PRIVACY POLICY

Categorization: **Restricted**

TABLE OF CONTENT

1. PURPOSE 4
2. SCOPE 4
3. DEFINITIONS 4
4. BRIEF SUMMARY OF PERSONAL DATA PROTECTION LAW 6
5. BASIC PRINCIPLES 6
5.1 PRINCIPLE 1: Responsibility 6
5.2 PRINCIPLE 2: Setting Objectives 7
5.3 PRINCIPLE 3: Explicit Consent 7
5.4 PRINCIPLE 4: Limited Data Collection 7
5.5 PRINCIPLE 5: Limited Processing and Storage 8
5.6 PRINCIPLE 6: Erasure, Destruction and Anonymization 8
5.7 PRINCIPLE 7: Measures 8
5.8 PRINCIPLE 8: Access to Information by Data Subjects 8
6. PERSONAL DATA 8
6.1 All Information About a Person 9
6.2 Identified or identifiable 9
6.3 Natural Person 9
6.4 Special Categories of Personal Data 9
7. LEGAL BASIS 9
7.1 Basic Principles of Processing Personal Data 10
7.2 Conditions for Processing Personal Data 10
7.3 Disclosure 11
7.4 Explicit Consent and Exceptions 11
8. PERSONAL DATA RETENTION TIME LIMIT 12
8.1 What is the erasure of personal data? 13
8.2 What is the destruction of personal data? 14
8.3 What is the anonymization of personal data? 15
9. TRANSFER OF PERSONAL DATA (DOMESTIC and INTERNATIONAL) 15
9.1 Domestic Transfer of Personal Data 15
9.2 International Transfer of Personal Data 17
10. DATA CONTROLLER AND DATA PROCESSOR 18
10.1 Data Controller 18
10.2 Data Processor 19
11. DATA CONTROLLERS' REGISTRY (VERBIS) 19
12. OBLIGATIONS OF THE DATA CONTROLLER 21
12.1 Data controller's disclosure obligation 21
12.2 Obligations regarding data security 21
13. SECURITY OF PERSONAL DATA 22
13.1 Identification of Risks 22
13.2 Implementation of Administrative and Technical Security Measures 22
13.3 Risk and Security Level Controls and Assessments 22
14. TECHNICAL AND ADMINISTRATIVE MEASURES 23

15. DATA BREACH 23
16. RIGHTS OF THE DATA SUBJECT 24
16.1 Application to the Data Controller 24
16.2 Complaint to the Board 25
17. CONTRACTS 25
17.1 Personal Data Processing Protocols 25
18. PRIVACY IMPACT ASSESSMENT (PIA) 25
19. BIG DATA, PUBLIC DATA, AND SOCIAL MEDIA 26
19.1 What is big data? 26
19.2 What is public data? 27
19.3 What is social media? 27
20. PUBLISHING AND STORAGE OF THE POLICY 27
21. UPDATE PERIOD OF THE POLICY 27
22. EFFECTIVENESS AND WITHDRAWAL OF THE POLICY 27
23. OTHER PROVISIONS 28
24. APPENDICES 28
Annex 1. Legislation, Policy, and Guidelines 28
Annex 2. Personal Data Processing Inventory 28

1. PURPOSE

The purpose of this Privacy Policy ("Policy") is to explain the basic principles, legal bases and responsibilities taken as basis when processing personal data in Eureko Insurance Inc. (ES; Company) and to specify the operation, process and responsibilities carried out to ensure data security and confidentiality in this respect.
The Policy is a declarative document that provides information about some or all of the ways of collecting, storing, transferring or processing personal data.

2. SCOPE

Personal data in the Company is used for conducting insurance activities, policy production, execution of insurance premiums (including compensation processes), claims management and policy renewal offers, etc. and other related insurance activities.
In order to protect the privacy of data subjects, great care must be taken to comply with legislation and regulations in the field of processing and protection of personal data. All employees at ES must comply with this Privacy Policy in their daily activities.
This policy is in compliance with the Personal Data Protection Law ("PDPL"), which entered into force on April 7, 2017 on the protection of natural persons in relation to the processing of personal data.

3. DEFINITIONS

The general description of the definitions is in line with the definitions of the Personal Data Protection Law (KVKK, art.3).
Explicit consent: Freely given, specific and informed consent,
Recipient group: The category of natural or legal person to whom personal data is transferred by the data controller,
Anonymization: Rendering personal data impossible to link with an identified or identifiable natural person, even through matching them with other data,
Data subject: The natural person whose personal data is processed,
Data subject group: The category of data subjects whose personal data are processed by data controllers,
Relevant user: Persons who process personal data within the organization of the data controller or in accordance with the authorization and instruction received from the data

controller, except for the person or unit responsible for the technical storage, protection and backup of the data,

Law or PDPL: Law No. 6698 on the Personal Data Protection,

Registration: The notification made by the data controllers under the obligation to register in accordance with the procedures and principles set out by the Regulation,

Registered electronic mail (REM) address: A qualified form of electronic mail that provides legal evidence regarding the use of electronic messages, including their sending and delivery,

Obligation to register: The registration-related obligation that must be fulfilled in accordance with the Regulation,

Personal data: All information relating to an identified or identifiable natural person,

