A D C O PETROL KATKILARI SANAYİ VE TİCARET ANONİM ŞİRKETİ

THE POLICY ON THE PROCESSING AND PROTECTION OF PERSONAL DATA

1 – PURPOSE OF THE POLICY

A D C O PETROL KATKILARI SANAYİ VE TİCARET ANONİM ŞİRKETİ ("A D C O" or "COMPANY"), is committed to complying with the legal regulations of the Constitution of the Republic of Turkey, the Law on the Protection of Personal Data No. 6698 ("LPPD") and other legislation regarding the protection of personal data, and to protecting the rights and freedoms of the persons whose data is processed by A D C O. For this purpose, as the Data Controller, this Policy on the Processing and Protection of Personal Data ("Policy") has been prepared to explain the processes regarding personal data processing activity and personal data protection conducted by our Company, ensure transparency and legality in all activities, to inform the data owner natural persons whose personal data is processed by our Company, and to develop in line with new legal regulations.

The right to the Protection of Personal Data is stated in **ARTICLE 20 of the Constitution of the Republic of Turkey** as follows:

"Everyone has the right to demand respect for his/her private and family life. Privacy of private or family life shall not be violated. (Sentence repealed on May 3, 2001; Act No. 4709) Everyone has the right to request the protection of his/her personal data. This right includes being informed of, having access to, and requesting the correction and deletion of his/her personal data, and to be informed whether these are used 29 in consistency with envisaged objectives. Personal data can be processed only in cases envisaged by law or by the person's explicit consent. The principles and procedures regarding the protection of personal data shall be laid down in law."

The Law on the Protection of Personal Data No. 6698, which aims to protect the fundamental rights and freedoms of individuals during the processing of personal data, was submitted to the Presidency of the Grand National Assembly of Turkey on January 18, 2016, with various amendments made to the previous texts and was accepted by the General Assembly of the Grand National Assembly of Turkey on March 24, 2016, and became law. It entered into force upon publication in the Official Gazette dated April 7, 2016, and numbered 29677.

In Article 12, paragraph (1) of the Law on the Protection of Personal Data No. 6698 (Law), it is stipulated that the Data Controller is obliged to take all necessary technical and organizational measures to provide an appropriate level of security for the purposes of:

- ✓ preventing unlawful processing of personal data,
- ✓ preventing unlawful access to personal data,
- ✓ ensuring the protection of personal data.

In paragraph (5), it is stipulated that in case the data processed are obtained by others by unlawful means, the data controller shall communicate the breach to the data subject and notify the Personal Data Protection Board ("Board") within the shortest time. Where necessary, the Board may announce such breach at its official website or through any other way it deems appropriate.

In the scope of the LPPD No. 6698, as the Data Controller, this Policy has been prepared to explain the processes regarding personal data processing activity and personal data protection conducted by our Company, ensure transparency and legality in all activities, inform the data owner natural persons whose personal data is processed by our Company.

This Policy establishes the principles for the legal protection and processing of personal data of our employees, job candidates, interns, potential customers, employees of our customers, authorities and employees of suppliers of goods/services, our visitors, our shareholders, employees and shareholders of institutions we cooperate with, authorities, solution partners, consultants who have business relations with the Company, and other third parties.

With this Policy, the Company makes the Protection of Personal Data, which is a constitutional right, a Company Policy and undertakes to comply with the Personal Data Protection Law and legislation and regulations within the scope of its legal and social responsibility. The PDP Policy aims to create awareness about the legal processing and protection of personal data within the Company and to establish a sustainable and auditable system to ensure compliance with the legislation in all processes.

In order to implement the Law on the Protection of Personal Data and additional legislation, the necessary policies and procedures are determined within the Company, disclosure texts are created, explicit consents are applied, confidentiality agreements are made, job descriptions are revised, administrative and technical security measures in accordance with the legislation are taken by our Company to protect personal data, and necessary audits are carried out within this scope.

2- DEFINITIONS

Some definitions used in the Law on the Protection of Personal Data and the Company's Policy on the Protection and Processing of Personal Data are explained below:

Processing of Personal Data: Any operation which is performed on personal data, wholly or partially by automated means or non-automated means 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.

Data Subject: Employees, employee candidates, interns, shareholders/partners, supplier employees and officials, potential product or service buyer employees and product or service buyer employees, solution partner natural persons, visitors, persons shown as references, and other third-party natural persons within the scope of the contract made with the Company, whose personal data is processed.

Personal Data: Any information relating to an identified or identifiable natural person.

For example, first name&last name, Republic of Turkey ID number e-mail, address, business address, date of birth, place of birth, credit card number, driver's license number, bank account number, passport number, license number, diploma, etc.

