

DCS DİJİTAL GÜMRÜK HİZMETLERİ A.Ş.

PERSONAL DATA PROTECTION AND PROCESSING POLICY

INTRODUCTION

I. IMPORTANCE OF THE PROTECTION OF PERSONAL DATA

The protection of personal data is a fundamental constitutional right and constitutes one of the key priorities of DCS Digital Customs Services Inc. Accordingly, our Company has established a continuously updated personal data protection framework, and this Policy has been prepared within this scope.

Pursuant to the Turkish Personal Data Protection Law No. 6698 ("Law"), and in our capacity as the Data Controller, this Policy has been adopted by DCS Digital Customs Services Inc. ("Company") in order to fulfill the general obligation to inform and to set out the fundamental principles governing the processing of personal data within our Company. Within this framework, this Policy regulates the basic principles regarding the protection of personal data belonging to our customers, potential customers, employees, job applicants, interns and students, employees and authorized representatives of suppliers and subcontractors, company shareholders and partners, visitors, and other third parties whose personal data are processed by our Company.

To ensure the effective implementation of the matters set out in this Policy, the necessary internal procedures are established within the Company; information notices aligned with the Personal Data Processing Inventory and tailored to specific data subject categories are prepared; personal data protection and confidentiality agreements are executed with Company employees and third parties who have access to personal data; job descriptions are revised accordingly; and the required administrative and technical measures for the protection of personal data are implemented by DCS Digital Customs Services Inc. Within this scope, the necessary audits are conducted or commissioned.

The protection of personal data is also embraced at the senior management level. Accordingly, a dedicated committee (the Company's Personal Data Protection Committee) has been established, through which personal data protection processes are governed and monitored.

II. PURPOSE OF THE POLICY

The primary purpose of this Policy is to set out the principles governing the lawful processing and protection of personal data carried out by DCS Digital Customs Services Inc., and to ensure transparency by informing and enlightening the individuals whose personal data are processed by our Company within this framework.

III. SCOPE

This Policy applies to all personal data processed by DCS Digital Customs Services Inc. through fully or partially automated means, or by non-automated means provided that they form part of any data recording system, relating to individuals categorized under the following groups: customers, potential customers, employees, job applicants, interns and students, employees and authorized representatives of suppliers and subcontractors, company shareholders and partners, visitors, parents/guardians/legal representatives, and other third parties whose personal data are processed by our Company.

IV. IMPLEMENTATION OF THE POLICY AND RELEVANT LEGISLATION

With regard to the processing and protection of personal data, the applicable statutory regulations in force shall primarily apply. In the event of any inconsistency between the applicable legislation and this Policy, our Company acknowledges and undertakes that the provisions of the applicable legislation shall prevail.

V. ACCESS AND UPDATES

This Policy is published on our Company's website at <http://www.dccustoms.com.tr/> and is made available to data subjects upon request. The Policy may be updated from time to time, as deemed necessary.

SECTION 2: PROCESSING OF PERSONAL DATA

In accordance with Article 20 of the Constitution of the Republic of Türkiye and Article 4 of the Turkish Personal Data Protection Law No. 6698 ("Law"), our Company processes personal data in a manner that is lawful and consistent with the principles of good faith; accurate and, where necessary, kept up to date; for specific, explicit, and legitimate purposes; and limited, proportionate, and relevant to such purposes. Personal data are retained for the period stipulated in the applicable legislation or for as long as required by the purpose of processing.

Pursuant to Articles 20 of the Constitution and 5 of the Law, our Company processes personal data based on one or more of the legal grounds set out under Article 5 of the Law governing the processing of personal data.

In accordance with Article 419 of the Turkish Code of Obligations, and without prejudice to the provisions of the Turkish Personal Data Protection Law No. 6698, our Company processes the personal data of employees and job applicants for purposes related to their suitability for employment and the performance of the employment contract.

In line with Article 20 of the Constitution and Article 10 of the Law, our Company duly informs data subjects regarding the processing of their personal data. Where data subjects request information or submit applications to exercise their rights arising from the Law, the necessary information is provided and such requests are responded to within the statutory time limits.

Our Company acts in compliance with Article 6 of the Law and adheres to the regulations governing the processing of special categories of personal data.

In accordance with Articles 8 and 9 of the Law, our Company complies with the statutory rules regarding the transfer of personal data and carries out such transfers by taking into account the decisions of the Personal Data Protection Board, published communiqués, and the lists of countries deemed to provide an adequate level of protection.

I. PROCESSING OF PERSONAL DATA IN COMPLIANCE WITH THE PRINCIPLES AND RULES PRESCRIBED BY LEGISLATION

1. Principles of Personal Data Processing

A) Processing in Compliance with the Law and the Principle of Good Faith

Our Company acts in compliance with the principles introduced by applicable legal regulations and the principle of good faith in the processing of personal data. Within this scope, our Company identifies the legal grounds that require the processing of personal data, takes into account the principle of proportionality, refrains from using personal data beyond the purposes for which they are processed, and does not carry out personal data processing activities without the knowledge of the data subjects.

B) Ensuring That Personal Data Are Accurate and, Where Necessary, Kept Up to Date

Our Company ensures that the personal data it processes are accurate and, where necessary, kept up to date, taking into consideration the fundamental rights of data subjects and its own legitimate interests, and implements the necessary measures accordingly. In this context, efforts are made to keep the data relating to all data subject categories up to date. In particular, customer and potential customer data are updated with due care, and marketing or promotional emails and offers are not sent to individuals in a manner contrary to their consent.

C) Processing for Specific, Explicit, and Legitimate Purposes

Our Company determines its personal data processing purposes in a clear, explicit, and lawful manner. Personal data are processed only to the extent necessary and in connection with the services provided by our Company. The purposes for which personal data will be processed are determined prior to the processing activity and are recorded in the Personal Data Processing Inventory.

