

ARKAS PETROL ÜRÜNLERİ VE TİCARET A.Ş.
POLICY OF PROCESSING AND PROTECTING SPECIAL CATEGORIES OF PERSONAL DATA
6.11.2019 / Version No: 1

TABLE OF CONTENTS

- 1. Purpose**
- 2. Definitions**
- 3. Scope**
- 4. Principles Regarding the Measures to be Taken when Processing Special Categories of Personal Data**
- 5. Other Safety Measures**
- 6. Other Legal Regulations**
- 7. Notification of Breach**
- 8. Application**
- 9. Storing the Policy**

ARKAS PETROL ÜRÜNLERİ VE TİCARET A.Ş.
POLICY OF PROCESSING AND PROTECTING SPECIAL CATEGORIES OF PERSONAL DATA
6.11.2019 / Version No: 1

1. Purpose

This Policy of Processing and Protecting Special Categories of Personal Data (Policy) regulates the principles set by our company to ensure compliance with the applicable legislation regarding the measures to be taken when processing special categories of personal data.

2. Definitions

The terms used in this Policy shall have the meanings stated below. Definitions not included herein shall be used as defined in the Law and regulations.

Two-stage Authentication	Two stage authentication system that uses the combination of the username and password of the person as well as an external authentication system (mobile phone, personal question, cryptographic key, etc.).
Registered E-mail address (REM)	Electronic mail address which provides legal evidence regarding the use of electronic messages, including their transmission and delivery.
The Law	Personal Data Protection Law No. 6698.
Personal Data	Any information related to an identified or identifiable natural person.
Processing of Personal Data	Refers to any operation which is performed on personal data, wholly or partially by automated means or non-automated means which provided that form part of a data filing system, such as collection, recording, storage, protection, alteration, adaptation, disclosure, transfer, retrieval, making available for collection, categorization, preventing the use thereof.
Special Categories of Personal Data (SCPD)	Refers to personal data relating to the race, ethnic origin, political opinion, philosophical belief, religion, religious sect or other belief, appearance, membership to associations, foundations or trade-unions, data concerning health, sexual life, criminal convictions and security measures, and the biometric and genetic data.
SFTP	A file transfer protocol that transfers files by using the cryptographic network protocol SSH.
Virtual Private Network (VPN)	A type of connection that enables data exchange over a virtual network extension as if it is physically connected to a private network over the Internet or another open network.

ARKAS PETROL ÜRÜNLERİ VE TİCARET A.Ş.
POLICY OF PROCESSING AND PROTECTING SPECIAL CATEGORIES OF PERSONAL DATA
6.11.2019 / Version No: 1

Leak Testing	Operations and attempts to infiltrate information systems by trying every possible scenario.
<i>Secure vault</i>	Software area created to protect unmovable valuable data against reading, modifying and moving.
The Company	Refers to the Data Controller.
End-to-End Encryption	Encryption methods that enable only the sender and the receiver to read the messages by encrypting the sent message.
Data Controller	Means the 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.
Data Controllers' Data Subject (DCCP)	It refers to the natural person assigned and notified during registry by the data inventory responsible for natural and legal entities established in Turkey and by the data controller's representative for real and legal entities not established in Turkey in order to ensure communication with the Authority in relation to the obligations under the Law and secondary regulations to be issued based on this Law.
Data Inventory Responsible	Refers to the employee appointed by the Data Controller that creates the personal data inventory of the Company in accordance with the Law, keeps it up to date and communicates the necessary changes to the Data Controllers' Contact Person.
Authorization Matrix	A matrix that indicates whether users in systems where personal data are present are authorized or not to access, create records, display and modify personal data.

3. Scope

Pursuant to Article 12 of the Law, as a data controller, the Company is obliged to take all kinds of technical and administrative measures to protect personal data, to prevent unauthorized access and processing of personal data in violation of the Law and to determine the appropriate security level.

Additionally, in accordance with the Decision of the Personal Data Protection Board (Board) dated 31/01/2018 and numbered 2018/10 regarding "Adequate Measures to be Taken by Data Controllers when Processing Special Categories of Personal Data" (decision on special categories of personal data), the scope and duration of the authorization of the users who are authorized to access personal data should be clearly defined.

ARKAS PETROL ÜRÜNLERİ VE TİCARET A.Ş.

POLICY OF PROCESSING AND PROTECTING SPECIAL CATEGORIES OF PERSONAL DATA

6.11.2019 / Version No: 1

This Policy covers the regulations regarding the measures to be taken by the Company when processing special categories of personal data pursuant to the Law and the principle decision on processing special categories of personal data.