Sensitive Personal Data: Data related to race, ethnic origin, political opinion, philosophical belief, religion, sect or other belief, appearance, membership to associations, foundations, or unions, health, sexual life, criminal conviction, data regarding security measures, as well as biometric and genetic data.

Data Controller: 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 filing system, where data is systematically processed and stored.

Data Processor: The natural or legal person who processes personal data on behalf of the data controller upon its authorization.

Explicit Consent: Freely given, specific, and informed consent about a certain subject.

Erasure of Personal Data: The process of making personal data inaccessible and non-reusable for the relevant users in any way.

Destruction of Personal Data: The process of making personal data inaccessible, irreversible, and non-

reusable by anyone.

Anonymization: Rendering personal data impossible to link with an identified or identifiable natural person, even through matching them with other data.

LPPD: The Law on the Protection of Personal Data published in the Official Gazette dated April 7, 2016, numbered 29677.

PDP Board: Personal Data Protection Board

Personal Data Storage and Destruction Policy: The Company's "Personal Data Storage and Destruction Policy", created to determine the maximum period required for the purpose for which personal data is processed by the Company and for the deletion, destruction, and anonymization process in accordance with the Regulation on the Erasure, Destruction, and Anonymization of Personal Data.

Data Controller's Registry: The Data Controllers Registry, kept under the supervision of the Personal Data Protection Board and is open to the public.

Communiqué on the Procedures and Principles of Application to the Data Controller: Communiqué on the Procedures and Principles of Application to the Data Controller, entered into force upon being published in the Official Gazette dated March 10, 2018, numbered 30356.

2-GENERAL PRINCIPLES ON THE PROCESSING AND PROTECTION OF PERSONAL DATA

2.1. Personal data shall only be protected and processed in compliance with procedures and principles laid down in LPPD and other relevant legislation.

2.2. This Policy establishes the principles for the legal protection and processing of personal data of our employees, job candidates, interns, shareholders, potential product/service buyer employees, product/service buyer employees, supplier employees, visitors, referenced persons, consultants who have a contractual and business relationship with our Company, and other third parties, and the processing and protection of sensitive data by our Company within the principles specified in the legislation.

2.3. Personal data shall not be processed, transferred to another person/system, used, and provided without explicit consent of the Data Subject. The individual's explicit consent is obtained in a clear, informed and free-willed manner.

2.4. Personal data shall be stored in the departments and systems determined by the Company. Processing, access to and use of personal data shall be carried out only by persons authorized by the Personal Data Protection Officer.

2.5. The protection of personal data is a constitutional right and is among the priorities of our Company. For this purpose, a "Personal Data Protection Officer" has been appointed within the Company to manage personal data protection processes and monitor and analyze developments.

2.6. In order to implement the principles laid out in this Policy, the necessary procedures are determined within the Company, disclosure texts are created, confidentiality agreements are made, job descriptions are revised, and all administrative and technical security measures required to protect personal data are taken.

2.7. All Company employees are personally responsible for the protection and security of personal data. Periodic audits shall be carried out to check compliance with the LPPD, other related legal regulations, and this Policy.

2.8. This Policy, which enters into force on the date it is prepared and released by the Company, is published on the Company's website and made available to the relevant persons upon the request of Personal Data Owners. The Company reserves the right to make changes to the Policy in line with legal regulations. The current version of the Policy is available on the Company's website.

2.9. The sanctions specified in Articles 135-140 of the Turkish Penal Code (TCK) shall be applied to those who record, share and/or fail to delete personal data when necessary, in violation of the principles outlined in this policy and legal regulations.

3. GENERAL PRINCIPLES ON THE PROCESSING OF PERSONAL DATA

The Company processes Personal Data in accordance with the procedures and principles stipulated in the Law and this Policy. While processing Personal Data, the Company acts in accordance with the following principles within the scope of Article 4 of the LPPD:

- ***Personal data is processed in accordance with the law and the rules of integrity:*** The Company acts in accordance with the laws, secondary regulations and general principles of law in the processing of your personal data, attaches importance to processing personal data limited to the purpose of processing and taking into account the reasonable expectations of data owners.
- ***Personal data is accurate and up-to-date:*** The Company ensures that your personal data is kept up-to-date through regular checks and updates. In this context, data owners are granted the right to request correction or deletion of their inaccurate and out-of-date data.
- ***Personal data is processed for specific, clear, and legitimate purposes:*** The Company determines the purposes of data processing before each personal data processing activity and takes care that these purposes are not unlawful.
- ***Personal data is related, limited, and proportionate to the purpose for which it is processed:*** The Company limits its data processing activity to the personal data necessary to achieve the purpose of collection, and takes the necessary steps to ensure that personal data that is not related to this purpose is not processed.
- ***Personal data is stored for the period required by the legislation or the processing purposes:*** Personal data is erased, destroyed, or anonymized after the purpose of processing personal data by the Company ceases to exist or after the period stipulated in the legislation expires.

