PERSONAL DATA RECORDING, MAINTAINING AND DESTRUCTION PROCEDURE

Version : 1

Issue date : 01.01.2020

1. INTRODUCTION

1.1. Purpose

Personal Data Maintaining, Recording and Destruction Procedure (the "**Procedure**") is issued in order to determine the methods and principles about the works and processes related with the maintaining and destruction activities which are performed by Öz-Ege Tütün Sanayi ve Ticaret Anonim Şirketi (Öz-Ege Tobacco Industry and Trade Joint Stock Company, the "**Company**")

The works and processes related with the recording, maintaining and destruction of the personal data are performed according to this procedure issued in line with this by the Company.

1.2. Scope

The personal data belonging to the company employees, employee candidates, service providers, suppliers, visitors, and the other third persons are in the scope of this procedure and this procedure is applied for all recording environments in which the personal data managed by the company are processed and the activities for processing personal data.

1.3 Abbreviations and definitions

Receiver group:	The real or legal person category to which the personal data is transferred by the data officer company.
Clear consent:	The consent depending on information and declared with free will related with a certain subject.
Making anonymous:	Making personal data such that it can't be correlated with a real person, the identity of who is known or can be known in any condition, even by matching with other data.
Employee:	The company personnel.
Electronic media:	The media in which the personal data can be created, read, changed, and written via electronic devices.
Un-electronic media:	All of the other media, such as written, printed, visual etc., other than electronic media.
Service provider:	The real or legal person providing service in the framework of a certain contract with the company.
Related person:	The real person whose personal data is to be processed.
Related user:	The persons who process the personal data in the organization of the data officer or according to the authority and directive he is granted by the data officer, excluding the person or department responsible for technically maintaining, preserving and backing up the data.
Destruction:	Deleting, destruction or making personal data anonymous.
Law:	The law on protection of the personal data no: 6698.
Recording media:	All kinds of media in which there are personal data processed, which are completely or partially automatic or through non-

	automatic ways provided that it is a part of any data recording system.
Personal data:	All kinds of information about a real person, the identity of whom is certain or can be found out.
Personal data processing inventory:	The inventory which the data officers create by correlating the personal data processing activities they conduct; the purposes and legal reason for personal data processing, data category, the receiver group to which it is transferred and the person group which is the subject of the data depending on the business processes and which they detail by stating the maximum maintaining term, necessary for the purposes for which the personal data is processed, the personal data anticipated to be send to foreign countries and the precautions taken related with data security.
Processing personal data:	All kinds of processes performed on the data such as obtaining, storing, maintaining, changing, rearranging, transferring, taking over, making obtainable, classifying, or preventing that the personal data is used through ways which are completely or partially completely automatic or, provided that it is a part of any data recording system, through non-automatic ways.
The Board:	Personal Data Protection Board.
Personal data with private nature:	The data of the people related with race, ethnical origin, political thought, philosophical belief, religion, sect or other beliefs, clothing, membership to society, foundation or trade union, health, sexual life, penal conviction, and security precautions and their genetic data.
Periodical destruction:	The deletion, destruction or making anonymous procedure to be performed ex officio, stated in the personal data maintaining and destruction policy and to be done with repeating intervals, in case that all of the personal data processing conditions, included in the law, disappears.
Procedure:	This Personal Data Recording, Maintaining and Destruction Procedure.
Data processor:	The real or legal person processing the personal data on behalf of the data officer, depending on the authority granted by the data officer.
Data recording system:	The recording system where personal data is structured and processed based on certain criteria.
Data officer:	The company responsible for establishing and managing the data recording system, which determines the personal data processing targets and means.
Data officers registry information system:	The information system, created and managed by the Personal Data Protection Board which the data officers shall use for applying to the Registry and the other procedures related with the Registry, which can be accessed over internet.
VERBİS:	Data Officers Registry Information System.
Regulation:	The regulation on deleting, destruction or making the personal data anonymous, published in the Official Paper dated: 28.10.2017.