4. Principles Regarding the Measures to be Taken when Processing Special Categories of Personal Data

- 4.1. Electronic and physical environments in which special categories of personal data are processed, stored and/or accessed are specified in the inventory. Special categories of personal data are classified as high-risk personal data.
- 4.2. Access to special categories of personal data is limited to the Company employees and the sub-contractors' employees. Special categories of personal data access shall never be granted to service providers or employees outside the Company except in cases where the legal obligations stipulated by the laws are fulfilled.
- 4.3. It is obligatory for the Company's employees to sign "Information Systems General Standards and Security Policy" to ensure the confidentiality of special categories of personal data and to receive a training determined by the Company on the Law, secondary legislation and the security of special categories of personal data. The company organizes activities regarding the protection of personal data in order to increase the awareness of the employees.
- 4.4. The company published the following policies "Personal Data Protection and Processing Policy" and "Personal Data Retention and Destruction Policy" that include principles to be applied by all employees regarding the confidentiality of special categories of personal data. This policy, however, is the main policy to be followed regarding the confidentiality of special categories of personal data.
- 4.5. For special categories of personal data stored in the electronic environment,
 - 4.5.1. A data recording system is used that utilizes cryptographic encryption methods or that has a cryptographic encryption system to be used in recording environments where special categories of personal data are recorded.
 - 4.5.2. Email systems containing End-to-End Encryption protection at the least are used or installed as encryption methods to be used in transfers of special categories of personal data.
 - 4.5.3. Cryptographic keys are kept in a *secure vault*.
 - 4.5.4. The transaction records of the data movements are logged, signed with a timestamp, and stored by applying access controls in a secure environment.
 - 4.5.5. Safety updates published by manufacturers are applied to data systems.
 - 4.5.6. Safety tests of the environments where the data are available are performed once a year and the test results are recorded.
 - 4.5.7. Access authorization control methods are applied to access the data. These methods are applied as per the "Information Systems Access Control Management Policy".
- 4.6. For SCPD processed, stored and/or accessed in physical environment,

ARKAS PETROL ÜRÜNLERİ VE TİCARET A.Ş.

POLICY OF PROCESSING AND PROTECTING SPECIAL CATEGORIES OF PERSONAL DATA

6.11.2019 / Version No: 1

- 4.6.1. Environments where special categories of personal data are present and their requirements are determined in the personal data inventory by each department.
- 4.6.2. It is important to ensure that necessary measures are taken according to the nature of the environment where special categories of personal data are present.
- 4.6.3. The Company puts "Crisis Response Procedure" into effect to any legal obligations that may arise in case of any data breaches and to act in accordance with the regulations in this regard.
- 4.6.4. In order to ensure the security of the physical environments where special categories of personal data are present, all entrances and exits to these areas are monitored and kept under control with additional security methods such as entrance/exit card system, encrypted system, locking, etc. and unauthorized entrances and exits to these areas are prevented.
- 4.7. When transferring special categories of personal data, the transfer modes and methods below are applied. The transfer is made only by employees that are authorized to transfer special categories of personal data.

Mode of Transfer	Method of Transfer
E-mail transfer	An encrypted corporate e-mail address or a Registered E-mail (REM) account is used.
Transfer via media such as flash memory, CD, DVD	Cryptographic methods are encrypted and the cryptographic key is kept in different media
Transfer between servers in different physical environments	Data transfer is performed by installing a VPN between servers or by the SFTP method.
Transfer via paper media	The determined measures against risks such as theft, loss of documents or access by unauthorized persons shall be taken and the document shall be sent to the receiver as "STRICTLY CONFIDENTIAL".

- 4.8. All authorizations given to the employees regarding special categories of personal data (including access and, if applicable, transfer authorization) shall be removed as of the termination of their duties. In this context, records are kept indicating that access has been terminated, authorizations have been removed, documents kept in physical environment have been delivered to the authorities and all items in the company inventory given to the use of these persons are returned.

5. Other Safety Measures

ARKAS PETROL ÜRÜNLERİ VE TİCARET A.Ş.
POLICY OF PROCESSING AND PROTECTING SPECIAL CATEGORIES OF PERSONAL DATA
6.11.2019 / Version No: 1

Other security measures to be taken are determined in "Information Systems General Standards and Security Policy" and "Personal Data Retention and Destruction Policy".

6. Other Legal Regulations

Additionally, for the implementation of this Policy, industry practices, professional rules, and other regulations are also taken into account, especially the technical and administrative measures to ensure the appropriate level of security specified in the Personal Data Security Guide published on the website of the Personal Data Protection Authority (Authority).

Within the scope of this Policy, the Company regularly performs the necessary audits or has them performed in order to ensure compliance with the Law and the principle decision on special categories of personal data.

7. Notification of Breach

In case of any data breach including special categories of personal data, the "Crisis Response Procedure" is applied.

Pursuant to the Article 12 of the Law, the company is obliged to notify the data subject and the Board within 72 hours if the processed personal data are illegally obtained by third parties.

8. Application

8.1. Publishing: This Policy will be provided to employees by the Data Controller.

8.2. Effective Date: This Policy shall enter into force on release.

8.3. Amendments: Prior to any changes to this Policy, the Data Controllers' Contact Person or Data Inventory Responsible may request the changes to be applied from the Data Controller. Policy changes are made by the Data Controller.

9. Storing the Policy

The Data Controller is responsible for publishing and storing this Policy. Each department manager is responsible for the implementation of this Policy. Questions related to the implementation of this Policy should be directed to the Data Controller's Contact Person and the Data Inventory Responsible.