4.ISSUES REGARDING THE PROCESSING OF PERSONAL DATA

4.1-CONDITIONS FOR PROCESSING PERSONAL DATA

Personal data is processed within the scope of the personal data processing conditions specified in Articles 5 and 6 of the Law. If the processing activity carried out for the aforementioned purposes does not meet any of the conditions stipulated under the Law, the Company obtains explicit consent for the relevant processing process. Within the framework of the regulation in the first paragraph of Article 5 of the Law, which states that *"Personal data shall not be processed without explicit consent of the data subject"*, our Company processes personal data in the presence of explicit consent, except for the exceptional cases recognized by the Law.

Per Article 5 of the LPPD, personal data may be processed without seeking the explicit consent of the data subject only in cases where one of the following conditions is met:

- ***It is expressly provided for by the laws:*** This data processing condition will be deemed to be fulfilled if there is a clear legal provision regarding the processing of the data owner's personal data.
- ***There is an inability to obtain the explicit consent of the data subject due to actual impossibility:*** If the data subject is unable to give explicit consent due to actual impossibility or if the consent is not legally valid, the personal data of the data subject may be processed if it is necessary to protect the life or physical integrity of the data subject or another person.
- ***It is directly related to the establishment or performance of the contract:*** This condition will be deemed to be fulfilled if the processing of personal data is necessary, provided that it is directly

related to the establishment or performance of a contract to which the data owner is a party.

- ***It is necessary for compliance with a legal obligation:*** Personal data may be processed if processing personal data is necessary for the Company, which is the data controller, to fulfill its legal obligations.
- ***Personal data have been made public by the data subject himself/herself:*** If the data owner has made his/her personal data public, the relevant personal data may be processed limited to the purpose of making it public.
- ***Data processing is necessary for the establishment, exercise, or protection of any right:*** If data processing is necessary for the establishment, exercise, or protection of a right, the data subject's personal data may be processed.
- ***Data processing is necessary for the legitimate interests pursued by the data controller:*** If data processing is necessary for the legitimate interests pursued by the Company, the data subject's personal data may be processed, provided that this processing shall not violate the fundamental rights and freedoms of the data subject.

4.2- CONDITIONS FOR PROCESSING SENSITIVE PERSONAL DATA

Sensitive personal data is processed by the Company in accordance with the principles set forth in this Policy, by taking all necessary administrative and technical measures and in the presence of the following conditions. In order to process sensitive personal data, it is mandatory to obtain the explicit consent of the data owner, other than the exceptions set forth in Article 6 of the Law below.

***Sensitive personal data excluding those concerning health or sexual life of the data owner*:** Such data may be processed without the explicit consent of the data subject, provided that there is an express provision in the law regarding the processing of such personal data.

Sensitive personal data regarding the health and sexual life of the data owner: It is for the protection of public health, preventive medicine, medical diagnosis, treatment and care services, planning and management of health services and their financing, and such data can be processed by persons or authorized institutions and organizations under the obligation of confidentiality without obtaining explicit consent. Otherwise, the data owner's explicit consent will be obtained to process such special personal data.

5. CONDITIONS FOR PROTECTING PERSONAL DATA

In accordance with Article 12 of the Law, our Company takes all necessary administrative and technical measures according to the nature of the data to be protected to prevent unlawful disclosure, access, transfer, or other security deficiencies that may occur in personal data. Administrative and technical measures are detailed in Article 13 of this Protocol titled "Ensuring the Confidentiality and Security of Personal Data".

Protection of Sensitive Personal Data

Our company attaches special importance to the protection of sensitive personal data determined as "Sensitive" within the scope of the LPPD and processed in accordance with the law. In Article 6 of the LPPD, some personal data that carry the risk of causing victimization or discrimination to individuals when processed unlawfully are determined as "sensitive", and care must be taken when processing this data.

The LPPD attaches special importance to certain personal data due to the risk of causing victimization or discrimination to individuals when processed unlawfully. These data are those 'related to race, ethnic origin, political opinion, philosophical belief, religion, sect or other beliefs, appearance, membership to associations, foundations, or unions, health, sexual life, criminal conviction, security measures, and biometric and genetic data'.

Our Company acts sensitively to protect the personal data determined as "sensitive" by the LPPD and processed in accordance with the law. In this context, the technical and administrative measures taken by the Company to protect personal data are implemented meticulously and specifically in terms of sensitive personal data.