Personal data processing: Any operation which is performed on personal data, such as the collection, recording, storage, alteration, reorganization, disclosure, transfer, acquisition, retrieval, classification or prevention of the use of personal data in whole or in part, provided that the automated means or process is not part of any data recording system

Personal data processing inventory: The inventory that data controllers create by associating the personal data processing activities they carry out depending on their business processes with the purposes of personal data processing, data category, transferred recipient group and data subject group, and detailing the maximum time required for the purposes for which personal data are processed, personal data foreseen to be transferred to foreign countries and the measures taken regarding data security,

Personal data retention and destruction policy: The policy on which data controllers base the process of determining the maximum period necessary for the purpose for which personal data are processed and the process of erasure, destruction and anonymization,

Board: Personal Data Protection Board,

Authority: Personal Data Protection Authority,

Data processor: A natural or legal person who processes personal data on behalf of the data controller upon its authorization,

Data category: A class of personal data in which the data subject group or groups are grouped according to common characteristics,

Data Controllers' Registry Information System (VERBIS): A registry system where personal data are recorded by structuring them according to certain criteria,

Data Controller: The natural or legal person who determines the purpose and means of processing personal data and is responsible for the establishment and management of the data recording system,

Data controller representative: A legal person resident in Turkey or a natural person who is a citizen of the Republic of Turkey authorized to represent non-resident data controllers in the matters specified in the second paragraph of Article 11 of the Regulation on Data Controllers' Registry,

Special categories of personal data: Data relating to race, ethnic origin, political opinions, philosophical beliefs, religion, sect or other beliefs, appearance and dress, membership of associations, foundations or trade unions, health, sexual life, criminal convictions and security measures, and biometric and genetic data,

Policy on the Security of Special Categories of Personal Data: The policy that determines the technical and administrative measures to be taken by the data controller for special categories of personal data,

4. BRIEF SUMMARY OF PERSONAL DATA PROTECTION LAW

Law No. 6698 on the Protection of Personal Data (hereinafter PDPL) was published in the Official Gazette dated 07.04.2016 and numbered 29677.

The purpose of this Law is to protect the fundamental rights and freedoms of individuals, in particular the right to privacy, in the processing of personal data and to regulate the obligations of natural and legal persons who process personal data and the procedures and principles to be followed (Article 1).

The provisions of this Law shall apply to natural persons whose personal data are processed and to natural and legal persons who process such data wholly or partially by automatic means or by non-automatic means, provided that they are part of any data recording system (Article 2).

5. BASIC PRINCIPLES

5.1 PRINCIPLE 1: Responsibility

ES is responsible for ensuring the safeguarding of, and preventing unlawful processing and access to, personal data held by the direct data subject or personal data supplied to ES by a third party or provided by ES to a third party for processing.

ES supports its Privacy Policy with other policies and processes.

5.2 PRINCIPLE 2: Setting Objectives

ES informs the data subjects about the personal data processed, the purpose and lawfulness of the processing activities, personal data transfers and data subject rights before processing personal data or at the latest at the time of processing. According to the conditions specified in the Law, it also obtains explicit consent from the data subject when necessary.

5.3 PRINCIPLE 3: Explicit Consent

Explicit consent may be given verbally or in writing or via electronic media, must be related to a specific subject, must be based on information and must be given with free will. For example, explicit consent for sensitive personal data may be given verbally over the phone following the customer's disclosure, or in writing by signing the explicit consent text transmitted with the disclosure text. ES records the explicit consents given so that they can be easily accessed if necessary.

Personal data subject to the previously given explicit consent continues to be processed by ES within the scope of the previously given explicit consent, unless there is a change in the personal data and processing purposes.

Data subjects may request the processing, transfer, alteration, erasure or destruction of personal data at any time by applying to ES as specified in the Law. However, the data subject should be aware that withdrawal of explicit consent may affect the establishment and performance of the insurance contract. ES responds to data subject applications in the manner set out in the Law.

5.4 PRINCIPLE 4: Limited Data Collection

ES only collects personal data that is sufficient and necessary for the specified processing purposes and uses this information for its legitimate interests or for the services requested by the data subject.

Before personal data is collected, the purposes of personal data processing and the sufficient data set to be used for those purposes are determined (neither too much nor too little).

Where data is no longer necessary for a personal data processing purpose, it is removed from the Personal Data Processing Inventory for that purpose, even if it is necessary to use that data for other personal data processing purposes.

5.5 PRINCIPLE 5: Limited Processing and Storage

ES does not continue to retain and process personal data for purposes other than those for which it was collected, except with the consent of the individual or as required or permitted by law, and retains it only for as long as necessary for those purposes.

5.6 PRINCIPLE 6: Erasure, Destruction and Anonymization

ES erases, destroys or anonymizes personal data within the periodic destruction periods (6 months) after the expiration of the retention periods as specified in the Personal Data Retention and Destruction Policy. The Personal Data Retention and Destruction Policy describes the relevant processes in detail.

5.7 PRINCIPLE 7: Measures

In accordance with its obligations as a data controller under the Law, ES establishes and operates security measures appropriate to the class of personal data and prevents unauthorized activities.