2. DISTRIBUTION OF THE RESPONSIBILITIES AND TASKS

All departments and employees of the company actively support the departments in charge about taking technical and administrative precautions for applying the technical and administrative precautions, taken in the scope of the procedure by the departments in charge, as required, increasing, monitoring, and continuously supervising the training and

awareness of the employees of the department and prevention of personal data from illegally processing, prevention of personal data from illegal accessing, and ensuring that the personal data is maintained according to the laws.

Table 1: Personnel in charge and distribution of tasks

PERSONNEL	OFFICER	RESPONSIBILITY
Name-Surname Title	PDP committee officer	Supervising whether the work procedures of every department are performed according to the maintaining and periodical destruction intervals or not
Name-Surname Title	Contact person	Ensuring the compatibility of the procedures, within his duty, to the maintaining period and management of the personal data destruction procedure according to the periodical destruction period
Name-Surname Title	Information Technology Department Personal data maintaining and destruction policy application officer	Ensuring the compatibility of the procedures, within his duty, to the maintaining period and management of the personal data destruction procedure according to the periodical destruction period
Name-Surname Title	Accounting department Personal data maintaining and destruction policy application officer	Ensuring the compatibility of the procedures, within his duty, to the maintaining period and management of the personal data destruction procedure according to the periodical destruction period
Name-Surname Title	Operations department Personal data maintaining and destruction policy application officer	Ensuring the compatibility of the procedures, within his duty, to the maintaining period and management of the personal data destruction procedure according to the periodical destruction period
Name-Surname Title	Trade and finance department Personal data maintaining and destruction policy application officer	Ensuring the compatibility of the procedures, within his duty, to the maintaining period and management of the personal data destruction procedure according to the periodical destruction period

3. RECORDING MEDİA

The personal data is maintained securely according to the law in the media listed in the Table 2 by the company.

Table 2: Personal data maintaining media

Electronic media	Non-electronic media
▪ Servers (domain, backing up, e-mail, database, web, file sharing etc.) ▪ Software (office software and the other software used by the company) ▪ Information security devices (firewall, intrusion detection and prevention, daily log file, antivirus etc.) ▪ Personal computers (desktop, laptop) ▪ Mobile devices (telephone, tablet etc.) ▪ Optic discs (CD, DVD etc.) ▪ Removable memories (USB, memory card etc.) ▪ Printer, scanner, photocopy machine	▪ Paper ▪ Manual data recording systems (survey forms, visitor entrance book) ▪ Written, printed, visual media

4. DESCRIPTIONS ON MAINTAINING AND DESTRUCTION

The personal data belonging to the employees, employee candidates, visitors, suppliers, service providers, the other third persons, the employees of the institutions and organizations are maintained and destroyed according to the law. In this scope, the detailed description on maintaining and destruction is given in order below.

4.1. Description about maintaining

In the article 3 of the law, the notion of processing personal data is defined; in the article 4, it is stated that the personal data processed should be connected, limited and measurable with the purpose for which it is processed and maintained for the period anticipated in the related legislation or necessary for the purpose for which they are processed; and in the articles 5 and 6 the conditions for processing personal data are listed. Accordingly, the personal data is maintained for the period anticipated in the related legislation or necessary for the purpose for which they are processed in the framework of the company activities.

4.1.1. Personal health data

The personal data, belonging to the employees, collected and maintained by the company shall be processed only by workplace physician serving in the organization of the company and maintained in the private room and locked cabins belonging to the workplace physician.

In mandatory cases, the access to the cabin in which the health data in question are, shall be provided only by the contact person; the access of no other employee or officer to the data in question shall be in question and with the end of the work required to be done related with the usage of the data, the data in question shall be brought to the same place and maintained as locked in the same way.

4.1.2. The other personal data with private nature

The personal data with private nature, belonging to both the company employees and 3rd persons, shall be maintained in locked cabins, allocated specially for keeping the media, such as document, record etc., to which only the contact person can access and where only this data is, regardless of the purpose of the processing.

