ES GROUP DENİZCİLİK SAN. VE TİC. A.Ş.

POLICY ON PROTECTION AND PROCESSING OF PERSONAL DATA

Version 1

TABLE OF CONTENTS

I. Introduction

II. Policy Owner

III. Purpose

IV. Scope

V. Update

VI. Definitions

VII. Roles and Responsibilities

1. Data Officer
2. Data Controller Contact Person
3. Senior Management of the Data Controller

VIII. Approval

IX. Data Subjects

X. Data Categories

XI. Activities and Purposes for Processing and Sharing Personal Data

XII. Measures Taken When Transferring Data to Third-Party Service Providers

XIII. Data Protection Policies and Procedures

XIV. Risk Analysis

XV. Cases Outside the Policy

XVI. Principles of Personal Data Processing

XVII. Conditions for Processing Personal Data

XVIII. Obligations of the Data Controller

I. Introduction

This Policy sets out the principles and rules adopted by ES GROUP DENİZCİLİK SAN. VE TİC. A.Ş. (Data Controller) with regard to the collection, processing, transfer, updating and destruction of personal data within the framework of the Personal Data Protection Law No. 6698 (Law) and related national legislation.

II. Policy Owner

The owner of the Policy on Protection and Processing of Personal Data is ES GROUP DENİZCİLİK SAN. VE TİC. A.Ş. in its capacity as the Data Controller.

III. Purpose

The purpose of this Policy is to set out the rules adopted by the Data Controller regarding personal data processing activities and protection of personal data; and to inform and ensure transparency for data subjects whose personal data are processed by our company, including our business partners, current and prospective employees, current and potential customers, company shareholders, visitors and third parties.

IV. Scope

The Data Controller covers its shareholders and partners, employees, prospective employees, interns, subcontractors, suppliers, current and potential customers, visitors and third parties whose personal data are processed.

V. Update

The Policy on Protection and Processing of Personal Data shall be reviewed and recorded once a year, regardless of whether changes in its content are required due to corporate or legal reasons. The most current version shall be published on the Data Controller's website.

VI. Definitions

Definitions not included herein shall be used as defined in the Law and secondary regulations.

- Explicit Consent: Consent related to a specific subject, based on information and expressed with free will.
- Anonymisation: Rendering personal data impossible to associate with an identified or identifiable natural person in any way, even when matched with other data.
- Obligation to Inform (Clarification Obligation): The obligation of the Data Controller to inform the persons whose personal data it processes, regarding by whom, for which purposes and on which legal grounds their data may be processed, and to whom and for which purposes they may be transferred.
- Data Subject: The natural person whose personal data is processed.
- Personal Data: Any information relating to an identified or identifiable natural person. Data such as a person's name, surname, date and place of birth, physical, familial, economic and other characteristics, name, telephone number, vehicle plate, social security number and passport number constitute personal data.

- Processing of Personal Data: Any operation performed on personal data such as collection, recording, storage, preservation, alteration, reorganisation, disclosure, transfer, retrieval, making available, classification or blocking of use, whether fully or partly automated or non-automated where part of a data filing system.
- Special Categories of Personal Data: Data relating to an individual's race, ethnic origin, political opinion, philosophical belief, religion, sect or other beliefs, physical appearance, membership of associations, foundations or trade unions, health, sexual life, criminal conviction and security measures, and biometric and genetic data.
- Data Processor: Natural or legal persons outside the organisation of the Data Controller who process personal data on behalf of the Data Controller based on the authority granted by the Data Controller. These persons process personal data within the scope of instructions given to them and are a separate natural or legal person authorised by the Data Controller through a data processing agreement. Any natural or legal person may be both a Data Controller and a Data Processor at the same time.
- Data Controller: The natural or legal person who determines the purposes and means of processing personal data and is responsible for establishing and managing the data filing system.
- Registry of Data Controllers (VERBİS): A publicly accessible registration system maintained by the Presidency of the Personal Data Protection Authority (Authority), in which those who are Data Controllers pursuant to the Personal Data Protection Law No. 6698 are required to register.

VII. Roles and Responsibilities

Four complementary roles have been defined within the scope of the Policy on Protection and Processing of Personal Data.