5.8 PRINCIPLE 8: Access to Information by Data Subjects

After receiving a request from data subjects in an appropriate manner, ES informs them of the personal data processing activities concerning them and grants them access to this information. If the data subject wishes to alter their data, ES shall alter the personal data in order to keep it up to date.
Requests for information are received in writing, by e-mail or letter. If all mandatory information is available in the request, ES responds to requests within 30 days in line with the "PDPL Request Process". It is important to verify that the individual requesting information is in fact the person in question.

6. PERSONAL DATA

The concept of "personal data" consists of various elements. A list of examples of personal data is included in Annex 9 'Personal Data Examples'.

6.1 All Information About a Person

Personal data refers to any information relating to an identified or identifiable natural person. This standard covers all situations in which a person is identified as a result of the fact that the person is associated with physical content that expresses his or her physical, economic, cultural, social or psychological identity or is associated with any record, such as an identity, tax, insurance number. Data such as name, telephone number, motor vehicle license plate, passport number are personal data because of their ability to identify a person.

6.2 Identified or identifiable

Personal data includes not only information such as a person's name, surname, date and place of birth, but also data relating to the physical, family, economic, social and other characteristics of the person. The concept of identifiability means that the person's existing data can be associated with any natural person.

6.3 Natural Person

Articles of law apply only to living people. The following items are excluded from the scope of the law.

a) Deceased persons are not covered by the Law;
b) Legal entities are not covered by the law, unless individual information is available.

6.4 Special Categories of Personal Data

The Law makes a distinction between personal data and special categories of personal data and subjects them to even stricter requirements. The Institution has determined special categories of personal data as follows; Race, Ethnic Origin, Political Thought, Philosophical Thought, Religion, Sect or other beliefs, Dress and Attire, Association, Foundation and Trade Union Memberships, Sexual Life, Criminal Conviction and Security Measures and Biometric and Genetic data.

7. LEGAL BASIS

Processing of personal data refers to all operations performed on such personal data (whether or not such operations are automated). Common types of personal data

processing include (but are not limited to) collection, recording, storage, alteration, reorganization, transfer.

7.1 Basic Principles of Processing Personal Data

Processing in accordance with the law and good faith: Eureko Insurance acts in accordance with the applicable legislation and complies with the rules of honesty in any personal information processing process.

Ensuring the accuracy and currency of personal data: Eureko Insurance takes the necessary measures to ensure that personal data is accurate, up-to-date and provides the opportunity to update it in order to ensure that the data is accurately transferred to the databases.

Processing for specific, explicit and legitimate reasons: Eureko Insurance restricts its personal data processing activities for specific and legitimate purposes and clearly informs about such purposes in the explanation text.

Having limits and acting conservatively towards processing: Eureko Insurance processes personal data to the extent necessary for the limited purpose declared and in a limited manner.

Storing for a longer period of time than stipulated in the relevant legislation or necessary for the purposes of processing: Eureko Insurance stores personal data for a certain period of time in accordance with the relevant legislation. If this period is not specified in the legislation, reasonable retention periods are determined by taking into account the purpose of data use and company procedures, and the data is stored in a limited manner. After the expiration of such periods, personal data are deleted, destroyed or anonymized in accordance with the "Eureko Insurance Personal Data Retention and Destruction Policy".

7.2 Conditions for Processing Personal Data

PDPL also regulates the processing of personal data in Article 5 and the processing of special categories of personal data in Article 6. PDPL stipulates that personal data may be processed even if the person in question does not have an explicit consent in the cases written in these articles and that he/she shall allow this processing to be in accordance with the law. These processing conditions vary depending on whether the personal data is personal or special categories of personal data. Special categories of personal data are

data that may discriminate between individuals. The disclosure of this information by others may lead to victimization of the person concerned and the PDPL stipulates adequate measures to be determined by the Board in the processing of such data.

7.3 Disclosure

Disclosure shall be made verbally or in writing in a manner that is actually accessible to the Data Subjects. In the disclosure, the purpose of data processing, purpose of data collection, method of data collection and legal reason are notified. ES disclosure text is available on the Company's official website https://www.eurekosigorta.com.tr.

7.4 Explicit Consent and Exceptions

Explicit consent means that the data subject is given a clear choice to be included in processing activities such as the collection and storage of personal data. Explicit consent can be given verbally and in writing.

The cases where personal data can be processed without explicit consent as regulated under art. 5/2 of the PDPL and art. 6/3 of the PDPL are set out below, and Eureko Insurance may process personal data based on explicit consent, except in these cases.

According to art. 5/2 of the PDPL, it is possible to process personal data without explicit consent in the presence of one of the following conditions:

- It is explicitly stipulated in the laws,
- It is mandatory for the protection of the life or physical integrity of the person who is unable to disclose his/her consent due to actual impossibility or whose consent is not legally valid,
- It is necessary to process personal data of the parties to a contract, provided that it is directly related to the conclusion or performance of the contract,
- It is mandatory for the data controller to fulfill its legal obligation,
- It has been made public by the data subject,
- Data processing is mandatory for the establishment, exercise or protection of a right,
- Data processing is mandatory for the legitimate interests of the data controller, provided that it does not harm the fundamental rights and freedoms of the data subject.

