TURCAS PETROL ANONİM ŞİRKETİ

PERSONAL DATA RETENTION AND ERASURE POLICY

TURCAS PETROL ANONİM ŞİRKETİ

PERSONAL DATA RETENTION AND ERASURE POLICY

Name of Document
Turcas Petrol Anonim Şirketi Personal Data Retention and Erasure Policy

Version:
[0].[1]

Approved by:
Approved by Senior Management of Turcas Petrol A.Ş.

Date of Revision:
01/01/2021

TABLE OF CONTENTS

1. SECTION 1- INTRODUCTION

This Personal Data Retention and Erasure Policy ("**Erasure Policy**") has been prepared by Turcas Petrol Anonim Sirketi ("**Turcas**" or "**Company**") in accordance with article 7 of the Law on the Protection of Personal Data No. 6698 ("**Law**") and Regulation on Deletion, Destruction or Anonymization of Personal Data ("**Regulation**").

Objective of this Policy is to (i) determine durations in compliance with the Law and Regulation for the purpose storing and deleting personal data; (ii) provide information to employees and independent subcontractors about duration and conditions of storing personal data; (iii) store personal data in accordance with the Law and Regulation; and (iv) allow quick, easy and efficient access to personal data through determination of recording media, in case reasons of processing are no longer valid.

2. SECTION 2- ROLES AND RESPONSIBILITIES

The Company's Information Technologies Department is responsible for implementing this Erasure Policy in all operations, activities and processes of the Company and the Company's Legal Affairs Department and Human Resources Department will take a role in implementation of the procedures, guidelines, standards and training activities in the Company upon preparing them in accordance with the Erasure Policy. All employees of the Company, stakeholders and relevant third persons are required to comply with the Erasure Policy and collaborate with the Company's Information Technologies Department in connection with prevention of legal risks and imminent risks. All bodies and departments of the Company are obliged to oversee compliance with the Erasure Policy.

3. SECTION 3- PRINCIPLES OF THE POLICY

Pursuant to Article 7 of the Law, data controller deletes, destructs or anonymizes the personal data at its own discretion or upon request of the data subject in case reasons of processing are no longer valid even though processing is performed in accordance with provisions of the Law and other applicable laws.

Preparation of this Erasure Policy does not necessarily mean that personal data is stored, deleted, destroyed or anonymized in accordance with the Law and Regulation. The Company should oversee compliance with the Erasure Policy in accordance with the section "Roles and Responsibilities".

3.1. PURPOSE OF PREPARING PERSONAL DATA RETENTION AND ERASURE POLICY

This Erasure Policy explains the legal grounds for determination of maximum duration required for the purpose of processing of personal data that is stored by the Company and the processes of deletion, destruction and anonymization, for the purpose of ensuring the Company's ,i.e., data controller's, compliance with the deletion, destruction or anonymization of personal data upon request of the data subject in accordance with Article 7 of the Law and Regulation, when reasons of processing are no longer valid.

3.2. RECORDING MEDIA

Turcas performs data processing activities in the recording media detailed below:

- **Physical Records:** Physical records such as paper documents or hydrocarbon copies. The records in question contain physical items and meta data that describe physical items.
- **Electronic Records:** Electronic documents such as e-mail and electronic charts. The record contains electronic document and meta data that describe electronic document. Both document and meta data describing the document are kept in Exchange Server, File Server and LOGO application.

- **Application Records:** Electronic structural data records such as customer data. They consist of all data items including meta data that complement collective presentation of the structure, order and data items recorded (when all data items are converted into readable format), in a manner ensuring integrity of the record. Meta data for each type of record contain bibliographical, administrative data, audit and access data.

3.3. DEFINITIONS OF LEGAL AND TECHNICAL TERMS USED IN PERSONAL DATA RETENTION AND ERASURE POLICY

"Annex-1 Definitions" provide definitions of legal and technical terms used in the Erasure Policy.

3.4. INFORMATION ON LEGAL, TECHNICAL OR OTHER REASONS REQUIRING RETENTION AND ERASURE OF PERSONAL DATA

3.4.1. Reasons Requiring Retention of Personal Data

Reasons of storing personal data are specified in the Personal Data Processing Inventory.

3.4.2. Reasons Requiring Erasure of Personal Data

The Company destroys personal data at its own discretion in case reasons of processing are no longer valid even though processing is performed in accordance with the Law and provisions of the other applicable laws (for example, expiry of maximum duration for retention of personal data and absence of any condition that justifies longer storage of personal data).

In addition, in case data processing activity is performed solely based on explicit consent of data subject among other conditions for processing of personal data, the Company destroys personal data when the data subject revokes explicit consent or data subject requests deletion, destruction or anonymization of the personal data and such request is found acceptable or application of the data subject is rejected by the Company, response of the Company is found unsatisfactory by data subject or a complaint is filed to the Board and the application is accepted by the Board when response is not provided within the period of time specified in the Law.