1. Data Officer

Two "Data Officers" — one primary and one alternate — are appointed for the Data Controller. The Data Officer has the following responsibilities:

1. To create a detailed personal data processing inventory together with all employees of the Data Controller and coordinate related activities.
2. To monitor changes and amendments in data processing activities and keep the inventory up to date.
3. To communicate potential changes to the Data Controller Contact Person.
4. To perform the duties and procedures specified in company policies, procedures and instructions.

2. Data Controller Contact Person

A "Data Controller Contact Person" is appointed for each Data Controller. The responsibilities of the Data Controller Contact Person are as follows:

5. To be aware of all processes and activities regarding the protection of personal data within the Data Controller.

6. To represent the Data Controller in formal and internal audit processes, to take and finalise the required actions.
7. To respond to applications from data subjects.
8. To inform company management and the Legal Department in the event of a data breach.
9. To monitor changes and amendments in data processing activities reported by the Data Controller and related units within the scope of responsibilities, together with the Data Officer, and to keep the inventory up to date.
10. To notify the Authority through VERBİS of any changes in the information registered in VERBİS within seven days of the change.
11. To ensure communication with the Authority.
12. To make required legal notifications in the event of a data breach in accordance with applicable procedures.
13. To perform the duties and procedures specified in company policies, procedures and instructions.

3. Senior Management of the Data Controller

14. The responsibility of the Senior Management of the Data Controller (Chairman of the Board, General Manager, etc.) is to supervise the Data Controller Contact Person in fulfilling their duties as described in the Law.
15. Changes and appointments of the Data Controller Contact Person and Data Officer shall be made by the Senior Management of the Data Controller upon termination of the employment contract, and the relevant departments shall be notified.

VIII. Approval

The Policy is approved by the relevant senior management representatives on behalf of the Data Controller.

IX. Data Subjects

Personal data of the following natural persons are processed: job applicants, employees, persons mentioned in news items, shareholders/partners, potential product or service recipients, interns, supplier employees, supplier authorised persons, product or service recipients, legal guardians/representatives and visitors, etc.

X. Data Categories

The following categories of data are processed in accordance with the purposes of personal data processing: identity, contact, location, personnel, legal transaction, customer transaction, physical space security, transaction security, risk management, finance, professional experience, marketing, visual and audio records, philosophical belief, religion, sect and other beliefs, association membership, health information, criminal conviction and security measures, and biometric data.

XI. Activities and Purposes for Processing and Sharing Personal Data

Personal data are processed and shared for the following purposes: conducting emergency management processes; managing information security processes; conducting employee satisfaction and engagement processes; fulfilling employment contract and statutory obligations for employees; conducting benefit and employee rights processes; conducting audit and ethics activities; conducting training activities; managing access authorisations; ensuring regulatory compliance of activities; conducting finance and accounting operations; ensuring physical premises security; conducting assignment processes; monitoring and conducting legal affairs; conducting internal audit, investigation and intelligence activities; conducting communication activities; planning human resources processes; managing and auditing business activities; conducting occupational health and safety activities; receiving and evaluating suggestions for improvement of business processes; conducting business continuity activities; conducting logistics activities; managing goods/service procurement processes; managing goods/service sales processes; managing goods/service production and operations processes; managing events and organisational activities; conducting performance appraisal processes; conducting advertising, campaign and promotional processes; conducting risk management processes; conducting storage and archiving activities; conducting social responsibility and civil society activities; managing contract processes; conducting strategic planning activities; monitoring requests and complaints; ensuring security of movable assets and resources; implementing remuneration policies; ensuring security of Data Controller operations; processing work and residence permits for foreign personnel where applicable; informing authorised persons, institutions and organisations; conducting management activities.

XII. Measures Taken When Transferring Data to Third-Party Service Providers

Provisions regarding the protection of personal data are added to contracts and annexes concluded with third-party service providers; separate confidentiality agreements are executed; additional undertakings or protocols are arranged; and such service providers are audited to verify that personal data are adequately protected.

XIII. Data Protection Policies and Procedures

This Policy sets out the general conditions for the protection and processing of personal data within the Data Controller.

16. The "Personal Data Retention and Disposal Policy" contains the rules and procedures for storage and disposal of personal data within the Data Controller.
17. The "Policy on Processing and Protection of Special Categories of Personal Data" contains the rules and procedures governing specific conditions and methods for processing special categories of personal data within the Data Controller.
18. The "Policy on Protection and Processing of Employee Personal Data" contains the rules and procedures governing the conditions and methods for protection and processing of personal data belonging to persons employed within the Data Controller.
19. The "Information Systems General Standards and Security Policy" aims to ensure the security and confidentiality of information and data in all commercial and operational electronic, written or other media; and determines the general principles regarding the processing of personal data for employees.