Within the scope of Sensitive Data, documents containing health information such as criminal record certificates, blood type, and health reports are included in the employee personnel files within the Company. Periodic confidentiality training is provided to personnel authorized to access this sensitive personal data, the scope and duration of access authorization are determined, periodic audits are conducted, and confidentiality agreements are signed. If the relevant personnel leaves the job, the access authorization is immediately revoked.

The physical files containing personal health data stored physically in employees' personnel files are kept in locked areas and accessible only to authorized employees and administrative affairs employees authorized within the scope of personnel files.

6. CATEGORIZATION OF PERSONAL DATA PROCESSED BY THE COMPANY AND PURPOSES OF PROCESSING

6.1- Personal Data Categories and Descriptions:

The categories of personal data processed by the Company within the framework of the purposes and conditions specified in the LPPD and this Policy, and the explanations of the categories are given below:

Identity Data	**:**	First name, last name, date of birth, country of birth, city of birth, gender, marital status, nationality, information on the Turkish identity card (Republic of Turkey Identity Number, serial number, wallet number and sequence number, volume number, registration number, province/district/village/neighbourhood where registered, place of issue, reason for issue, date of issue), tax number, SSI number, signature information, photograph, driver's license, passport, foreign identity number, etc.
Contact Data	**:**	Address, telephone number, e-mail address, mobile phone number, corporate e-mail address, registered e-mail address, internal company communication information, extension phone number, fax number, etc.
Location Data	**:**	Location data (when company vehicles are used)
Customer Transactions	**:**	Identity and billing information required to issue an invoice, order forms, written offers, contracts, e-mails, etc.
Legal Transactions	**:**	Seizure notice/salary deduction information, correspondence with judicial authorities, file and debt information regarding employee enforcement proceedings files, power of attorney, determination and follow-up of legal receivables and rights, and data processed within the scope of legal obligations.
Sensitive Personal Data	**:**	Data specified in Article 6 of the PPD Law (health data of employees, including blood type, criminal record)
Finance	**:**	Financial data and salary details, payrolls, premium entitlements, premium amounts, personal data processed regarding information, documents and records showing all kinds of financial results, bank account number, IBAN, contract information, financial profile-performance information, asset data, title deed and asset information, income information, balance sheet information.

Physical Space Security	**:**	Security footage
Transaction Safety	**:**	IP address information, key and password information.
Personnel Information	**:**	Registry number, position name, department and unit, title, previous titles, last employment date, start and end dates of employment, insurance start date/retirement allocation number, social security number, tax number, total monthly working hours, permission documents, start and end dates of vacation, photograph and signature, current resume, resigning personnel release form, personnel liabilities information, employee employment contract and job descriptions, statement and warning documents, releases, minutes, name and surname of dependents, name, surname and T.R. Identity Number of spouse and children, gender, date of birth, minimum living allowance (AGİ) Certificate, telephone number of employee's relatives.
Work Experience	**:**	Certificate, diploma and mastery information, foreign language information, education and skills, courses taken, seminars attended, places of employment, profession, previous titles-positions, information in current CV, license, level information-certificates for computer programs, skills, reference information (Reference persons' name/surname, mobile phone, company phone, company name, position, e-mail address)
Health Data	**:**	Blood type, personal health data
Visual and Audio Data	**:**	Photograph and security footage data (except for the recordings in the scope of Physical Space Security Data)
Criminal Conviction and Security Measures	**:**	Personal data regarding the receipt and evaluation of any requests or complaints to the Company, criminal records

6.2-Purposes of Processing Personal Data:

All your personal data, including your sensitive personal data, can be processed by the Company, including but not limited to those listed under the heading of data categories above, in a proportionate manner in connection with the data categories and in accordance with the purposes set forth in this Policy and by determining the legal reasons set forth in Articles 5 and 6 of the Law. In the Disclosure Texts, your processed personal data is included separately on the basis of each data category by matching it with the purpose and legal reasons for processing.

All kinds of personal data obtained by the Company and included in this section (including, but not limited to sensitive personal data) may be processed in accordance with the law and the purpose of the Law, provided that it is not limited to the following purposes of the Company:

1. Execution of Emergency Management Processes
2. Execution of Information Security Processes
3. Execution of Candidate Employee/Intern/Student Selection and Placement Processes
4. Execution of Candidate Employee Application Processes
5. Fulfilment of Employment Contract and Legislative Obligations for Employees
6. Execution of Side Rights and Benefits Processes for Employees
7. Execution of Audit/Ethics Activities
8. Execution of Access Authorizations