3.5. TECHNICAL AND ADMINISTRATIVE MEASURES TAKEN TO ENSURE SECURE STORAGE OF PERSONAL DATA AND PREVENT UNLAWFUL PROCESSING OF AND ACCESS TO PERSONAL DATA

Technical Measures
- **Data loss/ leakage prevention (DLP): Security software is used to prevent, or report without preventing erroneous leakage of personal data or leakage of the data by ill-intentioned persons.**
- **Secure sockets layer (SSL): Certificates are used to ensure security and integrity of data flowing between server and client.**
- **In addition, products such as antivirus, antispam are used for regular scanning and detection of risks in the information system network and it is ensured that the entire structure is up-to-date in order to establish protection against malware.**
- **Password Management**
- **Monitoring of software inventory and performance of necessary updates**
- **Keeping LOGS at system level**
- **Leakage and security check operations are performed in detailed on annual basis. Vulnerabilities are eliminated based on risk and priority status.**

- **Disk Encryption Software is used.**
- **Mobile Device Management Software is used to ensure data security in Mobile devices.**

Administrative Measures

- **For the purpose of improving skills of employees, trainings are provided on prevention of illegal processing of personal data, prevention of unauthorized access to personal data, secure storage of personal data, communication techniques, technical information and skills, Law No. 657 and other applicable legislation.**
- **Employees are required to sign nondisclosure and confidentiality agreements in connection with activities performed by the Company.**
- **A discipline procedure has been prepared for employees who fail in complying with the security policy and procedures.**
- **The Company complies with its obligation to provide information before commencing data processing activity.**
- **Personal data processing inventory has been prepared.**
- **Periodical internal audits are conducted.**
- **Employees are provided data security training on annual basis.**

3.6. METHODS IMPLEMENTED AND TECHNICAL AND ADMINISTRATIVE MEASURES TAKEN FOR ERASURE OF PERSONAL DATA IN ACCORDANCE WITH THE LAW

The Company destroys personal data upon selection of one of the deletion, destruction or anonymization methods.

3.6.1. Methods for Deletion of Personal Data

Deletion of personal data means rendering personal data into a format that is not accessible or reusable by the relevant users. The Company utilizes technological resources and takes technical and administrative measures depending on the cost of implementation for the purpose of ensuring that deleted personal data cannot be accessed or reused by the relevant users. For this purpose, Turcas implements the following methods in order to ensure secure deletion of personal data:

a. Cloud Solutions of Application Type as a Service (Office 365, Salesforce, Dropbox)

A solution implemented over cloud systems was not deemed necessary as cloud structures are not used pursuant to CMB Legislation.

b. Office Files in Central Server

Data that are described as sensitive data in the data classification matrix and hosted in central servers are scanned within certain intervals and reports are issued to the data subjects. Data subjects are required to complete the necessary procedures in accordance with PDPL obligations.

c. Databases

Lines where personal data are available are deleted or anonymized manually or by using database commands. Attention is paid that the relevant user is not the same person as the database administrator during performance of the aforementioned activity.

3.6.2. Methods for Destruction of Personal Data

Destruction of personal data means rendering personal data into a format that is not accessible, recoverable or reusable by the relevant users. The Company utilizes technological resources and takes technical and administrative measures depending on the cost of implementation in connection with the destruction of personal data. For this purpose, Turcas implements the following methods in order to ensure secure destruction of personal data:

a. Local Systems

Demagnetization, physical destruction, overwriting methods are used.

b. Peripheral Systems

- Network devices (switch, router, etc.)
- Flash-based media
- Magnetic band
- Magnetic disk units
- Mobile phones
- Optical disks
- Peripheral units such as printer with removable data recording media, access systems with finger print reader
- Peripheral units such as printer with fixed data recording media, access systems with finger print reader
- Paper and microfiche
- Cloud

3.6.3. Methods for Anonymization of Personal Data

Anonymization of personal data is the process of removing personally identifiable information related with an identified or identifiable real person even when data are matched with the other data. Personal data will be anonymized only when they cannot be associated with an identifiable or identified real person even when suitable techniques are used in connection with the recording media and the relevant activity such as recovery of personal data by the Company, recipients or groups of recipients and matching the data with other data. The Company utilizes technological resources and takes technical and administrative measures depending on the cost of implementation in connection with anonymization of personal data. For this purpose, Turcas implements the following methods in order to ensure secure anonymization of personal data:

Anonymization methods that do not create value irregularity	• Removal of variables • Removal of records • Coding lower and upper limit • Geographical redaction • Sampling

Anonymization methods that create value irregularity	• Micro-Combining • Data Exchange • Noise Addition • Resampling
Statistical methods enhancing anonymization	• K-Anonymity • L-Diversity • T- Closeness

Endeavours are made to manually implement the methods in case it is feasible depending on the application received.