20. Clarification and explicit consent texts are used to inform data subjects and to ensure that personal data processing is conducted in accordance with the Law.
21. Internal training sessions are conducted to raise awareness among employees about the Law.
22. The "Data Subject Request Management Procedure" establishes the rules and conditions for investigating requests from data subjects, responding to such requests and taking the necessary actions.
23. Personal data processing activities within the Data Controller are audited on a regular basis.

XIV. Risk Analysis

Risk findings arising from regular audits conducted by the Data Controller's audit unit are evaluated. The Senior Management and Contact Person of the Data Controller are informed of the necessary actions to be taken or processes to be changed, and required measures are ensured.

XV. Cases Outside the Policy

Should practices different from those described in this Policy be identified, the persons making such identification shall obtain support from the Data Controller Contact Person and Data Officers and shall notify Senior Management and the Legal Department in writing.

XVI. Principles of Personal Data Processing

In order to ensure compliance with the Law, personal data are processed in accordance with the general principles and provisions set out in the legislation. In this context, the Data Controller acts in accordance with the following principles when processing personal data:

1. Lawful and Fair Processing

The Data Controller acts in accordance with the law and principles of fairness in personal data processing activities.

2. Accuracy and Up-to-Date Data

The Data Controller establishes the necessary systems to ensure that the personal data it processes are accurate and current, taking into account the fundamental rights of data subjects and its own legitimate interests.

3. Processing for Specified, Explicit and Legitimate Purposes

The Data Controller determines the purposes for which personal data will be processed and communicates these purposes to data subjects before processing. Personal data shall not be processed for purposes other than the specified legitimate and lawful purposes.

4. Relevant, Limited and Proportionate Processing

The Data Controller processes personal data in a manner appropriate to the purposes and refrains from processing personal data that are not related to or not needed for achieving the purpose.

Proportionality requirements are taken into account and personal data are not used beyond the processing purpose.

5. Retention for the Period Stipulated by Law or Required for the Purpose

The Data Controller first determines whether a retention period is stipulated in the relevant legislation for personal data. If a period is specified, it complies with that period. If no period is specified, it retains personal data for as long as necessary for the purpose for which they are processed.

6. Building Entry and Internal Personal Data Processing Activities, and Network and Website Users

For the purpose of ensuring security, the Data Controller carries out personal data processing activities involving CCTV monitoring and tracking visitor entry/exits at its buildings and premises. CCTV footage of visitors and all data subjects at building and premises entrances is recorded. The CCTV monitoring activities aim to improve service quality, ensure reliability, protect the security of the Data Controller, customers and third parties, and safeguard customer interests. CCTV monitoring is conducted in compliance with the Law and Law No. 5188 on Private Security Services and related legislation. Technical and administrative measures are taken to ensure the security of personal data obtained through CCTV monitoring. Internet access may be provided to visitors upon request during their stay in the buildings and premises. In such cases, internet access logs are recorded in accordance with Law No. 5651 and related regulations, and these logs are processed only when requested by authorised public authorities or for legal compliance purposes in internal audits. Access to digitally recorded and stored data is limited to authorised personnel only. Log records are saved with timestamps to ensure immutability and are retained with limited authorised personnel access.

7. Processing of Customer and Business Partner Data

Personal data of customers and business partners may be processed to the extent necessary for the purposes set out above. Personal data of existing and potential customers and business partners (or authorised representatives where the partner is a legal entity) may be processed without obtaining separate consent in relation to the establishment, performance and termination of a contract. Prior to contract formation, personal data may be processed to prepare offers, procurement forms or to meet the data subject's requests related to contract performance. Personal data may be processed without consent where explicitly stipulated by law or for fulfilling a legal obligation. Special categories of personal data are processed within the framework of the Law, subject to taking adequate measures as determined by the Authority, and with the data subject's explicit consent where no statutory exception applies.