According to PDPL 6/3, it is possible to process special categories of personal data provided that adequate measures determined by the Board are taken in the following cases:

- a) Explicit consent of the data subject,
- b) It is explicitly stipulated in the law,
- c) It is mandatory for the protection of the life or physical integrity of the person who is unable to disclose his/her consent due to actual impossibility or whose consent is not legally valid, himself/herself or of another person,
- ç) It is related to the personal data made public by the data subject and is in accordance with the will of the data subject to make it public,
- d) It is mandatory for the establishment, exercise or protection of a right,
- e) It is necessary for the protection of public health, preventive medicine, medical diagnosis, treatment and care services, and the planning, management and financing of health services by persons under the obligation of secrecy or authorized institutions and organizations,
- f) It is mandatory for the fulfillment of legal obligations in the areas of employment, occupational health and safety, social security, social services and social assistance,
- g) Current or former members and members of foundations, associations and other non-profit organizations or formations established for political, philosophical, religious or trade union purposes, or persons who are in regular contact with these organizations and formations, provided that they comply with the legislation to which they are subject and their purposes, are limited to their fields of activity and are not disclosed to third parties.

In the processing of special categories of personal data, adequate measures determined by the Board must also be taken.

8. PERSONAL DATA RETENTION TIME LIMIT

The Law stipulates that personal data shall not be kept for longer than is necessary for the purposes for which they were collected or for the purposes for which they are subsequently processed (Article 4 (d) PDPL).

The Law does not provide any personal data retention period. However, Local Commercial Laws give specific retention periods for personal data. Furthermore, retention periods are important for keeping accounting records up to date.

Personal data is stored by ES as long as the purpose of data processing is valid. If data is subject to statutory time limits and must be retained for reporting purposes to public authorities in connection with legal authorities, these limits are respected. Necessary security measures are taken to prevent loss of data stored at ES, to prevent access by unauthorized persons and to prevent illegal use.

Legal retention periods must always be observed. These are minimum time limits (e.g. a ten-year financial period based on the Turkish Commercial Code). If the ES has a good reason to keep data longer, this is permitted (unless otherwise regulated by law). Under the Law, the Authority states (on the basis of legislation) that these retention periods should continue to apply. ES includes data retention periods in its Personal Data Retention and Destruction Policy and Personal Data Processing Inventory.

8.1 What is the erasure of personal data?

ES defines "erasure" as the process of making personal data completely inaccessible and unusable by "relevant users". ES defines relevant users as persons who process personal data within the organization of the data controller or with the authorization granted by the data controller, other than administrators who are responsible for the technical storage, protection and backup of the data.

In order to perform erasure; in general terms, data controllers must deny "data subjects" access to the personal data in question and prevent the processing of such data. The Personal Data Retention and Destruction Policy emphasizes that the users concerned shall not be administrators (database administrators) in order to eliminate all opportunities to regain access of the users concerned. This access restriction must not leave any open door for the relevant user to restore or reuse this data.

For personal data stored on electronic storage media (portable disk, etc.) or servers (file servers, database servers, ftp servers, etc.), the Personal Data Retention and Destruction Policy recommends preventing or restricting the relevant user from re-accessing such personal data.

For personal data on paper, the Personal Data Retention and Destruction Policy proposes to cut it or block it using technological means, using special ink, so as to prevent any

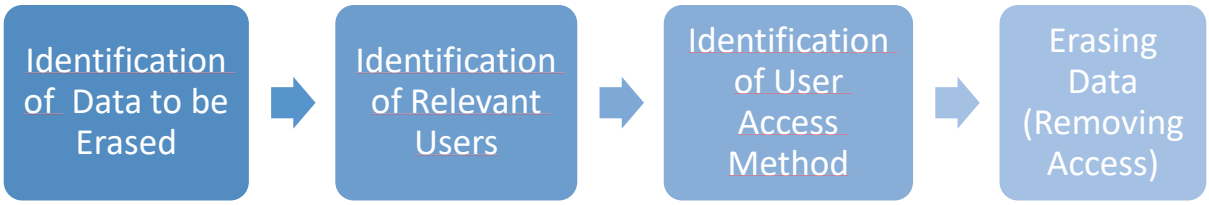
possibility of restoration or any possibility of reading it. Most importantly, the data controller must take care to identify all personal data on paper when erasure is carried out.

What Data is Erased?

1. Data on paper,
2. Data on servers (file servers, database servers, ftp servers, etc.),
3. Data on electronic storage devices (cd, usb, portable disk, etc.)

The data in the above-mentioned places shall be erased within certain destruction periods after the retention periods.

Erasure Process of Personal Data



8.2 What is the destruction of personal data?

ES defines the destruction of personal data as the process by which personal data is made inaccessible and unusable by everyone, or rendered unusable.

Destruction; The data controller must ensure that no one has access to personal data or that processing is impossible.

For physical and electronic environments (including but not limited to servers or disks where personal data is stored), the Personal Data Storage and Destruction Policy offers various methods. These methods render the respective physical or electronic environment unusable (e.g., melting, burning, etc.).

For cloud services, the law recommends the encryption of all personal data and the application of separate encryption keys for the use of all different cloud services. Destruction can be achieved by destroying all copies of the keys.

For paper environments, the Personal Data Storage and Destruction Policy recommends the shredding of papers; this process involves vertically and horizontally shredding the papers into small pieces that make the data on them unrecognizable.