D) Being Relevant, Limited, and Proportionate to the Purpose of Processing

Our Company processes personal data in a manner suitable for achieving the specified purposes and refrains from processing personal data that are not relevant to or required for the realization of such purposes. Within this framework, processes are continuously reviewed, and the principle of Data Minimization is implemented and reinforced.

E) Retention of Personal Data for the Period Prescribed by the Relevant Legislation or Required for the Purpose of Processing

Our Company retains personal data only for the period stipulated under the relevant legislation or for as long as required for the purposes for which they are processed. Within this scope, our Company first determines whether a specific retention period is prescribed under the applicable legislation. Where such a period is specified, personal data are retained in compliance with such period, taking into consideration statutory limitation periods under civil and criminal law.

Upon the expiration of the retention period or where the purposes requiring the processing of personal data cease to exist, personal data are deleted, destroyed, or anonymized in accordance with our Company's Personal Data Retention and Destruction Policy.

2. Rules on the Processing of General Categories of Personal Data

The protection of personal data is a constitutional right. Fundamental rights and freedoms may be restricted only by law and solely for the reasons specified in the relevant provisions of the Constitution, without prejudice to their essence. Pursuant to the third paragraph of Article 20 of the Constitution, personal data may be processed only in cases expressly provided for by law or with the explicit consent of the data subject.

Accordingly, our Company processes personal data without seeking the explicit consent of the data subject only where one or more of the following conditions are met:

- a. Processing is expressly provided for by law;
- b. Processing is mandatory for the protection of the life or physical integrity of the data subject or another person where the data subject is unable to express consent due to actual impossibility or where such consent is not legally valid;
- c. Processing is directly related to the establishment or performance of a contract, provided that it is necessary to process the personal data of the parties to the contract;
- d. Processing is mandatory for the data controller to fulfill its legal obligation;
- e. The personal data have been made public by the data subject;
- f. Processing is mandatory for the establishment, exercise, or protection of a right;
- g. Processing is mandatory for the legitimate interests of the data controller, provided that such processing does not violate the fundamental rights and freedoms of the data subject.

Where none of the above conditions apply, our Company relies on the explicit consent of the data subject, which must be freely given, informed, and based on the individual's own will.

In particular, within the scope of Human Resources and employment relations, taking into account the dependency inherent in the employment relationship, our Company primarily relies on lawful processing grounds other than explicit consent. Explicit consent is sought only where such lawful grounds are not applicable. Conversely, in activities such as marketing, personal data processing is carried out primarily based on the data subject's consent.

In all cases where personal data are processed, data subjects are duly informed through appropriate information notices, and processing activities are carried out in accordance with the obligation to inform.

3. Rules on the Processing of Special Categories of Personal Data

In the processing of personal data classified as “special categories of personal data” under the Turkish Personal Data Protection Law No. 6698 (“Law”), our Company acts in full compliance with the regulations stipulated under the Law. Article 6 of the Law defines certain categories of personal data which, if processed unlawfully, may give rise to discrimination or serious harm to individuals, and therefore require a higher level of care and sensitivity.

These special categories of personal data include data relating to race, ethnic origin, political opinion, philosophical belief, religion, sect or other beliefs, attire, membership of associations, foundations or trade unions, health, sexual life, criminal convictions and security measures, as well as biometric and genetic data.

In accordance with the Law, and subject to the implementation of adequate safeguards, our Company processes special categories of personal data only in the following circumstances:

Special categories of personal data other than data relating to health and sexual life may be processed where expressly provided for by law or where the data subject has given explicit consent;

Special categories of personal data relating to health and sexual life may be processed only for the purposes of protecting public health, preventive medicine, medical diagnosis, treatment and care services, or the planning and management of healthcare services and their financing, by persons or authorized institutions and organizations under a duty of confidentiality, or based on the explicit consent of the data subject;

Regardless of the legal ground relied upon, all processing activities are carried out in compliance with the general principles of personal data processing set out under Article 4 of the Law (see Section 2, I, 1 above).

With regard to the protection of special categories of personal data, our Company has adopted and implemented a Special Categories of Personal Data Protection Policy, and all relevant business units act in accordance with this policy and take the necessary administrative and technical measures.

4. Informing and Providing Information to Data Subjects

In accordance with Article 10 of the Law, our Company informs data subjects at the time personal data are obtained. Within this scope, data subjects are informed about the purposes of processing their personal data, the persons to whom and the purposes for which such personal data may be transferred, the method and legal basis of personal data collection, and the rights of the data subject whose personal data are processed.

The relevant departments of our Company carry out the necessary procedures in line with the Company’s Information Notice Principles Policy.

Furthermore, pursuant to Article 11 of the Law, the right to request information is among the rights granted to data subjects. Accordingly, in compliance with Article 20 of the Constitution and Article 11 of the Law, where a data subject submits a request for information, our Company provides the necessary information and processes such requests in accordance with the Company’s Data Subject Application Procedure.

II. TRANSFER OF PERSONAL DATA

In line with its lawful personal data processing purposes, and by taking the necessary administrative and technical security measures, our Company may transfer the personal data and special categories of personal data of data subjects to third parties. In this respect, our Company acts in compliance with the provisions set forth under Article 8 of the Turkish Personal Data Protection Law No. 6698 (“Law”).