4.1.3. Legal reasons requiring maintaining

The personal data, processed in the framework of the activities of the company are maintained before the company as long as the term anticipated in the related legislation.

With this respect, the personal data:

- Law on Protection of Personal data no: 668,
- Turkish code of liabilities no: 6098,
- The law on organization and duties of the tobacco and alcohol market regulatory institution no: 4733 and the secondary legislation,
- The tax procedures law no: 213 and the other related tax legislation,
- Social insurances and general health insurance law no: 5510,
- The law on regulation of the publishing made in the internet environment and struggling against the crimes committed through these publishing no: 5651,
- Work health and safety law no: 6331,
- Labor law no: 4857,
- Turkish code of commerce no: 6102,
- The regulation related with the health and security precautions to be taken in the workplace buildings and annexes

is maintained as long as the maintaining terms anticipated in the framework of the other secondary regulations which are in effect according to these laws.

4.1.4. Processing targets requiring maintaining

The company maintains the personal data, she processes in the framework of her activities, according to the targets below:

- Conducting human resources processes,
- Conducting work health and safety processes,
- Performing export processes,
- Ensuring the monitoring of product safety and STP processes and fulfilling the conditions,
- Ensuring company security,
- Conducting information technology processes,
- Ensuring system access and security,
- Being able to do execute businesses and deeds as a result of the contracts and protocols signed,
- Being able to do customer reporting,
- Ensuring that legal obligations are fulfilled as required or necessitates by the legal regulations,
- Having contact with the real/legal persons who have business relationship with the company,
- Making legal reporting,
- Managing call center procedures,
- Fulfilling evidencing obligation as a proof in the legal discrepancies which may arise in the future.

4.2. Reasons requiring destruction

The personal data deleted, destroyed or ex officio deleted upon the request of the related person by the company in cases that

- The provisions of the related legislation, establishing the basis for processing are changed or annulled,
- The purpose requiring processing or maintaining disappears,

- The related person revokes the clear consent in cases where personal data processing is performed only with respect to the clear consent condition,
- The application done by the related person for deleting and destroying his personal data is accepted by the company in the framework of his rights as required by the article 11 of the law,
- A complaint is filed to the board and this request is considered as fit by the board in cases where the request of the related person for deleting, destroying or making the personal data anonymous by the related person is rejected, the answer given by him is considered as inadequate by the company or it is not responded in the term anticipated by the law,
- The maximum period requiring maintaining the personal data is exceeded and there isn't any condition which gives grounds for maintaining personal data for a longer period.

4.3. Issuing minute for the destruction

At the end of each destruction procedure, the related destruction procedure is recorded with a minute by the officer of the department performing the destruction process and PDP committee officer. The minute in question is kept in the body of the company for 5 years.

5. TECHNICAL AND ADMINISTRATIVE PRECAUTIONS

The technical and administrative precautions are taken in the scope of the personal data with private nature procedure created by the company and in the framework of the adequate precautions determined and announced by the Board for the personal data with private nature as required by the fourth paragraph of the article 6 and article 12 of the law for securely maintaining the personal data, prevention of illegal processing and accessing and destroying the personal data according to the law.

5.1. Technical precautions

The technical precautions taken related with the personal data she processes are listed below:

- With the penetration tests, the risks, threats, weakness and, if exists, holes for the information systems of the company are detected and necessary precautions are taken.
- Access to the information systems and authorization of the users are done with the access and authorization matrix through security policies over corporate active index.
- Network security and application security are ensured.
- A closed system network is used for personal data transfer through network.
- Key management is applied.
- Partial data masking precaution is applied.
- Updated anti-virus systems are used.
- Firewalls are used.
- The security of physical media, containing personal data, is ensured against external risks (fire, flooding etc.).
- The personal data is backed up and the security of personal data backed up is also ensured.
- The user account management and authority control system is applied and also they are monitored.
- Attack detection and prevention systems are used.
- Transferring personal data with private nature in flash memory, CD, DVD media is closed.
- It is ensured that security problems are reported as soon as possible.