9. Execution of Activities in Accordance with Legislation
10. Execution of Finance and Accounting Affairs
11. Ensuring Physical Space Security
12. Execution of Assignment Processes
13. Follow-up and Execution of Legal Affairs
14. Execution of Internal Audit/Investigation/Intelligence Activities
15. Execution of Communication Activities
16. Planning of Human Resources Processes
17. Execution/Supervision of Business Activities
18. Conducting Occupational Health / Safety Activities
19. Conducting Logistics Activities
20. Conducting Goods/Services Purchasing Processes
21. Conducting Goods/Services After-Sales Support Services
22. Conducting Goods/Services Sales Processes
23. Conducting Goods/Services Production and Operation Processes
24. Organization and Event Management
25. Conducting Marketing Analysis Studies
26. Conducting Advertising/Campaign/Promotion Processes
27. Conducting Risk Management Processes
28. Conducting Storage and Archive Activities
29. Conducting Contract Processes
30. Conducting Strategic Planning Activities
31. Monitoring Requests/Complaints
32. Ensuring the Security of Movable Goods and Resources
33. Conducting Supply Chain Management Processes
34. Conducting Wage Policy
35. Marketing of Products/Services Execution of Processes
36. Ensuring the Security of Data Controller Operations
37. Foreign Personnel Work and Residence Permit Procedures
38. Execution of Investment Processes
39. Execution of Talent/Career Development Activities
40. Providing Information to Authorized Persons, Institutions and Organizations
41. Execution of Management Activities
42. Creation and Monitoring of Visitor Records

7. METHOD AND LEGAL REASON OF COLLECTING PERSONAL DATA

Personal data is collected physically and digitally through information and documents requested by our Company from you due to its legitimate interests, information transmitted and obtained verbally, in writing, visually or electronically, information submitted and obtained verbally, in writing, via e-mail, the website, in a manner appropriate to our fields of activity, your data shared with us physically and digitally within the scope of the business relationship, the public information records that you have recorded open to access by 3rd parties and made public by you, your financial data that you have transmitted, your information included in the contracts, your digital applications made through our websites, the information you have transmitted via e-mail and registered electronic mail, your petitions and applications, legal notifications, your correspondence with our Company, HR institutions serving the Company, and legal documents and notifications sent to us to fulfil our legal obligations.

Within the framework of the regulation in the first paragraph of Article 5 of the Law, which states that *"Personal data shall not be processed without explicit consent of the data subject"*, our Company processes personal data in the presence of explicit consent, except for the exceptional cases recognized

by the Law.

Within the scope of Article 5, paragraph 2 of the LPPD, personal data may be processed by the Company without seeking the explicit consent of the data subject only in cases where one of the following conditions is met:

"5/2-a:It is expressly provided for by the laws, 5/2-b: It is necessary for the protection of life or physical integrity of the person himself/herself or of any other person, who is unable to explain his/her consent due to the physical disability or whose consent is not deemed legally valid. 5/2-c: Processing of personal data of the parties of a contract is necessary, provided that it is directly related to the establishment or performance of the contract. 5/2-ç: It is necessary for compliance with a legal obligation to which the data controller is subject. 5/2-e: Data processing is necessary for the establishment, exercise or protection of any right. 5/2-f: Processing of data is necessary for the legitimate interests pursued by the data controller, provided that this processing shall not violate the fundamental rights and freedoms of the data subject."

Before the Company starts data processing activities, explicit consent shall be obtained unless at least one of the legal reasons set forth in Article 5 of the LPPD regarding your personal data and Article 6 of the LPPD regarding sensitive data is detected. If explicit consent cannot be obtained, the data is not processed and the processing is stopped immediately.

8. PURPOSES OF TRANSFERRING PERSONAL DATA

8.1-Transfer of Personal Data:

Our Company may transfer the Data Owner's personal data and sensitive personal data to third parties and institutions in accordance with the lawful personal data processing purposes, by taking the necessary security measures, if one of the conditions set forth in Article 5 of the LPPD is present.

Within the scope of Article 5 of the Law, the Company may transfer the data of personal data owners without obtaining their explicit consent based on the following legal grounds: Law on the Protection of Personal Data Art. 5/2-c: "Processing of personal data of the parties of a contract is necessary, provided that it is directly related to the establishment or performance of the contract." 5/2-ç: "It is necessary for compliance with a legal obligation to which the data controller is subject." 5/2-e: "Data processing is necessary for the establishment, exercise or protection of any right."

Personal data may be transferred to official authorities, authorized public institutions, real or private legal entities, third parties from whom consultancy is received, including lawyers, tax and financial advisors with whom contractual business relationships are established, suppliers, Company shareholders and officers, business partners and group companies, in accordance with the personal data transfer conditions specified in Articles 8 and 9 of the LPPD and this Policy, to carry out the company's business processes and also for the purposes stated above, and in a limited manner and if it is foreseen in the laws, in accordance with the relevant legislation.

Your personal data may be transferred to the relevant authorities upon request within the framework of Article 28/1 of the LPPD, without any obligation to inform and without your explicit consent.