1. Principles Governing the Transfer of Personal Data

For legitimate and lawful personal data processing purposes, our Company may transfer personal data to third parties in a limited manner and based on one or more of the personal data processing conditions specified under Article 5 of the Law, as set out below:

- Where the data subject has given explicit consent; or
- Where the transfer of personal data is expressly provided for by law;
- Where the transfer is mandatory for the protection of the life or physical integrity of the data subject or another person, and the data subject is unable to express consent due to actual impossibility or where such consent is not legally valid;
- Where the transfer of personal data of the parties to a contract is directly related to and necessary for the establishment or performance of the contract;
- Where the transfer of personal data is mandatory for our Company to fulfill its legal obligations;
- Where the personal data have been made public by the data subject;
- Where the transfer of personal data is mandatory for the establishment, exercise, or protection of a right;
- Where the transfer of personal data is mandatory for the legitimate interests of our Company, provided that such transfer does not violate the fundamental rights and freedoms of the data subject.

Regardless of the legal ground relied upon, all transfer processes are carried out in compliance with the general principles of personal data processing set out under Article 4 of the Law (see Section 2, I, 1 above).

2. Transfer of Special Categories of Personal Data

By exercising due care, implementing the necessary administrative and technical security measures, and taking the adequate safeguards prescribed by the Personal Data Protection Board, our Company may transfer special categories of personal data of data subjects to third parties in line with its legitimate and lawful personal data processing purposes, under the following circumstances:

- Where the data subject has given explicit consent; or
- Where the data subject has not given explicit consent:
 - Special categories of personal data other than data relating to the data subject's health and sexual life (including data relating to race, ethnic origin, political opinion, philosophical belief, religion, sect or other beliefs, attire, membership of associations, foundations or trade unions, criminal convictions and security measures, as well as biometric and genetic data) may be transferred in cases expressly provided for by law;
 - Special categories of personal data relating to the data subject's health and sexual life may be transferred only for the purposes of protecting public health, preventive medicine, medical diagnosis, treatment and care services, or the planning and management of healthcare services and their financing, by persons or authorized institutions and organizations under a duty of confidentiality.

Regardless of the legal ground relied upon, all transfer processes are carried out in compliance with the general principles of personal data processing set out under Article 4 of the Law (see Section 2, I, 1 above).

3. Transfer of Personal Data Abroad

In line with its lawful personal data processing purposes and by implementing the necessary administrative and technical security measures, our Company may transfer the personal data and special categories of personal data it processes to third parties abroad. Personal data are transferred by our Company either to foreign countries declared by the Personal Data Protection Board as providing an adequate level of protection ("Foreign Countries with Adequate Protection") or, where an adequate level of protection is not available, to foreign countries in which the data controllers in Türkiye and the relevant foreign country have provided a written undertaking to ensure adequate protection and where the permission of the Personal Data Protection Board has been obtained ("Foreign Countries Where the Data Controller Has Undertaken Adequate Protection").

In this regard, our Company acts in compliance with the provisions set forth under Article 9 of the Turkish Personal Data Protection Law No. 6698 ("Law").

For legitimate and lawful personal data processing purposes, our Company may transfer personal data to Foreign Countries with Adequate Protection or to Foreign Countries Where the Data Controller Has Undertaken Adequate Protection, where the data subject has given explicit consent or, in the absence of explicit consent, where one of the following conditions exists:

- Where the transfer of personal data is expressly provided for by law;
- Where the transfer is mandatory for the protection of the life or physical integrity of the data subject or another person, and the data subject is unable to express consent due to actual impossibility or where such consent is not legally valid;
- Where the transfer of personal data of the parties to a contract is directly related to and necessary for the establishment or performance of the contract;

AUTHORIZED PUBLIC INSTITUTIONS	Public institutions and organizations legally authorized to request and receive information and documents from our Company	Personal data are shared in accordance with the provisions of the applicable legislation.
AUTHORIZED PRIVATE LAW PERSONS	Private law entities legally authorized to request and receive information and documents from our Company	Personal data are shared in a limited manner and solely for the purpose requested, within the scope of the legal authority of the relevant private law entities.
AFFILIATES	Companies in which our Company holds shares	Personal data are shared in a limited manner to ensure the execution of commercial activities that require the involvement of our Company's affiliates.
SHAREHOLDERS	Shareholders of Our Company	Personal data are shared in a limited manner for the purposes of designing strategies related to our Company's commercial activities and for audit and oversight purposes..
OUR BUSINESS PARTNERS (I)	Parties with whom our Company has established business partnerships for purposes such as the sale, promotion, and marketing of its products and services, after-sales support, and the execution of joint customer loyalty programs while conducting its commercial activities	Personal data are shared in a limited manner to ensure the fulfillment of the purposes for which the business partnership has been established.
SUPPLIERS	Parties providing services to our Company while carrying out its commercial activities	Personal data are shared in a limited manner to ensure the provision of services outsourced by our Company from suppliers and required for the performance of its commercial activities.

OUR BUSINESS AND CLOSE SOLUTION PARTNERS (II)	Close solution partners with whom our Company collaborates	Personal data are shared and transferred within the group due to operational and support services provided to and received from our Company. For example, ATEZ Software Technologies Inc. provides information technologies support and services to our Company, while our Company provides human resources support and services to the relevant group companies.
--	--	---

- Where the transfer of personal data is mandatory for our Company to fulfill its legal obligations;
- Where the personal data have been made public by the data subject;
- Where the transfer of personal data is mandatory for the establishment, exercise, or protection of a right;
- Where the transfer of personal data is mandatory for the legitimate interests of our Company, provided that such transfer does not violate the fundamental rights and freedoms of the data subject.

4. Purposes of Personal Data Transfers and Categories of Recipients

A) Purposes of Data Transfers

Personal data transfers are carried out for purposes such as ensuring the fulfillment of our Company's activities and objectives of incorporation; enabling the provision of services obtained by our Company from suppliers and third-party service providers that are necessary for the conduct of our commercial activities; ensuring the execution of our Company's human resources and employment policies; and fulfilling obligations and implementing necessary measures within the scope of occupational health and safety.