- Hardware (the access control system enabling only authorized personnel entering the system room, 24/7 running monitoring system, ensuring physical security of side switches, consisting of the local area network, fire extinguishing system, air conditioning system etc.) and software (firewalls, attack prevention systems, network access control, systems preventing harmful software etc.) precautions are taken for ensuring information system security against environmental threats.
- Accesses to the storage areas where the personal data is are recorded and unsuitable accesses or access trials are kept under control.
- The company takes necessary precautions for making deleted personal data is inaccessible and reusable for the related users.
- The security holes are monitored and suitable security patches are loaded and information systems are kept updated.
- Strong passwords are used in the electronic environments where personal data is processed.
- Secure logging systems are used in the electronic environments where personal data is processed and the log records are saved such that there is no user intervention.
- Access to the personal data stored in the electronic environment is classified according to the access principles.
- Secure protocol (https) is used for accessing the internet page of the company and it is encrypted with SHA 256 bit RSA algorithm.
- If it is necessary to transfer personal data with private nature through e-mail, it is transferred as encrypted via the corporate e-mail address or using KEP account. If transfer is done between servers in different physical environment, the data transfer is performed by establishing VPN between the servers or through sFTP and/or data masking methods.

5.2 Administrative precautions

The administrative precautions taken by the company related with the personal data she processes are listed below:

- Trainings are provided at certain intervals for improving the quality of the employees, preventing personal data from illegally processing, preventing the personal data from accessing illegally, ensuring maintenance of the personal data, communication techniques, technical knowledge, skill and related other legislation.
- An authority matrix is formed for the employees.
- The personal data is decreased as much as possible.
- Confidentiality and personal data protection commitment letters are made signed by the employees about the activities conducted by the employee.
- The necessary provisions were added to the discipline regulation for applying against employees not following security policies and procedures.
- Before starting processing personal data, the obligation to inform related people is fulfilled by the company.
- The personal data processing inventory was prepared.
- The general policy on personal data processing and the procedures related with this topic were prepared and issued.
- Periodical and random audits are done in the company.
- A separate procedure was determined for the security of personal data with private nature
- Adequate security precautions are taken for the physical environments where personal data with private nature is processed, maintained and/or accessed, physical security is ensured and unauthorized access is prevented.
- If transfer in paper media is necessary, precautions necessary for risks like paper stolen, lost or seen by unauthorized people and the paper is sent in “secret” format.
- Information security trainings are provided to the employees.

6. PERSONAL DATA DESTRUCTION TECHNIQUES

At the end of the term anticipated in the related legislation or the maintaining period which is necessary for the purpose for which they are processed, the personal data is destroyed ex officio by the company or upon the application by the related person again according to the provisions of the related legislation with the techniques stated below.

6.1. Deleting personal data

The personal data is deleted with the methods given in the Table 3.

Table 3: Deleting personal data

Data recording media	Description
Personal data included in the servers	For the ones of the personal data placed in the servers, the term of which, requiring them to be maintained is ended, the deletion process is done by eliminating the authority to access by the system manager.
Personal data included in the electronic media	For the ones of the personal data placed in the electronic media, the term of which, requiring them to be maintained is ended, they are made inaccessible and unusable in any way for the other employees (the related users) by the database manager.
Personal data included in the physical media	The ones of the personal data placed in the physical media, the term of which, requiring them to be maintained is ended, are made inaccessible and unusable in any way for the other employees except the manager of the department to which the related document belongs, are kept in locked cabins in the archive and the keys of these cabins are kept only by the manager of the department responsible for the document archive.
Personal data present in the removable memory	The ones of the personal data placed in the flash based saving media, the term of which, requiring them to be maintained is ended, are encrypted and the access authority is granted only to the system manager by the system manager and kept in the secure media with encryption keys.

6.2. Destruction of the personal data

The personal data is destroyed with the methods given in the Table 4 by the company.