8.2- Transfer of Sensitive Personal Data:

Our Company may transfer sensitive personal data in accordance with the principles set forth in this Policy and by taking the necessary security measures if one of the conditions outlined in Article 6 of the LPPD is present.

In order to transfer special data, obtaining the explicit consent of the data owner, other than the exceptions set out in Article 6 of the Law below is mandatory.

"Personal data concerning health and sexual life may only be processed, without seeking explicit consent of the data subject, by the persons subject to secrecy obligation or competent public institutions and organizations, for the purposes of protection of public health, operation of preventive medicine, medical diagnosis, treatment and nursing services, planning and management of health-care services as well as their financing."

9. DURATION FOR STORING PROCESSED PERSONAL DATA

The Company stores Personal Data for the period specified in the legislation if required by the legislation. If the duration of storing personal data is not regulated in the legislation, Personal Data is processed for the period required by the Company's business and commercial practices, depending on the activity carried out by the Company while processing that data, and then erased, destroyed, or anonymized.

The storage periods for all personal data within the scope of activities carried out in accordance with the processes are specified in the Storage and Destruction Policy.

If the purpose of processing personal data has ended and if the storage periods determined by the relevant legislation and the Company have also expired, personal data can only be stored for the purpose of providing evidence in possible legal disputes or for the assertion of the relevant right related to personal data or for the establishment of defense. In establishing the periods here, the storage durations are determined based on the limitation periods for asserting the said right and the examples of previous requests made to the Company on the same issues despite the expiration of the limitation periods. In this case, the stored personal data is not accessed for any other purpose, and access is provided only when it is necessary to use it in the relevant legal dispute. After the mentioned period has expired, personal data is erased, destroyed, or anonymized.

Personal data is not stored by the Company for the possibility of future use.

10. OBLIGATION TO ERASE, DESTRUCT, OR ANONYMIZE PERSONAL DATA

Article 7 of the Law regulates the erasure, destruction, and anonymization of personal data. Despite being processed in compliance with the provisions of this Law and other relevant laws, personal data shall be erased, destructed, or anonymized by the data controller, ex officio or on the request of the data subject, in the event that the reasons for the processing no longer exist.

In particular, it is accepted that the conditions for processing personal data no longer exist in the following cases:

- Amendment or removal of relevant legislative provisions constituting the basis for processing personal data,
- The contract between the parties has never been established, the contract is not valid, the contract expires, the contract is terminated, or the contract is withdrawn,
- The purpose requiring the processing of personal data no longer exists,
- The processing of personal data is against the law or the rule of honesty,
- In cases where the processing of personal data is carried out only based on the condition of explicit consent, the relevant person withdraws his/her consent,
- The application made by the relevant person regarding the processing of personal data within the framework of his/her rights in subparagraphs (e) and (f) of Article 11 of the Law is accepted by

the data controller,

- In cases where the data controller rejects the application made by the relevant person requesting the erasure or destruction of his/her personal data, the response given is found insufficient or he/she does not respond within the period stipulated in the Law, the relevant person files a complaint to the Board and the Board approves this request,
- Although the maximum duration requiring the storage of personal data has expired, there are no conditions that would justify storing personal data for a longer period,
- The conditions requiring the processing of personal data in Articles 5 and 6 of the Law no longer exist.

In the specified cases, personal data is erased, destroyed, or made anonymous by the data controller ex officio or upon the request of the relevant person.

The process of erasing personal data is defined as *"rendering the personal data in question inaccessible and non-reusable by the relevant users in any way"*. In this context, if the reasons for processing personal data are eliminated, the data in question is irreversibly erased from all media, including backups.

The Data Protection Officer is responsible for deciding which technique for erasing and destroying personal data and which technique for anonymizing personal data will be used.

The personal data that will be subject to the erasure process is determined. The erasure processes are carried out by the personnel determined beforehand. The authorities of these personnel are specially arranged. The access rights of the personnel performing the erasure process to retrieve and reuse the deleted data are revoked.

The Company Data Protection Officer checks whether the erasure, destruction, or anonymization of the data that needs to be erased is carried out in accordance with the law, regulations, and Company policies and procedures and whether the record-keeping for the transactions is accurate.

11. ENLIGHTENING AND INFORMING THE DATA OWNER

The Company, in accordance with Article 10 of the Law, informs Personal Data Owners during the collection of Personal Data. In this context, it provides information on who can process personal data and for what purposes, to whom and for what purposes the processed Personal Data can be transferred, the method and legal reason for collecting personal data, and the rights of the personal data owner.