8.3 What is the anonymization of personal data?

ES defines the anonymization of personal data as the process of making it impossible to associate personal data with an identified or identifiable real person, even if it is matched with other data.
To anonymize; the data controller uses various methods such as masking.
The Personal Data Storage and Destruction Policy offers various methods for anonymization. ES shall determine the most appropriate method among these to perform the anonymization.

9. TRANSFER OF PERSONAL DATA (DOMESTIC and INTERNATIONAL)

According to Article 8 of PDPL, personal data cannot be transferred without the explicit consent of the data subject. However, personal data may be transferred without the explicit consent of the data subject if one of the conditions specified in the third paragraph of Article 6 of the law is present, provided that adequate measures are taken.
In this context, ES processes and transfers special categories of personal data in compliance with the Law and fulfills its obligations related to data security as stipulated in Article 12 of the Law. It takes the necessary technical and administrative measures to ensure the level of security and complies with the additional measures determined by the Board for the processing of special categories of personal data.
The Personal Data Transfer Process is managed in accordance with the "PDPL Operations" process within the company's process management application, ESBox.

9.1 Domestic Transfer of Personal Data

ES acts in accordance with the decisions taken by the Board and specified in PDPL. Personal data may be transferred to authorized administrative or legal institutions and organizations without the explicit consent of the data subject in circumstances permitted by PDPL and within the limits defined by legislation. Under the conditions explained in Article 5, paragraph 2, and Article 6, paragraph 3 of PDPL, personal data may also be transferred without the explicit consent of the data subject.
ES transfers personal data domestically under the following conditions;

- When the explicit consent of the data subject is obtained,
- When explicitly stipulated by the law,

- When it is mandatory to protect the life or physical integrity of the person or another person who is unable to express their consent due to actual impossibility or whose consent is not legally valid,
- When it is necessary to process personal data of the parties to a contract, provided that it is directly related to the establishment or performance of the contract,
- When it is mandatory for the data controller to fulfill its legal obligations,
- When data processing is mandatory for the establishment, exercise, or protection of a right,
- When data processing is mandatory for the legitimate interests of the data controller, provided that it does not harm the fundamental rights and freedoms of the data subject,
- When it is related to personal data that the data subject has made public and in line with the purpose of making it public,
- When it is mandatory for the establishment, exercise, or protection of a right,
- When it is necessary for the protection of public health, preventive medicine, medical diagnosis, treatment, and care services, as well as the planning, management, and financing of health services by persons or authorized institutions and organizations that are under the obligation of confidentiality,
- When it is mandatory to fulfill legal obligations in the fields of employment, occupational health and safety, social security, social services, and social assistance,
- For foundations, associations, and other non-profit organizations or formations established for political, philosophical, religious, or trade union purposes, provided that it is in accordance with their legislation and purposes, limited to their fields of activity and not disclosed to third parties; it is aimed at their current or former members and affiliates or individuals who are regularly in contact with these organizations and formations,

Any natural or legal person who processes personal data is either a data controller or a data processor, depending on the purposes and methods of data processing. ES complies with the regulations in Article 8 of the Law for all data transfers between these two categories of individuals.

9.2 International Transfer of Personal Data

In accordanca with the conditions specified in PDPL, ES may transfer personal data processed in Turkey by taking the administrative and technical measures defined in the legislation unless there is no explicit provision in PDPL or current legislation.

(1) Personal data can be transferred abroad by data controllers and data processors if one of the conditions specified in Articles 5 and 6 is met and if there is an adequacy decision regarding the country to which the data shall be transferred, the sectors within that country, or international organizations.

(2) The adequacy decision is given by the Board and published in the Official Gazette. The Board may seek the opinions of relevant institutions and organizations if necessary. The adequacy decision is reviewed at least every four years. Based on the review results or other circumstances deemed necessary, the Board may amend, suspend, or revoke the adequacy decision with prospective effect.

(3) In the absence of an adequacy decision, personal data may be transferred abroad by data controllers and data processors if one of the conditions specified in Articles 5 and 6 is met and if the data subject has the opportunity to exercise their rights and seek effective legal remedies in the country to which the data shall be transferred, provided that one of the following appropriate safeguards is ensured by the parties:

a) Presence of non-international treaty agreements between public institutions or international organizations abroad and public institutions or public-law professional organizations in Turkey and permission for transfer by the Board.

b) Presence of binding corporate rules approved by the Board, containing provisions on the protection of personal data, which companies within the group of enterprises engaged in joint economic activity are obligated to comply with.

c) Presence of a standard contract containing details such as data categories, purposes of data transfer, recipients and recipient groups, technical and administrative measures to be taken by the data recipient, additional measures for special categories of personal data, as declared by the Board.

ç) Presence of a written commitment containing provisions ensuring adequate protection and permission for transfer granted by the Board.

(4) The standard contract shall be notified to the Board by the data controller or data processor within five business days from its signing.