B) Categories of Recipients to Whom Personal Data Are Transferred

In accordance with Articles 8 and 9 of the Turkish Personal Data Protection Law No. 6698 ("Law"), our Company may transfer personal data to the following categories of recipients:

(Recipient categories to be listed below, e.g. suppliers, service providers, public authorities, business partners, etc.)

In all personal data transfer activities carried out by our Company, the principles and rules set forth in this Policy are strictly observed.

III. PERSONAL DATA CATEGORIZATIONS

The categories of data subjects whose personal data are processed by our Company, as well as the types of personal data processed within this scope, are classified as follows:

DATA SUBJECT CATEGORIZATION

JOB APPLICANT	Natural persons who have applied for a position with our Company through any means or who have shared their résumés and relevant information with our Company for evaluation.
EMPLOYEE	Natural persons employed by our Company.
SHAREHOLDER / PARTNER	Natural persons who are shareholders or partners of our Company.
POTENTIAL CUSTOMER	Natural persons who have requested or shown interest in using our products and services, or who are reasonably assessed to have a commercial relationship with our Company in accordance with the principles of good faith.
INTERN / STUDENT	Individuals who are undertaking internships at our Company or working within the scope of programs subject to compulsory internship or practical training requirements.
SUPPLIER EMPLOYEE	Natural persons employed by institutions with which our Company has any type of business relationship (such as business partners, suppliers, without limitation).
SUPPLIER AUTHORIZED PERSON	Natural persons who are shareholders or authorized representatives of institutions with which our Company has a business relationship.
CUSTOMER	Natural persons who use or have used the products and services provided by our Company, regardless of whether they have any contractual relationship with our Company.
PARENT / GUARDIAN / REPRESENTATIVE	Natural persons whose personal data are processed in their capacity as a parent, guardian, or representative.
VISITOR	Natural persons who have entered the physical premises owned by our Company for various purposes or who visit our Company's websites.
OTHER	Third-party natural persons who are related to the above-mentioned parties for the purposes of ensuring the security of commercial transactions between our Company and the aforementioned parties, or protecting the rights of such persons and securing legitimate interests (e.g., family members and relatives).

DATA CATEGORIES

IDENTITY INFORMATION	Information contained in documents such as Driver’s License, National Identity Card, Certificate of Residence, Passport, Attorney Identification Card, and Marriage Certificate, which clearly belong to an identified or identifiable natural person and are processed partially or fully by automated means or by non-automated means provided that they form part of a data recording system.
CONTACT INFORMATION	Information such as telephone number, address, and e-mail address, which clearly belong to an identified or identifiable natural person and are processed partially or fully by automated means or by non-automated means provided that they form part of a data recording system.
LOCATION INFORMATION	Information that clearly belongs to an identified or identifiable natural person and is processed partially or fully by automated means or by non-automated means provided that it forms part of a data recording system, which identifies the location of the data subject while using our products and services or the location of employees of institutions with which we cooperate while they are using vehicles belonging to our Company.
EMPLOYEE PERSONAL FILE (PERSONNEL INFORMATION)	Any personal data processed, which clearly belong to an identified or identifiable natural person and are processed partially or fully by automated means or by non-automated means provided that they form part of a data recording system, relating to the acquisition of information that forms the basis for the establishment of personal rights of our employees or natural persons who have an employment relationship with our Company.
LEGAL TRANSACTION AND COMPLIANCE INFORMATION	Personal data that clearly belong to an identified or identifiable natural person and are processed partially or fully by automated means or by non-automated means provided that they form part of a data recording system, processed within the scope of determining, following up, and enforcing our legal receivables and rights, fulfillment of our obligations, and compliance with our Company’s policies.
CUSTOMER TRANSACTION INFORMATION	Information that clearly belongs to an identified or identifiable natural person and is included in a data recording system, such as records relating to the use of our products and services, and instructions and requests necessary for the customer’s use of products and services.
PHYSICAL PREMISES SECURITY INFORMATION	Personal data that clearly belong to an identified or identifiable natural person and are included in a data recording system, relating to records and documents obtained during entry into physical premises and during presence within the physical premises.

PROCESSING SECURITY INFORMATION	Personal data that clearly belong to an identified or identifiable natural person and are included in a data recording system, processed to ensure technical, administrative, legal, and commercial security during the conduct of activities.
RISK MANAGEMENT INFORMATION	Personal data that clearly belong to an identified or identifiable natural person and are included in a data recording system, processed through methods used in accordance with generally accepted legal and commercial practices and the principle of good faith, in order to manage our commercial, technical, and administrative risks.
FINANCIAL INFORMATION	Personal data that clearly belong to an identified or identifiable natural person and are processed partially or fully by automated means or by non-automated means provided that they form part of a data recording system, relating to information, documents, and records reflecting all kinds of financial outcomes arising according to the type of legal relationship established between our Company and the data subject.
PERFORMANCE AND CAREER DEVELOPMENT INFORMATION (PROFESSIONAL EXPERIENCE INFORMATION))	Personal data that clearly belong to an identified or identifiable natural person and are processed partially or fully by automated means or by non-automated means provided that they form part of a data recording system, processed for the purposes of measuring the performance of our employees or natural persons who have an employment relationship with our Company, and planning and conducting their career development within the scope of our Company's human resources policy.
PAZARLAMA BİLGİSİ	Personal data that clearly belong to an identified or identifiable natural person and are processed partially or fully by automated means or by non-automated means provided that they form part of a data recording system, processed for the purpose of marketing our products and services by customizing them in line with the usage habits, preferences, and needs of the data subject, as well as the reports and evaluations generated as a result of such processing.
VISUAL / AUDIO INFORMATION	Personal data that clearly belong to an identified or identifiable natural person and are processed partially or fully by automated means or by non-automated means provided that they form part of a data recording system; for example, photographs and camera recordings (excluding records falling within the scope of Physical Premises Security Information), audio recordings, and data contained in documents that constitute copies of documents containing personal data.
SPECIAL CATEGORIES OF PERSONAL DATA – I	Data relating to health and sexual life.
SPECIAL CATEGORIES OF PERSONAL DATA – II	Data relating to race, ethnic origin, political opinion, philosophical belief, religion, sect or other beliefs, appearance and attire, membership in associations, foundations, or trade unions, criminal convictions and security measures, as well as biometric and genetic data.