Within the scope of Article 10 of the LPPD, the "Disclosure Text" is communicated to real persons whose data will be processed and relevant information is provided. The General Disclosure Text, which is intended to inform potential product/service buyers, supplier employees and authorities, consultants with whom contractual work is carried out, legal advisors, visitors, partners/shareholders, persons sought for reference, other third parties whose personal data is processed within the scope of the contract and business relationship, and other third parties whose data is processed, is included on our Company's website and is kept physically within the company and presented for the review of the relevant parties. The Disclosure Texts for Employees, Job Candidates, and Interns clearly inform data owners before the business/contractual relationship is established.

Article 20 of the Constitution states that everyone has the right to be informed about personal data relating to them. Accordingly, Article 11 of the PDP Law includes the right to "request information" among the rights of personal data owners.

In accordance with Article 11 of the PDP Law, the Company provides the necessary information to the

relevant person within the stipulated duration in case the Data Owner requests information. To ensure that the application is answered in a timely and lawful manner, the 'Application Response Procedure' has been drawn up and responsible persons have been determined and assigned within the Company.

12. RIGHTS OF THE DATA OWNER AND EXERCISE OF THESE RIGHTS

12.1- Rights of The Data Owners Per The LPPD:

In case the Data Owner requests information in accordance with Article 11 of the LPPD, our Company provides the necessary information to the relevant person within the time limit. Responses to applications are made in a timely manner and in accordance with the law.

The Company explains to the persons whose Personal Data is collected that they have the following rights in accordance with Article 11 of the Law:

- to learn whether his/her data are processed or not,
- to demand for information as to if his/her data have been processed,
- to learn the purpose of the processing of his/her data and whether these personal
- data are used in compliance with the purpose,
- to know the third parties to whom his data are transferred in the country or abroad,
- to request the rectification of the incomplete or inaccurate data, if any,
- to request the erasure or destruction of his/her data under the conditions referred to in Article 7,
- to request reporting of the operations carried out pursuant to sub-paragraphs (d) and (e) to third parties to whom his/her data have been transferred,
- to object to the occurrence of a result against the person himself/herself by analyzing the data processed solely through automated systems,
- to claim compensation for the damage arising from the unlawful processing of his/her data.

12.2- Exercise of Data Owner's Rights:

The data owner may exercise the rights listed under Article 11 above, in accordance with Article 13, paragraph 1 of the LPPD.

To exercise your rights specified in Article 11 of the LPPD:

You can personally submit your application to the address "Hacımimi Mah. Kemeraltı Cad. No.15 Kat 4 34424 Karaköy/ İstanbul", send it via notary or (KEP) Registered Electronic Mail adco@hs01.kep.tr with secure electronic signature, mobile signature or your electronic mail address previously notified to the data controller by the relevant person and registered in the data controller's system. Data owner's request will be finalized free of charge as soon as possible and within thirty days at the latest, depending on its nature. If the transaction creates an additional cost for the Company, the data owner may be charged a fee according to the tariff to be determined by the Communique on the Principles and Procedures For the Application to Data Controller. In case the request is rejected, the reasons for rejection will be notified to the data owner in writing or electronically with the reasons.

Third parties cannot make a request on behalf of personal data owners.

For a person other than the personal data owner to make a request, there must be a special power of attorney issued by the personal data owner on behalf of the person who will apply.

In accordance with Article 14 of the Personal Data Protection Law, if the data owner's request is refused, the response is found insufficient, or the request is not responded within the specified time period, the

data subject may lodge a complaint with the Personal Data Protection Board within thirty days as of he/she learns about the response of the data controller, or within sixty days as of the request date, in any case.

12.3- The Company's Right to Reject the Application of the Data Owner:

The company may reject an applicant's application, providing reasons in the following situations:

- Processing of personal data made public by the personal data owner.
- The request of the personal data owner is likely to interfere with the rights and freedoms of other persons,
- The requested information is public.
- Processing of personal data for official purposes such as research, planning, and statistics by making it anonymous.
- Processing of personal data within the scope of security and intelligence activities carried out by public institutions and organizations authorized by law to ensure public order in the fields of national defense, national security and public safety, and economic security.
- Processing of personal data by the judicial authority in relation to investigation, prosecution, trial, or execution proceedings.
- Processing of personal data is necessary for the investigation or examination carried out by official and authorized public institutions and organizations.

To determine whether the applicant is the personal data owner, the Company may request additional information and documents from the relevant person and may ask questions to the personal data owner regarding the matters included in the application.

13. ENSURING THE SECURITY OF PERSONAL DATA

The Company has implemented the infrastructure and controls that will protect the integrity of information and guarantee its continuous accessibility. In order to prevent the reckless or unauthorized disclosure, access, transfer, or other unlawful access of personal data and against other technical threats that may occur, the following technical and administrative measures have been implemented according to the nature of the data to be protected.