(5) Data controllers and data processors may transfer personal data abroad only on an ad hoc basis if one of the following conditions is present, in the absence of an adequacy decision and the inability to provide any of the appropriate safeguards specified in the third paragraph:

a) The data subject giving explicit consent to the transfer, with informed consent regarding potential risks.
b) The transfer being necessary for the performance of a contract between the data subject and the data controller, or for pre-contractual measures taken at the data subject's request.
c) The transfer being necessary for the establishment or performance of a contract between the data subject and the data controller or another natural or legal person, for the benefit of the data subject.
ç) The transfer being necessary for an overriding public interest.
d) The transfer of personal data being necessary for the establishment, exercise, or protection of a right.
e) The transfer of personal data being necessary for the protection of the life or physical integrity of the data subject or another person who is unable to express their consent due to physical impossibility or whose consent is not legally recognized.
f) The transfer from a publicly accessible register open to the public or persons with a legitimate interest, provided that the conditions required by the relevant legislation for accessing the register are met and the person with a legitimate interest requests it.

10.DATA CONTROLLER AND DATA PROCESSOR

10.1 Data Controller

The Law defines the Data Controller as the natural or legal person who determines the purposes and means of processing personal data, responsible for establishing and managing the data recording system. The Data Controller has the authority to make decisions regarding the processing of personal data, answering the questions of "why" and "how" the processing activities shall be conducted. For example, ES acts as the Data Controller in processing the data of relevant individuals throughout all activities from preparing proposals to approving policies and endorsements.

10.2 Data Processor

The Law defines the Data Processor as the natural or legal person who processes personal data on behalf of the Data Controller, based on the authority granted by the Data Controller. These individuals or entities process personal data within the framework of instructions provided to them by the Data Controller. For example, companies that receive data for technical support purposes act as Data Processors.
According to Article 12 of the Law titled "Obligations Regarding Data Security," the Data Controller is required to;

1. Take all necessary technical and administrative measures to ensure an appropriate level of security in order to prevent unlawful processing of personal data, unauthorized access to personal data, and to ensure the protection of personal data,
2. Be jointly liable with any other natural or legal person who processes personal data on their behalf, for ensuring that these measures are taken,
3. Ensure that both Data Controllers and Data Processors do not disclose personal data they have learned in violation of this Law to others, and do not use it for purposes other than those for which it was processed. This obligation continues even after they cease their duties.

11.DATA CONTROLLERS' REGISTRY (VERBIS)

The Data Controllers' Registry (VERBIS) is a registration system where data controllers are obliged to register and provide information about their data processing activities. he procedures and principles regarding the registry are specified in the Data Controllers' Registry Regulation. Generally, all data controllers must register in the Data Controllers' Registry, and this registration process must be completed before their data processing activities commence.
Aritcle 16 provisions regulating the obligation to register in the Data Controllers' Registry (VERBIS) cannot be applied in the cases listed in the second paragraph of Article 28 of the Law. These cases are listed as follows:

a) When personal data processing is necessary for the prevention of crime or for criminal investigations,
b) Processing personal data that has been made public by the data subject themselves,

c) When personal data processing is necessary for regulatory, disciplinary, or enforcement actions by competent public authorities or professional organizations with public authority status,
d) When personal data processing is necessary for protecting the economic and financial interests of the State concerning budgetary, tax, and financial matters.

Furthermore, the Law grants the Board the authority to exempt from the obligation to register. In applying exemptions, factors such as the nature and quantity of processed personal data, the source of data processing equipment, or the status of data transfer to third parties are taken into consideration.
The obligation to register in the Data Controllers' Registry aims to establish a more secure environment by clarifying personal data processing activities and ensuring compliance with regulations.
Applications for registration in the Data Controllers' Registry are made with the following information;

- Identity and address information of data controllers and, if applicable, their representatives,

The notification to the registry shall be made with the following information. The source of this information is the personal data processing inventory prepared by ES.

- Purpose of processing personal data,
- Data categories,
- Recipients or recipient groups to whom personal data may be transferred,
- Personal data intended for transfer abroad,
- Measures related to personal data security,
- Maximum duration for which personal data shall be processed for the purpose.

If there are any changes to the information listed above, these changes shall be reported to the Authority by ES within 7 days. This is aimed at ensuring the currency of the Personal Data Processing Inventory.
The obligation to register for the specified natural and legal persons responsible for data has begun since October 1, 2018.

12.OBLIGATIONS OF THE DATA CONTROLLER

ES follows all obligations mandated by the Board as published on the official PDPL website or other sources.

12.1 Data controller's disclosure obligation

ES informs individuals about the following issues when collecting personal data;

1. The identity of the data controller and, if any, its representative,
2. The purposes for which the personal data shall be processed,
3. To whom and for what purposes the processed personal data may be transferred,
4. The method and legal basis of collecting personal data,
5. Other rights listed in Article 11 (Details are explained in the "Rights of the Data Subject" section of this document).

ES informs individuals about their personal data through prepared disclosure texts when collecting their information. When necessary, ES may employ layered information. Layered information means providing individuals with brief, understandable, clear, and simple information about the collection of personal data at the time of collection. After this initial notification, individuals are directed to a channel where they can access and read the full scope of information as outlined in Article 10 of the Law.

12.2 Obligations regarding data security

ES takes necessary technical and administrative measures to ensure an adequate level of security to:

1. Prevent unlawful processing of personal data,
2. Prevent unauthorized access to personal data,
3. Ensure the preservation of personal data.