SECTION 3: LEGAL GROUNDS AND PURPOSES OF PROCESSING PERSONAL DATA

I. LEGAL GROUNDS FOR THE PROCESSING OF PERSONAL DATA

1. General Principles

Although the legal grounds for processing personal data by our Company may vary depending on the nature of the processing activity, all personal data processing activities are carried out in compliance with the general principles set forth under Article 4 of the Turkish Personal Data Protection Law No. 6698 ("Law"). Accordingly, in all personal data processing activities, the following principles are taken into consideration:

- a) Processing in compliance with the law and the principle of good faith;
- b) Ensuring that personal data are accurate and, where necessary, kept up to date;
- c) Processing for specific, explicit, and legitimate purposes;
- d) Being relevant, limited, and proportionate to the purposes for which they are processed;
- e) Retaining personal data for the period prescribed under the relevant legislation or for as long as required for the purposes of processing.

2. Legal Grounds for Lawful Processing

A) Explicit Consent of the Data Subject

One of the legal grounds for the processing of personal data is the explicit consent of the data subject. The explicit consent of the data subject must be specific to a particular subject, based on adequate information, and freely given.

B) Processing Expressly Provided for by Law

Personal data of the data subject may be processed lawfully where such processing is expressly provided for by law.

For example: Notification of employee identity information to the competent authorities pursuant to identity notification legislation.

C) Inability to Obtain Explicit Consent Due to Actual Impossibility

Where the processing of personal data is mandatory for the protection of the life or physical integrity of the data subject or another person, and the data subject is unable to express consent due to actual impossibility or where such consent is not legally valid, personal data of the data subject may be processed. For example: Sharing the blood type information of an employee who has fainted with a physician.

D) Direct Relevance to the Establishment or Performance of a Contract

Personal data may be processed where such processing is directly related to and necessary for the establishment or performance of a contract, provided that the personal data belong to the parties to the contract.

For example: Obtaining a résumé from a job applicant for the establishment of an employment contract, or collecting address information to enable official notifications under a contract.

E) Fulfillment of the Company's Legal Obligations

Where the processing of personal data is mandatory for our Company, acting as the data controller, to fulfill its legal obligations, personal data of the data subject may be processed.

For example: Processing family information in order to enable employees to benefit from statutory tax allowances.

F) Personal Data Made Public by the Data Subject

Where the data subject has made their personal data public, such personal data may be processed.

For example: Where customers submit complaints, requests, or suggestions on a publicly accessible online platform, they are deemed to have made the relevant information public. In such cases, our Company may process such data solely for the purpose of responding to the complaint, request, or suggestion.

G) Necessity for the Establishment, Exercise, or Protection of a Right

Personal data may be processed where such processing is mandatory for the establishment, exercise, or protection of a right.

For example: Retention and use, when necessary, of evidentiary data such as sales contracts or invoices.

H) Necessity for the Legitimate Interests of the Company

Provided that it does not harm the fundamental rights and freedoms of the data subject, personal data may be processed where such processing is mandatory for the legitimate interests of our Company.

For example: Monitoring critical areas through security cameras for the purposes of preventing theft or ensuring occupational health and safety.

3. Processing of Special Categories of Personal Data and Legal Grounds

In the absence of the explicit consent of the data subject, special categories of personal data may be processed by our Company only in cases expressly provided for by law and subject to the implementation of adequate safeguards to be determined by the Personal Data Protection Board.

Special categories of personal data relating to the data subject's health and sexual life may be processed solely for the purposes of protecting public health, preventive medicine, medical diagnosis, treatment and care services, or the planning and management of healthcare services and their financing, and only by persons or authorized institutions and organizations under a duty of confidentiality.

Regardless of the legal ground relied upon, the general principles of personal data processing are always taken into consideration throughout the processing activities, and compliance with such principles is ensured (Article 4 of the Law; see Section 2, I, 1 above).

II. PURPOSES OF PROCESSING PERSONAL DATA

Our Company processes personal data solely for the purposes and under the conditions set out within the scope of the personal data processing grounds specified in paragraph (2) of Article 5 and paragraph (3) of Article 6 of the Turkish Personal Data Protection Law No. 6698 ("Law").

During the data processing activities, the legal grounds outlined above are taken into consideration, and where no other lawful basis exists, the explicit consent of the data subject is obtained. In this context, compliance with the general principles set forth under Article 4 of the Law is reviewed in all cases, and first and foremost, it is ensured that the data processing activity as a whole complies with the principles of lawfulness.

Where explicit consent is relied upon, such consent is obtained in a manner that is explicit, informed, and freely given. The purposes of processing personal data are also specified in our Company's Personal Data Processing Inventory.

Personal data are processed within our Company's departments primarily for the purposes set out below:

- As an employer, our Company is required to process employees' personal data in order to fulfill the mutual rights and obligations arising from employment contracts. Employees' personal data are processed and retained in a manner that is lawful and in accordance with the principles of good faith; accurate and, where necessary, kept up to date; processed for specific, explicit, and legitimate purposes; and limited, proportionate, and relevant to such purposes. Within this scope, employees' personal data are processed for purposes necessary to ensure lawful employment, including the lawful execution of processes relating to the establishment, performance, and termination of employment contracts; the legitimate interests of the Company, provided that such interests do not violate fundamental rights and freedoms; cases expressly provided for by law; the fulfillment of legal obligations arising from employment; situations where data processing is mandatory for the establishment, exercise, or protection of a right in the context of legal proceedings; and, in circumstances not covered by these grounds, based on the employee's explicit consent, which is obtained in an informed manner and freely given.