13.1-Technical Measures:

The security system protects personal data from all threats while it is kept within individuals' information systems.

Among all information security threats, internal threats, which we can define as conscious or unconscious threats that may be posed by people working within the Company, have a very important place.

Taking into account the conscious or unconscious threats that may be posed by people working within the Company, the necessary security controls have been implemented in all relevant areas to control access to information and prevent unauthorized access.

The Company's information system unit regularly checks whether employees' daily activities comply with their authorization profiles.

Authorization level approvals are given by the Data Protection Officer.

Passwords used by personnel or third parties to access personal data sources are regulated in accordance with the password determination rules defined for the relevant systems.

Multi-level network security measures have been established in the Company against threats from

external networks. Anti-virus software, firewalls, and central management software are used in the Institution's computer systems.

The services where viruses are most commonly spread, e-mail, http and ftp traffic, are directed to the anti-virus gateway based on firewall logic. After the scanning process here, they are directed to the necessary recipients. With this system, viruses coming from remote sources are blocked. With the anti-virus system installed on the mail servers, viruses circulating via e-mail within the local network are also neutralized.

With virus protection software installed on server computers and software that will monitor the systems of Company employees, a corporate anti-virus solution is provided within the Company. These monitoring activities include security scanning against known vulnerabilities, security scanning for applications according to the application type, and system configuration controls. The log programs used help system administrators monitor the system closely. A backup procedure is organized for backups, critical systems are periodically backed up, backup files are transferred to external media at certain intervals, and loopback tests are performed at specified times.

13.2- Administrative Measures:

The main purpose of the policies prepared by our Company regarding Data Security is to explain the personal data processing activities carried out and the processes for the protection of personal data, to inform the data owner natural persons whose personal data are processed by the Company, to ensure transparency in practice, data security and compliance with the Law.

The 'Risks and Threats Table', which lists the threats that may be consciously or unconsciously posed by employees within the company and the dangers that may come from external networks, is periodically reviewed by the Data Security Committee and the measures are updated.

Technical control systems have been established on the applications. As the data controller, the institution conducts systematic periodic audits through the Data Protection Officer. Audits will be carried out by expert companies or independent audit companies when deemed necessary.

In order to control access to information and prevent unauthorized access, ensure data security, and implement lawful storage and destruction procedures, the "Identity Management and Authorization Procedure" and "Personal Data Storage and Destruction Policy" have been prepared and put into practice in the relevant areas. In the event of a data breach, the Personal Data Protection Board and data owners are informed and assignments have been made to ensure that preventive measures regarding the breach are taken immediately.

Privacy commitments: "The data controllers and data processors shall not disclose the personal data that they have learned to anyone contrary to the provisions of this Law. This obligation shall continue even after the end of their term of office."

Pursuant to the second paragraph of Article 12 of the Law, Data Processors shall be jointly responsible with the data controller for ensuring the security of personal data.

The contract, which includes compliance with the law and confidentiality principles, and which also subjects data processors to the obligations of the data controller and holds the data processor jointly liable in the event of a violation of the law, is signed by the data processors. To the contracts made and to be made by the Company with persons and companies to which personal data is transferred in accordance with the law, joint responsibility provisions that stipulate them to take the necessary security and confidentiality measures for the protection of personal data and ensure that these measures are complied within their respective organizations shall be added.

It is mandatory to obtain a letter of commitment for ensuring data confidentiality and compliance with

security measures from all employees and other persons or institutions that process data.

In this context, confidentiality commitments are added to contracts made with employees, consultants, information system support companies, and other third parties or companies.

The company ensures that the necessary training is organized for business units to increase awareness on preventing the unlawful processing of personal data, unlawful access to data, and ensuring the protection of data.

Company employees are prohibited from using personal data for private or commercial purposes, sharing this data with unauthorized persons, or making this data accessible by any other means.

Company employees may only access personal information based on authorization within the scope and type of their duties. For this purpose, the roles and responsibilities are detailed, separated, and implemented with the authorization matrix.

The company establishes the necessary systems, provides training, and works with consultants when necessary to raise awareness of its current employees and newly recruited employees on the protection of personal data.

14. IMPLEMENTATION OF THE POLICY AND RELEVANT LEGISLATION

The relevant legal regulations in force regarding the processing and protection of personal data will primarily be applied. In the event of any inconsistency between the current legislation and the Company Policy, our Company accepts that the current legislation will be applied.

15. ENFORCEMENT OF THE POLICY

This Policy, prepared by the Company, is dated June 4, 2023. If the entire Policy or specific articles are renewed, the effective date will be updated accordingly. The Policy is published on the Company's website, and its review and update are conducted by the Data Protection Officer authorized by the Company. The Policy is reviewed at least once a year.