ES, if personal data for which it is responsible is processed by another natural or legal person, is jointly responsible with them for ensuring the implementation of the measures specified in the first paragraph. ES ensures that necessary audits are conducted to ensure compliance with the provisions of the Law.

In the event that unlawfully obtained personal data is processed by others, ES promptly **notifies the data subject within the shortest time and informs the Board within 72 hours**. The Board may announce this situation on its website or by any other appropriate means if deemed necessary.

13.SECURITY OF PERSONAL DATA

The security of personal data starts with a risk analysis. Measures to prevent a specific threat or breach and minimize the impact of any resulting consequences are determined as follows;

13.1 Identification of Risks

a) In which data processing category the risks occur,
b) For which personal data,
c) In which data recording environments, and
d) Potential users who may contribute to the occurrence of this risk are identified.
e) Risks are identified from the perspective of PDPL and are mapped onto the institution's risk map and classified according to the risk level. Attention is paid to the classification based on the category and size of personal data during this classification.

13.2 Implementation of Administrative and Technical Security Measures

Security standards included in both the Board and ES's specified administrative and technical measures guide the Company in reducing relevant risks. Proper use of current security standards ensures that the data controller takes sufficient measures and establishes effective safeguards.
ES creates a personal data security policy that complies with the specified measures in the law and meets the requirements specified in the law.

13.3 Risk and Security Level Controls and Assessments

Regular checks are conducted to determine whether relevant risks have occurred and whether security measures are in place. The Company stays updated with the latest information in the field of information security. If necessary, risk and security measures are updated following the checks and assessments.

14.TECHNICAL AND ADMINISTRATIVE MEASURES

Within this scope, ES takes necessary technical and administrative measures to prevent unlawful processing or access of personal data it processes, and to ensure the appropriate level of security for the protection of personal data. ES acts in accordance with decisions of the Board (Kurul), conducts necessary audits, or ensures they are conducted. Despite having implemented technical and administrative measures for the processed personal data, if it is obtained unlawfully by others, ES promptly notifies the data subjects within the shortest time and informs the Board within 72 hours.

Technical measures are logical and physical measures taken in information systems and their surroundings (e.g., access control/management, logging procedures, backups, encryption of personal data, secure data transportation, segregation of databases, etc.).

Organizational measures are measures taken by the organization to prevent breaches of personal data (e.g., defining responsibilities and authorities, instructions, training programs, and disaster management plans).

The technical and administrative measures taken by ES to ensure the security of personal data are included in the VERBIS notification.

15.DATA BREACH

A data breach is a security incident where personal data is unlawfully copied, transmitted, viewed, stolen, or used. Data Controllers are obligated to notify the data subjects within the shortest time and inform the Authority within 72 hours of any data breach.

According to Article 17 of the Law, Articles 135 to 140 of the Turkish Penal Code No. 5237 shall continue to apply to crimes related to personal data (unauthorized recording of personal data, illegal disclosure or acquisition of personal data, and failure to dispose of personal data).

According to Article 7 of the Law, data controllers who fail to erase, destroy, or anonymize personal data after processing shall be subject to legal proceedings under Article 138 of Law No. 5237.

In addition to the relevant articles of the Turkish Penal Code, data controllers found to be in violation of the obligations specified in the Law shall also be subject to administrative fines.

The Board is authorized to supervise these obligations and enforce the sanctions prescribed by the Law.

The Board, upon conducting an investigation in cases involving complaints or upon learning of alleged violations within its jurisdiction, determines the existence of any breaches. If a violation is identified, the Board decides on measures for the data controller to rectify the legal non-compliance and notifies the decision to the parties concerned. The data controller is obligated to comply with this decision without delay and no later than 30 days from the date of notification.

ES implements technical and administrative measures specified by the Board to prevent data breaches. Regular security checks are conducted on relevant data repositories.

ES records all data breaches and promptly reports/informs relevant departments and other necessary entities (such as the Board, data subjects, etc.).

If there is a data breach, the data subjects are informed by ES in clear and plain language about the breach:

- Description of the data breach,
- Name and contact details of the Data Controller and/or another person,
- Potential impacts of the breach,
- Measures proposed or taken by the Data Controller to address the breach, including any steps to mitigate any adverse effects.

16.RIGHTS OF THE DATA SUBJECT

16.1 Application to the Data Controller

The data subject has the following rights to request information on themselves by applying to ES;

1. To learn whether personal data is being processed,
2. To request information if personal data has been processed,
3. To learn the purpose of processing personal data and whether they are used in accordance with that purpose,
4. To know the third parties to whom personal data are transferred domestically or abroad,
5. To request correction if personal data is incomplete or incorrectly processed,
6. To request reasure or destruction of personal data,
7. To request notification to third parties to whom personal data have been transferred regarding corrections, erasures, or destructions requested,

8. To object to the occurrence of a result against the individual by exclusively analyzing the processed data through automated systems,
9. To request compensation for damages in case of suffering damage due to unlawful processing of personal data,

ES must finalize data subject requests within 30 days free of charge. ES accepts or rejects requests in writing or electronically. The relevant processes, tasks, and responsibilities are defined within the "PDPL Procedures" workflow.