- Within the scope of activities required by the Company's field of operation, the legitimate interests of the employer may necessitate the processing of employees' personal data. Accordingly, personal data processing activities may be carried out for purposes such as preventing abuse, deterring theft, ensuring general security, or maintaining occupational health and safety. In such cases, utmost care is taken to ensure that employees' fundamental rights and freedoms are not adversely affected.
- The majority of employees' personal data processed are obtained directly from the employees themselves. In certain cases, personal data may also be obtained from internal sources such as Company executives, from employee references, or from systems established by public institutions and organizations, as required by the obligations arising from working life.
- The personal data of employees processed by our Company include, but are not limited to, information contained in job application forms and employee references; employment contracts and any amendments thereto; employees' contact details; information required for payroll processing; family member or close contact information to be used in emergency situations; education records; performance evaluation records; disciplinary records; and camera recordings.
- With regard to the processing of employees' personal data, the rules governing such processing are set out in various Company policies and procedures. These documents are accessible via the Company's intranet system and may also be obtained in hard copy from the Human Resources Department.
- Employees' health data are also among the personal data processed by our Company. Personal data relating to employees' health and sexual life are, as a rule, processed solely for the purposes of protecting public health, preventive medicine, medical diagnosis, treatment and care services, or the planning and management of healthcare services and their financing, by persons or authorized institutions and organizations under a duty of confidentiality. Within this scope, employees' health data and related details are, as a rule, retained by the workplace physician and the occupational health unit.
- After an individual acquires employee status (and not at the job applicant stage), trade union membership information may be processed where an employee becomes a member of a trade union, as expressly required by applicable legislation in order to fulfill statutory obligations. Other special categories of personal data relating to employees—such as race, ethnic origin, political opinion, philosophical belief, religion, sect or other beliefs, or attire—are, as a rule, not processed unless expressly provided for by law. Where an exceptional practice is envisaged, the necessity and legal requirements are carefully assessed prior to any processing activity.
- Monitoring and supervision may be carried out with respect to the Company's information and communication tools (including telephones, mobile phones, computers, and internet access). Law No. 5651, the relevant legislation, and the legitimate interests of our Company constitute the legal basis for such practices. In addition to employees, visitors and other categories of individuals who access the internet through the Company's systems may also fall within the scope of such processing activities.
- Vehicle tracking systems may be implemented in Company vehicles for purposes such as security and the more effective management of vehicles and personnel. Although such processing activities are based on the legitimate interests of our Company, they are carried out with due care to ensure that employees' fundamental rights and freedoms are not adversely affected.
- For the purpose of ensuring the implementation of the Company's human resources policies, personal data are processed in order to recruit suitable candidates for open positions in line with such policies; to conduct human resources operations; to carry out candidate selection processes; to manage personnel records; to plan training and career development; and to fulfill obligations and take necessary measures within the scope of occupational health and safety.
- Personal data of supplier and subcontractor employees may also be processed by our Company. In this respect, Law No. 6331 on Occupational Health and Safety sets out the documents and information that the principal employer is required to verify regarding employees coming from other workplaces. Similarly, the Turkish Labor Law No. 4857 and the Social Insurance and General Health Insurance Law No. 5510 impose obligations on principal employers with respect to subcontractor and temporary workers and specify matters subject to verification. Accordingly, the processing of personal data of employees working at our workplace under suppliers or other

employers is based primarily on compliance with such legal requirements and the fulfillment of legal obligations, as well as the legitimate interests of our Company.

Personal data are also processed by our relevant departments for the following purposes:

- Conducting emergency management processes
- Managing information security processes
- Conducting audit and ethics activities
- Conducting training and development activities
- Managing access authorization processes
- Ensuring compliance of activities with applicable legislation
- Conducting finance and accounting operations
- Managing customer loyalty processes related to the Company's products and services
- Ensuring physical premises security
- Managing assignment and delegation processes
- Monitoring and conducting legal affairs
- Conducting internal audit, investigation, and intelligence activities
- Conducting communication activities
- Managing goods and services production and operational processes
- Managing customer relations processes
- Conducting customer satisfaction activities
- Organization and event management
- Conducting marketing analysis activities
- Managing performance evaluation processes
- Conducting advertising, campaign, and promotion activities
- Managing risk management processes
- Conducting retention and archiving activities
- Conducting social responsibility and civil society activities
- Managing contract processes
- Conducting sponsorship activities
- Conducting strategic planning activities
- Managing and responding to requests and complaints
- Ensuring the security of movable assets and resources
- Managing supply chain management processes
- Conducting marketing processes for products and services
- Ensuring the security of data controller operations
- Managing work permit and residence permit procedures for foreign employees
- Conducting investment processes
- Providing information to authorized persons, institutions, and organizations
- Conducting management activities
- Creating and maintaining visitor records

SECTION 4: RETENTION, DELETION, DESTRUCTION, AND ANONYMIZATION OF PERSONAL DATA

In accordance with Article 138 of the Turkish Penal Code and Article 7 of the Turkish Personal Data Protection Law No. 6698 ("Law"), although personal data may have been processed in compliance with the applicable legislation, such data are deleted, destroyed, or anonymized—either ex officio by our Company or upon the request of the data subject—where the reasons requiring their processing cease to exist.

I. RETENTION OF PERSONAL DATA AND RETENTION PERIODS

Where retention periods are prescribed under applicable laws and regulations, our Company retains personal data for the periods specified therein. Where no specific retention period is stipulated under the legislation, personal data are retained for the period required by the purpose of processing, taking into account our Company's practices and the customary practices of commercial life in connection with the services provided, and are subsequently deleted, destroyed, or anonymized.