8. Processing of Employee and Job Applicant Data

The rules and procedures governing the conditions and methods for protection and processing of personal data belonging to persons employed within the Data Controller are set out in the "Policy on Protection and Processing of Employee Personal Data". Collection and processing of employee personal data is necessary throughout the process from establishment to termination of the employment contract, and separate explicit consent may not be required. Personal data of prospective job applicants are also processed during job applications. In case of rejection of the application, personal data obtained during the application process are retained for the applicable

retention period and subsequently deleted, destroyed or anonymised. Employee personal data may be processed without separate consent where explicitly stipulated by law or for fulfilling a statutory obligation or where there is a legitimate interest of the Data Controller, provided that such processing is proportionate and does not infringe upon the employee's protected rights. Special categories of personal data may only be processed under specific conditions as defined by the Law.

XVII. Conditions for Processing Personal Data

1. Identification and Processing of Personal Data

Pursuant to the Law, personal data is defined as "any information relating to an identified or identifiable natural person." The concept of personal data is not limited to information that allows the identification of persons such as name, surname, place of birth and date of birth, but also encompasses all physical, social, cultural, economic and psychological information. In addition to identity information, all information that renders a person identifiable, such as national identification number, tax number, passport number, social security number, driver's licence number, vehicle plate, home address, work address, email address, telephone number, fax number, curriculum vitae, photograph, video, genetic information, blood type, criminal and judicial records, also constitutes personal data. The Data Controller identifies whether all data it collects, including from business partners, employees, customers and other third parties, falls within the scope of personal data, and processes such data in accordance with the Law.

2. Exceptional Cases

The Data Controller processes personal data with the explicit consent of data subjects pursuant to the Law. However, in the presence of any of the following conditions, personal data may be processed without seeking explicit consent:

24. Where explicitly stipulated by law (tax legislation, labour legislation, commercial legislation, etc.).
25. Where processing is necessary for the establishment or performance of a contract to which the data subject is party (employment contract, sales contract, transport contract, work contract, etc.).
26. Where processing is mandatory for the protection of life or physical integrity of the person themselves or another person who is unable to express their consent due to actual impossibility or whose consent is not legally valid.
27. Where processing is mandatory for the Data Controller to fulfil its legal obligation (financial audits, security legislation, sectoral regulatory compliance, etc.).
28. Where the personal data has been made public by the data subject themselves.
29. Where data processing is mandatory for the establishment, exercise or protection of a right (litigation, registration procedures, land registry transactions, etc.).
30. Where data processing is mandatory for the legitimate interests of the Data Controller, provided that it does not infringe the fundamental rights and freedoms of the data subject.

3. Processing of Special Categories of Personal Data

Certain personal data are designated as "special categories of personal data" under the Law. The Data Controller does not process such data without the data subject's explicit consent. "Explicit

consent" means consent relating to a specific subject, based on information and expressed with free will. The Law lists the following as special categories of personal data: race, ethnic origin, political opinion, philosophical belief, religion, sect or other beliefs, physical appearance, membership of associations, foundations or trade unions, health, sexual life, criminal conviction and security measures, and biometric and genetic data. The Data Controller shall also take adequate measures as determined by the Personal Data Protection Board (Board) when processing special categories of personal data. The Data Controller may process special categories of personal data only in the following circumstances: (1) with the explicit consent of the data subject; (2) as stipulated by law (for categories other than health and sexual life, without explicit consent where provided by law); (3) for public health purposes; (4) where processing is mandatory for the protection of life or physical integrity of a person unable to give consent; (5) where it relates to personal data made public by the data subject and in accordance with the intent to make it public; (6) where mandatory for the establishment, exercise or protection of a right; (7) where mandatory for fulfilling legal obligations in the fields of employment, occupational health and safety, social security, social services and social assistance; (8) where it concerns foundations, associations and other non-profit organisations or entities established for political, philosophical, religious or trade union purposes, in accordance with applicable legislation and their purposes, limited to their field of activity, not to be disclosed to third parties, and relating to their current or former members.

4. Conditions for Transfer of Personal Data

The Data Controller may transfer personal data to third parties, having taken the necessary security measures in line with lawful personal data processing purposes, subject to meeting the conditions (legal bases) set out in Articles 5(2) and 6(3) of the Law, or with the explicit consent of the data subject. The Data Controller may also transfer personal data to third parties without seeking explicit consent where the conditions for data processing set out in the Law are met. The Data Controller takes the necessary administrative and technical measures to ensure that transfers made without explicit consent are compliant with the restrictions set out in the Law.