16.2 Complaint to the Board

If the application is rejected, the response is found insufficient, or no response is received within the specified period, the data subject can file a complaint with the Board within 30 days from the date they learn of the response, and within 60 days from the application date. Pursuant to Article 13 of the Law, the complaint route cannot be pursued before exhausting the application process. Those whose personal rights have been violated retain the right to compensation under general provisions (Article 14).

17.CONTRACTS

17.1 Personal Data Processing Protocols

Personal data processing protocols are prepared between ES and the Data Processor and shared. If any transfer (one-way or two-way) is necessary, the existence of a personal data processing protocol is queried; if absent, its creation is considered.
The content of contract texts or additional protocols is prepared by the Legal Department. They are sent to the contracting unit for signature by the Data Processor. The contracting unit is responsible for signing these contracts or protocols and sharing them with the Data Processor.

18.PRIVACY IMPACT ASSESSMENT (PIA)

High-risk personal data processing activities can be demonstrated through a Privacy Impact Assessment (PIA).
A PIA is a designed process to identify a processing activity, and analyze the necessity and proportionality of a processing activity. A PIA is not mandatory for the Data Protection Law (PDPL). The PIA process is launched by the CEO-Office with related Business Units and/or

the Data Processor. A PIA is reviewed every year or before any critical data processing process changes occur within ES.
PIA must be implemented as early as possible before starting personal data processing (design phase). If a PIA is performed later, the approach to privacy risks can necessitate costly adjustments in processes or systems.
The CEO-Office creates the Privacy Impact Assessment (PIA) report through discussions with business units. In this analysis, the personal data processing activities of the business units are evaluated under the following headings;

a) Categories of processed personal data,
b) Purposes of data processing,
c) Evaluation of ES's legitimate interests where applicable,
d) Necessity of data processing and need for explicit consent,
e) Data transfer requirements, and
f) Data retention periods.

In addition to these steps, the texts used by the business units are also evaluated in parallel with this study and updated where necessary.

19.BIG DATA, PUBLIC DATA, AND SOCIAL MEDIA

The PDPL does not impose specific obligations regarding big data, public data, or social media. However, if personal data is processed in these contexts, the law fully applies, and therefore, all conditions must be met. This section briefly addresses these topics.
If personal data is included in any information within big data, public data, or transferred from social media to data recording environments, all data processing rules mentioned in the law fully applies.

19.1 What is big data?

Big data is not just about a large volume of data. The concept of big data refers to data that needs to be processed rapidly, often in various formats, and is frequently unstructured, meeting today's data consumption needs.

If personal data is processed in Big Data applications, both the PDPL (Personal Data Protection Law) and this Policy are fully applicable. If Big Data applications become part of ES systems, they are evaluated within the PIA (Privacy Impact Assessment) framework.

19.2 What is public data?

Public data refers to information that is accessible, usable, and shareable by everyone. Governments, businesses, and individuals can use public data for social, economic, and environmental benefits.
If public data is processed for business purposes within the Company, both the PDPL and this Policy are fully applicable. If publicly available data (in physical or electronic form) becomes part of ES systems, it is evaluated within the PIA framework.

19.3 What is social media?

Social media is interactive computer-mediated technologies that facilitate the creation and sharing of information, ideas, and other forms of expression through virtual communities and networks.
For example, ES can share various career opportunities on platforms like LinkedIn. When an individual applies for a job advertisement posted by ES, the person becomes accessible to ES, and a personal data processing activity occurs. If Social Media becomes part of ES systems in this or similar ways, it is evaluated within the PIA framework.

20.PUBLISHING AND STORAGE OF THE POLICY

The Policy is approved by the ES Board of Directors and communicated to Company employees electronically. It is published via the intranet.

21.UPDATE PERIOD OF THE POLICY

The Policy is updated every three years, except for changes introduced by the Personal Data Protection Authority regulations.

22.EFFECTIVENESS AND WITHDRAWAL OF THE POLICY

The Policy is approved by the ES Board of Directors. It is put into effect by delivering it to Company employees electronically. Updates are made as needed.

23.OTHER PROVISIONS

In case updates are made to this Policy by ES, the relevant information regarding such changes shall be specified in this Policy.

24. APPENDICES

Annex 1. Legislation, Policy, and Guidelines

European Legislation	Turkish Legislation	Guidelines / Circulars / Protocols	Domestic Politics / Guidelines
Privacy and electronic communication Directive 2002/58/EC General Data Protection Regulation (EU) 2016/679	PDPL (Personal Data Protection Law)	Ref. https://www.kvkk.gov.tr/	Privacy Policy and Appendices Information Security Policy Data Governance Policy Personal Data Retention and Destruction Policy Special Categories of Personal Data Protection Policy Incident Management Policy Disciplinary Regulation

Annex 2. Personal Data Processing Inventory

ES Personal Data Processing Inventory includes detailed information on the following headings;

- Responsible Unit / Job Process
- Activity Name
- Data Category
- Processing Purpose
- Data Subject
- Data Transfer
- Explicit Consent
- Transferred Person / Organization (domestic - international)
- Retention Periods

There is no specific format requirement defined for this inventory in the Law and Regulations.

Additionally, in accordance with Articles 5 and 9 of the Regulation, the Personal Data Processing Inventory is used for disclosure in the Data Controllers' Registry, fulfilling the obligation to inform data subjects, disclosing data responsibilities, and determining the scope of explicit consent.