Where the purpose of processing has expired and the retention periods prescribed under applicable legislation and determined by our Company have also elapsed, personal data may be retained solely for the purposes of constituting evidence in potential legal disputes or enabling the establishment, exercise, or defense of a right related to the personal data. In determining such retention periods, statutory limitation periods applicable to the assertion of the relevant right and prior similar claims made against our Company are taken into consideration. During such periods, personal data retained are not accessed for any other purpose and are accessed only where necessary for use in the relevant legal dispute. Upon the expiration of these periods, personal data are deleted, destroyed, or anonymized.

II. DELETION, DESTRUCTION, AND ANONYMIZATION OF PERSONAL DATA

In accordance with Article 138 of the Turkish Penal Code and Article 7 of the Law, although personal data may have been processed lawfully, such data are deleted, destroyed, or anonymized—either ex officio by our Company or upon the request of the data subject—where the reasons requiring their processing cease to exist. Our Company fulfills this obligation through the methods explained in this section.

1. Deletion of Personal Data

A) Deletion Process

Where the reasons requiring processing cease to exist, personal data may be deleted by our Company ex officio or upon the request of the data subject. Deletion refers to the process of rendering personal data inaccessible and unusable for the relevant users in any manner whatsoever. Our Company implements all necessary technical and administrative measures to ensure that deleted personal data cannot be accessed or reused by relevant users.

B) Deletion Procedure

The deletion of personal data is carried out in accordance with the following steps:

Identification of personal data subject to deletion;

- Identification of relevant users for each personal data set by using access authorization and control matrices or similar systems;
- Determination of the access, retrieval, and reuse rights and methods of the relevant users;
- Removal and elimination of such access, retrieval, and reuse rights and methods of the relevant users with respect to the personal data.

C) Methods of Deletion

As personal data may be stored in different recording environments, deletion is carried out using methods appropriate to the relevant recording environment.

2. Destruction of Personal Data

A) Destruction Process

Where the reasons requiring processing cease to exist, personal data may be destroyed by our Company ex officio or upon the request of the data subject. Destruction refers to the process of rendering personal data permanently inaccessible, irretrievable, and unusable by anyone. Our Company takes all necessary technical and administrative measures regarding the destruction of personal data.

B) Methods of Destruction

For the destruction of personal data, all copies of the data are identified, and the systems containing such data are individually destroyed.

3. Anonymization of Personal Data

A) Anonymization Process

Anonymization refers to the process by which personal data are rendered incapable of being associated with an identified or identifiable natural person, even when matched with other data. Where the reasons requiring processing cease to exist, our Company may anonymize personal data processed lawfully. Anonymization is carried out by ensuring that personal data cannot be associated with an identified or

identifiable natural person through any technical means, including reverse engineering or matching with other data, taking into account the relevant recording environment and processing activities. Our Company takes all necessary technical and administrative measures to anonymize personal data.

In accordance with Article 28 of the Law, anonymized personal data may be processed for purposes such as research, planning, and statistics. Such processing activities fall outside the scope of the Law, and explicit consent of the data subject is not required.

B) Methods of Anonymization

Anonymization involves the removal or alteration of all direct and/or indirect identifiers within a dataset to prevent the identification of a specific individual or to eliminate distinguishability within a group or crowd in a manner that cannot be associated with a natural person. Data that do not point to a specific individual as a result of such measures are considered anonymized data. The objective of anonymization is to sever the link between the data and the individual identified by such data. Methods such as grouping, masking, derivation, generalization, and randomization—applied through automated or non-automated means to records within a data recording system—are referred to as anonymization techniques. Data obtained through the application of such techniques must not enable the identification of a specific individual.

SECTION 5: RIGHTS OF DATA SUBJECTS

I. SCOPE AND EXERCISE OF DATA SUBJECT RIGHTS

1. Rights of Data Subjects

Individuals whose personal data are processed by our Company have the following rights:

- To learn whether their personal data are processed;
- To request information if their personal data have been processed;
- To learn the purpose of processing personal data and whether such data are used in accordance with their purpose;
- To know the third parties to whom personal data are transferred domestically or abroad;
- To request the correction of personal data if they are processed incompletely or inaccurately and to request notification of such correction to third parties to whom personal data have been transferred;
- To request the deletion or destruction of personal data where the reasons requiring processing cease to exist, despite having been processed in accordance with the Law and other applicable legislation, and to request notification of such actions to third parties to whom personal data have been transferred;
- To object to the occurrence of a result against the data subject arising from the analysis of personal data exclusively through automated systems;
- To request compensation for damages incurred due to unlawful processing of personal data.

2. Exercise of Data Subject Rights

Pursuant to paragraph (1) of Article 13 of the Law, data subjects may submit their requests regarding the exercise of the above-mentioned rights to our Company through the methods specified below, which shall be sufficient and valid for this purpose:

(Submission methods to be listed in the following section.)

Application Method	Address to Which the Application Will Be Submitted	Information to Be Specified in the Application Submission
In-Person Application (Application by the data subject appearing in person and verifying identity with an official identification document)	Huzur Mahallesi Azerbaycan Caddesi No:4 D3-Blok Daire: 317 34415 Seyrantepe Sarıyer / İstanbul	The envelope must be clearly marked with the phrase: “Information Request Within the Scope of the Personal Data Protection Law”
Notification via Notary Public	Huzur Mahallesi Azerbaycan Caddesi D Blok No: 4D/3 İç Kapı No: 317 34485 Sarıyer/İstanbul	The notification envelope must be clearly marked with the phrase: “Information Request Within the Scope of the Personal Data Protection Law”
Via Registered Electronic Mail (KEP) signed with a “Secure Electronic Signature	dcsdijital@hs03.kep.tr	The subject line of the e-mail must include the phrase: “Personal Data Protection Law – Information Request”

Requirements for Submitting an Application

In the application, the following information must be included:

Name and surname, and signature if the application is submitted in writing;
Turkish Identification Number for Turkish citizens; nationality and passport number or, if available, identification number for foreign nationals;
Residential address or workplace address for notification purposes;
Electronic mail address (if any) for notification purposes;
Telephone and fax number (if any);
Subject of the request.

