Personal Data Storage and Destruction Policy ("Policy"); It covers all Company directorates, units, employees and third parties involved in the processes where YUCHISOFT BİLİŞİM SİSTEM VE ÇÖZÜMLERİ SANAYİ VE TİCARET LİMİTED ŞİRKETİ ("Company") processes personal data.
2. This Policy; It covers all storage and destruction activities that the Company will perform on personal data.
3. This Policy will only apply to the destruction and storage of personal data.
4. In case the Law, Regulation or other legislation is partially or completely changed, amended, updated or repealed, the Company will update and change the Policy to comply with the new Law, Regulation or legislation.

2- DEFINITIONS

The concepts used in the implementation of this Policy have the meanings given below;

Recipient Group	It is the group of real or legal persons to whom personal data is transferred by the data controller.
Related User	Persons who process personal data within the data controller organization or in line with the authority and instructions received from the data controller, excluding the person or unit responsible for the technical storage, protection and backup of the data.
Destruction **Law** **Logging Media**	Deletion, destruction or anonymization of personal data Personal Data Protection Law No. 6698 It is any environment where personal data is processed by fully or partially automatic or non-automatic means, provided that it is part of any data logging system.
Personal Data Processing Inventory	Personal data processing activities carried out depending on the company's business processes; It is an inventory that is created by associating personal data with the processing purposes, data category, transferred recipient group and data subject person group, and details the maximum period required for the purposes for which personal data are processed, personal data envisaged to be transferred to foreign countries, and measures taken regarding data security.
Board **Periodic Destruction**	Personal Data Protection Board It is the process of deletion, destruction or anonymization to be carried out ex officio by the Company within certain time intervals specified in this Policy, in case all the conditions for processing personal data specified in the law are eliminated.
Registry	It is the Data Controllers Registry to be kept by the Board in accordance with the Draft Regulation on the Data Owners Registry, which is not currently in force.
Data Logging System	It is a logging system in which personal data is structured and processed according to certain criteria.
Data Owner Regulation	It is the natural or legal person who determines the purposes and means of processing personal data and is responsible for establishing and managing the data logging system. Regulation on Deletion, Destruction or Anonymization of Personal Data

3- PURPOSE AND SCOPE

This Policy applies to real or legal persons responsible for the destruction of personal data included in the Regulation established in accordance with Article 7 of the Law and determines the principles to be followed by the Company and third parties whom the Company holds contractually responsible.

Pursuant to the Regulation, the Company, as a Data Controller who is obliged to register in the Registry, is obliged to prepare and act in accordance with this Policy in order to store the personal data in its possession in accordance with the personal data inventory and to destroy it when necessary.

The following principles will apply to the storage and destruction of personal data:

a) The general principles in Article 4 of the Law will be complied with.

b) The Company acknowledges that preparing this Policy alone does not mean that personal data is destroyed in accordance with the Regulation, Law and relevant legislation.

c) The Company accepts, declares and undertakes that it will act in accordance with the security measures in Article 12 of the Law, the provisions of the relevant legislation, the decisions of the Board and this Policy when storing or deleting, destroying or anonymizing personal data.

d) The Company undertakes to comply with this Policy and the tools, programs and processes to be applied in accordance with the Policy during the destruction of the personal data it holds, whose purpose is fully or partially automatic or processed by non-automatic means provided that it is part of any recording system.

e) The Company takes all necessary technical and administrative measures to securely store personal data and prevent unlawful processing and access. These technical and administrative measures are described in technical guides regarding the methods to be used for the storage and destruction of personal data.

f) The Company determines the titles, units and job descriptions of those who will be involved in the storage and destruction of personal data.

4- LOGGING MEDIA

With this Policy, the Company agrees to include personal data in the environments listed below that contain personal data and in other media that may arise in addition to these, within the scope of the Policy.

a) Computers / servers used on behalf of the company
b) Network devices,
c) Shared / non-shared disk drives used for storing data on the network,
d) Mobile phones and all their storage areas,
e) Paper,
f) Microfiche,
g) Peripherals such as printer, fingerprint reader,
h) Magnetic tapes,
i) Optical discs,
j) Flash memories.

5- STATES REQUIRING DESTRUCTION OF PERSONAL DATA

In the event of a violation within the scope specified below, the Potential Security Violation situation will be accepted and the relevant security violation processes will be carried out by the Company, and relevant reports and notifications will be shared with the Company management, the Board and relevant personal data owners when deemed necessary. For this purpose, the Company's violation management processes will be applied to make such reports and notifications. In case of a personal data breach, the data owner will be notified of the breach on the website or via contact information after the necessary inspections.