3.7. TITLES, DEPARTMENTS AND JOB DESCRIPTIONS OF EMPLOYEES TAKING A ROLE IN THE PROCESS OF RETAINING AND ERASING PERSONAL DATA

Title	**Department**	**Job Description**
CEO, Directors and All Department Managers	All Departments/ Units of the Company	They are responsible for ensuring compliance of the employees with the policy.
Human Resources Legal Affairs Information Technologies	All Departments/ Units in PDPL Board	They are responsible for preparation, improvement, implementation, publication and revision of the Policy.
Information Technologies Manager Senior System Support Specialist System Support Specialist	Information Technologies	They are responsible for proposing technical solutions required for implementation of the Policy.
All Department/ Unit Managers, Employees	All Departments/ Units	They are responsible for implementation of the Policy in parallel with their respective job descriptions.

ANNEX-1 DEFINITIONS

The terms used in this Policy refer to meanings provided below:

Explicit consent	Consent given with free will upon being informed about a certain
Recipient group	Category of real or legal persons to whom data controller transfers personal data
Anonymization	Process of removing personally identifiable information related with an identified or identifiable real person even when data are matched with the other data.
Data subject	A real person of whom personal data are processed;
Relevant User	Persons that process personal data within the organization of data controller or based on authorization or instructions of data controller, except for the person or unit that is responsible for technical storage, protection and backup of the data.
Erasure	Deletion, destruction or anonymization of personal data;
Law	Law on the Protection of the Personal Data No. 6698 of 24/3/2016.
Recording media	Any media containing personal data that are processed by fully or partially automatic means, or non-automatic means provided that it is a part of any data recording system.
Personal Data	Any information related with an identified or identifiable real person;
Personal data processing inventory	Inventory that provides detailed information on personal data processing activities performed by the Company in parallel with business processes; purposes for processing personal data, data categories, recipient group and maximum duration required for purposes for processing personal data as determined based on the data subject group and recipient group, personal data transferred to foreign countries and measures taken about data security.
Erasure Policy	Policy prepared by the Company as basis to deletion, destruction and anonymization as well as determination of maximum duration required for the purpose of processing personal data.
Processing of personal data	Any process performed on personal data such as obtaining personal data by fully or partially automatic means, or non-automatic means that are part of a data registration system; recording, storage, revision, modification, disclosure, transfer, taking the transfer of data, rendering the date obtainable, classification or prevention of use.
Board	Personal Data Protection Board
Authority	Personal Data Protection Authority
Periodic erasure	The process of deletion, destruction or anonymization implemented at own discretion within repetitive intervals and as specified in personal data retention and erasure policy in case conditions of processing personal data that are described in the Law are no longer valid.
Data processor	A real or legal person that processes personal data for and on behalf of the data controller based on the authorization made by the data controller.
VERBIS	Data Controllers Registry

Data recording system	Recording system where personal data are entered upon configuration based on certain criteria.
Data controller	Real or legal person who determines purposes and means of processing personal data, and assumes responsibility for establishing and managing data recording system.

ANNEX-2 STORAGE AND PERIODICAL DESTRUCTION DURATIONS

Category of Personal Data	**Maximum Duration of Storage**
Financial Information	10 years upon expiry of the calendar year in which last record is entered into commercial books or accounting documents are created 10 years upon termination of business relationship
Contact Information	10 years upon termination of employment agreement or contractual relationship
Identification Information	10 years upon termination of business relationship
Training Information/ Performance and Career Development Information- Professional Experience (VERBIS)	10 years upon termination of employment agreement
Legal Action and Compliance Information	10 years upon termination of contractual relationship 10 years upon completion of litigation process
Customer Information/ Inquiry-Complaint Information- Customer Transactions	3 years upon creation of the record in case of not leading to sales 10 years following the date of purchase order 10 years upon processing of inquiry and complaint 10 years upon expiry of the agreement term
Personal Information	10 years upon termination of employment agreement
Video Audio Information	10 years upon processing of inquiry and complaint 10 years upon completion of litigation process
Employee Transaction Information- Transaction Security Information (VERBIS)	10 years upon termination of employment agreement 10 years upon completion of litigation process
Health Information	10 years upon termination of employment agreement
Prospective Employee Information- Recruitment and Interview Evaluation Information (VERBIS)	2 years following rejection of application
Criminal Convictions and Security Measures	10 years upon termination of employment agreement

Information on Family Members and Relatives	10 years upon termination of employment agreement
Vehicle Information	2 years
Security Information About Physical Spaces	10 years upon completion of litigation process
Audit and Inspection Information	2 years
Risk Management	6 months

Maximum and minimum durations of storing personal data are specified in Personal Data Inventory. The Company destroys personal data in the first periodic erasure process following the date on which obligation to destroy personal data arises. Accordingly, the Company destroys personal data within intervals of 6 months once the obligation to destroy personal data arises. Under no circumstances, the duration in question exceeds maximum periodic erasure duration specified in the Regulation.