Relevant information and documents relating to the request must also be attached to the application.

As a rule, requests may not be submitted by third parties on behalf of the data subject. For a request to be submitted by a person other than the data subject, a special power of attorney issued by the data subject specifically authorizing the applicant must be provided.

In applications submitted to exercise data subject rights, the request must be clear and explicit; the subject of the request must relate to the data subject or, where acting on behalf of another person, the applicant must be expressly authorized and such authorization must be documented; the application must include identity and address information; and documents verifying the applicant’s identity must be attached.

The Data Subject Application Form is available on our Company’s website.

3. Responding to Applications

Where the data subject submits their request to our Company in accordance with the prescribed procedure, our Company shall finalize the request free of charge as soon as possible and no later than thirty (30) days, depending on the nature of the request. However, where the processing of the request requires additional costs, the fee determined by the Personal Data Protection Board may be charged to the applicant.

Our Company may request additional information from the applicant in order to verify whether the applicant is the relevant data subject. Our Company may also ask questions to the data subject to clarify

matters stated in the application. Applications are managed within our Company in accordance with the Data Subject Application Procedure.

SECTION 6: ENSURING THE SECURITY OF PERSONAL DATA

I. TECHNICAL AND ADMINISTRATIVE MEASURES TAKEN TO ENSURE THE LAWFUL PROCESSING OF PERSONAL DATA

Our Company takes all necessary technical and administrative measures to ensure the lawful processing of personal data. Within this scope:

- A Data Inventory compliant with the VERBİS system is prepared (data mapping), and compliance audits regarding lawfulness and purpose limitation are carried out.
- In order to ensure that the obligation to inform data subjects is fulfilled fully and accurately, the Policy on Information Notices in the Processing of Personal Data has been adopted and implemented.
- Employees are informed and trained on personal data protection legislation and the lawful processing of personal data.
- All activities carried out by our Company are analyzed in detail on a departmental basis, and as a result of such analysis, personal data processing activities specific to each business unit are identified.
- The requirements necessary to ensure compliance of personal data processing activities carried out by our Company's business units with the conditions set out under Law No. 6698 are determined specifically for each business unit and its detailed activities.
- Clauses imposing obligations not to process, disclose, or use personal data—except in accordance with Company instructions and statutory exceptions—are included in contracts and documents governing the legal relationship between our Company and its employees; employee awareness is ensured in this regard, and audits are conducted.
- Similar clauses imposing obligations not to process, disclose, or use personal data—except in accordance with Company instructions and statutory exceptions—are included in contracts and documents governing the legal relationship between our Company and third parties processing data on behalf of our Company; in this context, the Policy on Confidentiality and Personal Data Protection Principles with Third Parties has been adopted.

II. TECHNICAL AND ADMINISTRATIVE MEASURES TAKEN IN THE PROCESSING OF SPECIAL CATEGORIES OF PERSONAL DATA

Certain personal data are accorded special importance under the Law due to the risk of causing discrimination or harm if processed unlawfully. These include data relating to race, ethnic origin, political opinion, philosophical belief, religion, sect or other beliefs, attire, membership of associations, foundations or trade unions, health, sexual life, criminal convictions and security measures, as well as biometric and genetic data.

Our Company acts with heightened diligence in the protection of special categories of personal data classified under the Law and processed lawfully. Within this scope, the technical and administrative measures taken for the protection of personal data are applied with particular care to special categories of personal data, and necessary audits are carried out.

Accordingly:

- A Policy on the Processing of Special Categories of Personal Data has been prepared to regulate the security and processing principles applicable to such data.
- Employees involved in the processing of special categories of personal data receive regular training on the Law, related regulations, and special data security; confidentiality agreements are executed; access authorizations, scopes, and durations for users with access rights are clearly defined; authorization controls are performed; and access rights of employees who change roles or leave employment are immediately revoked, with Company-issued inventories being collected.

- Where special categories of personal data are processed, stored, or accessed in electronic environments, data are protected using cryptographic methods; cryptographic keys are stored securely and in separate environments; all actions performed on the data are securely logged; security updates for the relevant environments are monitored; and necessary security tests are conducted and recorded.
- Where access to data is provided through software applications, user authorizations are implemented; security tests of such software are conducted regularly and recorded; and where remote access is required, at least two-factor authentication is ensured.
- Where special categories of personal data are processed, stored, or accessed in physical environments, adequate physical security measures are taken depending on the nature of the environment (against risks such as electrical leakage, fire, flooding, theft, etc.), and unauthorized access is prevented.
- Where special categories of personal data are transferred via e-mail, such transfers are carried out in encrypted form using corporate e-mail addresses or Registered Electronic Mail (KEP) accounts.
- Where special categories of personal data are transferred via storage media such as USB drives, CDs, or DVDs, data are encrypted using cryptographic methods and cryptographic keys are stored separately.
- Where special categories of personal data are transferred between servers located in different physical environments, data transfers are carried out via VPN connections or sFTP methods. Where transfer in paper format is required, necessary measures are taken against risks such as theft, loss, or unauthorized access, and documents are sent as confidential documents.
- In addition to the measures listed above, the technical and administrative measures recommended in the Personal Data Security Guide published on the website of the Personal Data Protection Authority are also taken into consideration to ensure an adequate level of security.