1. Contravention of the Law

ŞThe Company undertakes that it will not process personal data contrary to the manner specified in the Law. Unless there are exceptions to the conditions for processing personal data in Articles 5 and 6 of the Law, the Company;

a) It will not store the personal data of people whose express consent has not been obtained, except for the exceptions specified in the Law.

b) If the purpose of processing data processed within the scope of an exception or within the scope of explicit consent is eliminated and/or the legal retention period expires, the Company will not store and destroy this personal data.

2. Elimination of Personal Data Processing Conditions

The company is responsible for keeping the data processing conditions up-to-date and shares this responsibility with all relevant employees who process personal data.

Employees will not continue to process data in cases where the conditions for data processing no longer exist. These situations are determined by the Internal Control, Compliance and Legal department upon the recommendation of the relevant business unit and are destroyed in accordance with this Policy.

The Company accepts that the data processing conditions are eliminated in the relevant cases listed below and specified in the Regulation:

a) Amendment or repeal of the provisions of the relevant legislation that constitute the basis for processing personal data;

b) The contract between the parties has never been established, the contract is invalid, the contract terminates automatically, the contract is terminated or the contract is withdrawn,

c) Elimination of the purpose requiring the processing of personal data,

d) Processing personal data is against the law or the rule of honesty,

e) In cases where processing of personal data is carried out only on the basis of explicit consent, the relevant person may withdraw his/her consent,

f) Acceptance by the Company of the duly applied application made by the relevant person regarding the processing of personal data within the framework of his rights in paragraphs (e) and (f) of Article 11 of the Law,

g) In cases where the Company rejects the application made to it by the relevant person requesting the destruction of his personal data, his response is found insufficient, or he does not respond within the time period stipulated in the Law; Making a complaint to the Board and this request being approved by the Board,

h) Although the maximum period requiring personal data to be stored has passed, there are no conditions that would justify storing personal data for a longer period of time.

6- DESTRUCTION OF PERSONAL DATA

Destruction of personal data can be done in three different ways: deleting, destroying or anonymizing the data explained in detail below.

Relevant business units within the company, information systems and application owners containing the personal data in question, Internal Control, Compliance and Legal department and other persons or departments that may be relevant to the subject decide in writing on the method to be applied for the destruction of personal data, depending on the reason for this destruction. In accordance with this written decision, one of the destruction methods in Article G) of this Policy is applied in accordance with the Guide on Deletion, Destruction and Anonymization of Personal Data published by the Board. The Company also creates technical guides regarding the methods to be used for the storage and destruction of personal data and ensures their implementation.

Monitoring the destruction of personal data is the responsibility of the relevant data owner business unit within the Company. The data owner business unit receives support from different units of the Company for the destruction of the data, provided that the control is carried out by itself.

1. Erasure of Personal Data

Deletion of personal data processed wholly or partially by automatic means; It is the process of making the personal data in question inaccessible and unusable by the relevant users in any way.

In the process of deleting personal data that forms part of any data recording system and is processed by non-automatic means, the personal data to be subject to deletion is determined by taking into account the legal retention periods. In terms of access and authorization to personal data, the Company updates the role and authority matrices that the Company currently carries out on information systems and applications and identifies the relevant users. The authorities and methods of the relevant Users, such as access, retrieval and reuse, are determined in this context.

When the Company deletes personal data, it makes the data inaccessible or unusable in any way. In doing so, the company guarantees that the data is not accessible or reusable by any user.

2. Destruction of Personal Data

Destruction of personal data is the process of making personal data inaccessible, irretrievable and unusable by anyone.

Destruction will be carried out in cases where the Company processes data in physical recording environments, and the Company is obliged to make this data impossible to recover.

While this process is carried out for paper and microfiche media, the media will be destroyed by shredding or shredding machines by dividing it into small pieces of incomprehensible size that cannot be put back together. Additionally, the Company may receive destruction services from Third Parties in this context.

3. Anonymization of Personal Data

Anonymization is the process of making personal data impossible to associate with an identified or identifiable natural person, even if it is matched with other data, in cases where the Company processes personal data fully or partially by automatic means.

By removing or changing all direct and/or indirect identifiers in the relevant data set, the Company prevents the identification of the relevant person and ensures that he/she loses the feature of being distinguishable in a group or crowd in a way that cannot be associated with a natural person.