XVIII. Obligations of the Data Controller

1. Obligation to Inform Data Subjects (Clarification Obligation)

The Data Controller informs data subjects on the following matters at the time personal data is collected:

1.1. Identity of the Data Controller and, if any, its representative

1.2. The purposes for which personal data will be processed

1.3. The parties to whom and the purposes for which personal data may be transferred

1.4. The method and legal basis for collection of personal data

1.5. The rights of the data subject under Article 11 of the Law

In fulfilment of this obligation, the Data Controller informs data subjects through a prepared clarification text. Clarification is provided at the time of first contact with the data subject. Where personal data is not obtained directly from the data subject, clarification is provided within a reasonable period from collection; at the time of first communication where data will be used for communication; or at the time of first transfer where data is to be transferred.

2. Obligation to Respond to Data Subject Applications

Data subjects may apply to the Data Controller in writing or through other methods determined by the Board pursuant to the Law, to request information. The Data Controller responds to applications pursuant to Article 13 of the Law in order to assess the rights of data subjects and provide necessary information. The Data Controller is entitled to accept or refuse applications with justification and responds in a timely and reasoned manner. Data subjects may lodge a complaint with the Board within 30 days of learning the response, or in any case within 60 days of the application date, if their application is rejected, the response is deemed insufficient or no response is provided. The rights of data subjects are: (1) to learn whether personal data has been processed; (2) to request information if processed; (3) to learn the purpose of processing and whether data is used for that purpose; (4) to know third parties to whom data is transferred domestically or abroad; (5) to request correction of incomplete or incorrect data; (6) to request deletion or destruction; (7) to request notification of such operations to third parties to whom data was transferred; (8) to object to results arising from automated processing systems that are detrimental to the data subject; and (9) to claim compensation for damages arising from unlawful processing.

3. Obligation to Ensure Security of Personal Data

The Data Controller takes the necessary technical and administrative measures to prevent unlawful processing of and access to personal data it processes and to ensure the preservation of such data. The Data Controller establishes systems for conducting and having conducted necessary audits of the functioning of these measures. In the event that personal data is obtained by others through unlawful means, the Data Controller notifies the Board within 72 hours and notifies affected data subjects directly or through its website as soon as reasonably possible.

4. Technical and Administrative Measures to Ensure Lawful Data Processing

All processes relating to personal data processing activities carried out by business units within the Data Controller are compiled and analysed in the personal data processing inventory. Legal compliance audits are conducted for all activities from collection to deletion of data by business units. Personal data processing activities are monitored through established technical systems. The Data Controller informs and trains employees on data protection law and lawful processing of personal data. Provisions prohibiting unlawful processing, disclosure and use of personal data are included in contracts governing legal relationships between the Data Controller and its business partners, employees and customers.

5. Technical and Administrative Measures to Prevent Unlawful Access to Personal Data

The Data Controller takes the necessary administrative and technical measures appropriate to the nature of the data to be protected, to prevent unlawful acquisition, disclosure, viewing and transfer of personal data. Technical measures appropriate to technological developments are taken and updated periodically. Access and authorisation technical processes are designed and implemented in accordance with legal compliance requirements. The Data Controller ensures that employees sign the "Information Systems General Standards and Security Policy" to confirm that they will not disclose or use personal data in violation of the Law. Data protection provisions are added to contracts with parties to whom personal data is transferred.

6. Obligation to Register with the Registry of Data Controllers (VERBİS)

The Data Controller registers with the Registry of Data Controllers by submitting the required information and documents within the period announced by the Board before commencing data processing. Information to be declared to VERBİS includes: (1) identity and address of the Data Controller representative; (2) purposes for which personal data will be processed; (3) descriptions of the groups of data subjects and data categories; (4) recipient or recipient groups to whom personal data may be transferred; (5) personal data planned to be transferred to foreign countries; (6) measures taken for personal data security; and (7) maximum retention period required for the purposes of processing.

7. Deletion, Destruction and Anonymisation of Personal Data

Pursuant to Article 138 of the Turkish Penal Code and Article 7 of the Law, where the reasons requiring processing of personal data cease to exist, even if the data has been processed lawfully, the Data Controller shall delete, destroy or anonymise such data upon its own decision or upon the request of the data subject. The Data Controller takes the technical and administrative measures set out in detail in the "Personal Data Retention and Disposal Policy", develops the necessary operational mechanisms, and trains, assigns and raises awareness among relevant business units.