Table 4: Destruction of the personal data

Data recording media	Description
Personal data placed in the physical media	The ones of the personal data placed in the paper media, the term of which, requiring them to be maintained is ended, are

	destroyed irrevocably in the paper shredders.

6.3. Making personal data anonymous

Making personal data anonymous is making the personal data such that they can't be correlated to a real person, the identity of whom is known or can be found out in any way, even if they are matched with the other data.

For making the personal data anonymous, it is required that the personal data is made such that they can't be correlated to a real person, the identity of whom is known or can be found out in any way even by using the suitable techniques with respect to the recording media and related area of activity, like turning back and/or matching the data with other data by the data officer or third persons.

7. MAINTAINING AND DESTRUCTION TERMS

Related with the personal data processed by the company in the scope of her activities:

- The maintaining terms based on personal data related with all personal data in the scope of activities performed depending on the processes are included in the personal data processing inventory;
- The maintaining terms based on data categories in the VERBIS record,
- The maintaining terms based on process in the personal data recording, maintaining and destruction procedure.

On the maintaining terms in question, if required, updates are done by the company. The ex officio deletion, destruction or making anonymous procedure are performed by the people in charge stated in the article 2 of this Procedure for the personal data, the maintaining term of which is ended.

Table 5: Process based maintaining and destruction terms table

Process	Maintaining term	Destruction term
All kinds of HR forms and documents for the existing personnel	10 years after the end of the business relation	In the first periodical destruction term following the end of keeping term
Personnel personal files	10 years after the end of the business relation	In the first periodical destruction term following the end of keeping term
Recruitment	10 years after the end of the business relation	In the first periodical destruction term following the end of keeping term
Employee candidate resumes	1 year	In the first periodical destruction term following the end of keeping term
Payroll preparation	10 years after the end of the business relation	In the first periodical destruction term following the end of keeping term

Answering court/execution information requests related with the personnel	10 years after the end of the business relation	In the first periodical destruction term following the end of keeping term
Personnel private health and personal accident insurance policies	1 years	In the first periodical destruction term following the end of keeping term
Work health and safety application and training records	15 years after the end of the business relation	In the first periodical destruction term following the end of keeping term
Candidate supplier list	2 years	In the first periodical destruction term following the end of keeping term
Contracts signed with third persons	10 years after the termination of the contract	In the first periodical destruction term following the end of keeping term
Customer reports	5 years	In the first periodical destruction term following the end of keeping term
Laboratory analyses	3 years	In the first periodical destruction term following the end of keeping term
Record/Monitoring/Log systems	2 years	In the first periodical destruction term following the end of keeping term
Security camera videos	1 year from the date when the video is taken	In the first periodical destruction term following the end of keeping term
General assembly procedures	10 years	In the first periodical destruction term following the end of keeping term
Information of the shareholders and members of the board of directors of the company	10 years	In the first periodical destruction term following the end of keeping term
Payment procedures	10 years after the end of the business relation	In the first periodical destruction term following the end of keeping term
Information of the members of the board of directors and signature authorities of the company	10 years	In the first periodical destruction term following the end of keeping term

8. PERIODICAL DESTRUCTION TERM

The company has determined the periodical destruction term as six (6) months as required by the article 11 of the Regulation. Accordingly, the periodical destruction procedure is performed in months June and December every year before the company.

9. PUBLISHING AND KEEPING THE PROCEDURE

The procedure is published in two different media as with wet signature (printed paper) and in the electronic media, disclosed to the public in the internet page. The printed paper counterpart is kept in the file in the company.

10. UPDATING PERIOD OF THE PROCEDURE

The procedure is reviewed for the legislation changes and when required and the necessary parts are updated.

11. VALIDITY OF THE PROCEDURE AND REVOKE

The procedure was put into effect as of 01.01.2020.

In case that it is decided to revoke, the former copies of the procedure with wet signature are cancelled by the authorized bodies of the company and kept in the file for at least five (5) years by the company.