During anonymization of data, the Company may use methods such as one-way functions and encryption.

7- DESTRUCTION METHODS AND PROCESS OF PERSONAL DATA

For the destruction of personal data, the Company defines all methods that can be used during destruction in this Policy and its annexes. The data owner business unit is obliged to determine and apply the appropriate method in this Policy according to the appropriate situation.

During the destruction of personal data, the Company carries out the destruction by choosing the appropriate one of the following methods, according to the written decision it will make:

1. Overwriting

It is the process of making old data unreadable by writing random data consisting of 0s and 1s at least 7 times with software on magnetic media and rewritable optical media.

2. Magnetizing

It is the process of making the data on the magnetic media unreadable by physically changing it in a high magnetic field.

3. Physical Destruction

It is the process of physically destroying optical media or magnetic media by melting, pulverizing, grinding and similar processes. It can be applied in cases where magnetization or overwriting methods fail.

4. Cloud Destruction

It is the process of destroying all copies of the encryption keys of personal data after notification of the destruction of personal data held on cloud systems is made to the contracted service provider.

5. Destruction of Personal Data in Environmental Systems

It is the destruction process that must be carried out by overwriting, magnetizing or physical destruction on the internal unit, if available, or on the entire device, if not available, which contains personal data in systems such as printers, fingerprint units, door entry turnstiles. This type of destruction must be carried out before the devices are subject to backup, maintenance and similar operations.

8- STORAGE AND DISPOSAL PERIOD

1. Periodic Destruction and Legal Storage Periods

Physical and electronic data that have exceeded the legal retention and destruction periods are periodically destroyed. The Company destroys personal data in the first periodic destruction process following the date on which the obligation to destroy arises.

Periodic destruction is carried out at 6-month intervals for all personal data. Legal retention periods to be taken as basis during periodic destruction are determined in the Company's Personal Data Inventory (ANNEX-1). The destruction process is implemented during the first periodic destruction following the emergence of the obligation to destroy.

All transactions regarding destroyed personal data are recorded and these records are kept for 3 years.

2. Destruction Process if Requested by Data Owners

In cases where data owners apply to the Company and request the destruction of their personal data, the Company checks the current status of the conditions for processing personal data. As a result of this control;

- If it is understood that all the conditions for processing personal data are no longer valid, the personal data subject to the request will be destroyed within thirty days at the latest in accordance with the decisions and methods specified in this Policy and the relevant person will be informed.
- If it is understood that the conditions for processing personal data have been eliminated and the personal data subject to the request has been transferred to third parties, the Company notifies the relevant third party of this situation and ensures that the necessary actions are taken within the scope of the Regulation before the third party.
- If all the conditions for processing personal data have not been eliminated, the Company may reject the request by explaining the reason to the relevant data owner and notify the relevant person of the rejection response in writing or electronically within thirty days at the latest.

In order to meet and respond to requests from data owners, a Management Process for Requests and Complaints from Personal Data Owners is established within the Company.

AUTHORIZATION IN STORAGE AND DISPOSAL PROCESSES

The company's job descriptions and those responsible for storing and destroying personal data are as follows;

- GPDR Working Group: It decides on policies and methods by working with the relevant business units of the Company regarding the storage and destruction of personal data, ensures that the Policy and its annexes are kept up to date, and works closely with the relevant units of the Company when necessary to ensure that the Policy is carried out correctly and in accordance with the Law and Regulation.

- Internal Control, Compliance and Legal: It provides consultancy on legal issues regarding the storage and destruction of personal data, and provides the necessary information to the relevant business units in case of changes in the Law, Regulation and relevant legislation. Ensures that the Policy is implemented in accordance with the Law and Regulation.

- Information technologies: Ensures that the relevant destruction and storage processes are carried out in accordance with the Law and Regulation in the light of the decisions and methods specified in the Policy.

- Relevant business units of the Company: It expresses its opinions and justifications for determining the policies and methods regarding the storage and destruction of personal data and follows up the actions taken in accordance with this Policy.

9- CHANGES TO BE MADE IN THE POLICY

1. In case the Law, Regulation or other legislation is partially or completely changed, amended, updated or repealed, the Company will update and change the Policy to comply with the new Law, Regulation or legislation.

2. The Company will share the updated Policy with its employees via e-mail so that the changes made to the Policy can be reviewed and will make it accessible to its employees via the corporate intranet.