GÜNGÖR LAW FIRM

PERSONAL DATA PROTECTION AND PROCESSING POLICY

GÜNGÖR
LAW FIRM

Table of Content

1. SECTION: INTRODUCTION

I. IMPORTANCE OF PROTECTING PERSONAL DATA

The protection of personal data is a Constitutional right and is within the priorities ofDAta. As a matter of fact, for this purpose, this policy has been established. Within the scope of the Personal Data Protection Law No. 6698 ("Law"), this Personal Data Protection and Processing Policy ("Policy") is made in order to fulfil the general clarification obligation of Att. Deniz Güngör-Güngör Law Firm ("Data Controller") in the capacity of Data Controller and to determine the basic principles of Data Controller's personal data processing rules, and in this context, the basic principles of protecting the personal data of our clients, potential clients, employees, employee candidates, trainee and students, supplier/sub-employer employees and officials, visitors and other third persons whose data we process are set forth.

In order to implement the issues specified in this Policy, necessary procedures are set forth within the Data Controller , clarification texts are established in accordance with the specific to the categories of persons, personal data protection and confidentiality agreements are made with employees and third parties who have access to personal data, job descriptions are revised, administrative and technical measures are taken by the Data Controller for the protection of personal data, in this context necessary audits are carried out or have carried out

II. PURPOSE OF POLICY

The main purpose of this Policy is to establish the principles for personal data processing activities and protection of personal data carried out by the Data Controller in accordance with the law, and in this context, to ensure transparency by clarifying and informing the persons whose personal data are processed by Data Controller.

III. SCOPE

This Policy: relates to all personal data of the persons we categorize under the headings *"our clients, potential clients, employees, employee candidates, trainees and students, supplier/sub-employer employees and officials, business partners, visitors, officials of references of the employees, family and the relatives of the employees, parents/guardians/representatives and other third persons whose data we process"* that we process by automated or non-automated means, provided that it is part of any data recording system.

IV. IMPLEMENTATION OF POLICY AND RELATED LEGISLATION

The relevant legal regulations in force regarding the processing and protection of personal data shall be implemented. If there is incompatibility between the legislation in force and the Policy, Data Controller agrees that the legislation in force shall be implemented.

V. ACCESS AND UPDATE

The Policy is published on Data Controller 's website at www.gungorlaw.com and is made available to the persons concerned at the request of the data subjects and updated as necessary.

2. SECTION: PROCESSING OF PERSONAL DATA

In accordance with Article 20 of the Constitution and Article 4 of the Law, Data Controller carries out the processing of personal data; in accordance with the law and with good faith, accurate and up to date when necessary; for specific, explicit and legitimate purposes; in a limited and measured manner. Data Controller stores personal data for the period stipulated in the law or required by the purpose of personal data processing.

In accordance with Article 20 of the Constitution and Article 5 of the Law, Data Controller processes personal data on the basis of one or more of the conditions in Article 5 of the Law on the processing of personal data.

In accordance with Article 419 of the Code of Obligations, Data Controller processes the personal data of employees and employee candidates based on the purposes of work predisposition and performance of the employment contract, provided that this Law is reserved.

In accordance with Article 20 of the Constitution and Article 10 of the Law, Data Controller clarifies the data subjects and provides the necessary information if the data subjects request information and apply to exercise their rights arising from the law and responds to the applications within the legal period.

Data Controller acts in accordance with the regulations stipulated in terms of the processing of sensitive data in accordance with Article 6 of the Law.

In accordance with article 8 and 9 of the Law, Data Controller complies with the rules stipulated in the law on the transfer of personal data and implements the decisions taken and communiqués published by the PDP Board while taking into account the safe country lists.

I. PROCESSING OF PERSONAL DATA IN ACCORDANCE WITH THE PRINCIPLES AND RULES STIPULATED IN THE LEGISLATION

1. Principles for Processing of Personal Data

A) Processing In Accordance with the Law and With Good Faith

Data Controller acts in accordance with the principles introduced by legal regulations and with good faith in the processing of personal data. In this context, Data Controller operates by detecting the legal basis that will require the processing of personal data, takes into account the requirements of proportionality, does not use personal data outside the scope of the purpose, and does not carry out processing activities without the knowledge of individuals.

B) Ensuring That Personal Data Is Accurate and Up to Date When Necessary

Data Controller ensures that the personal data it processes is accurate and up to date taking into account the basic rights of the data subjects and its own legitimate interests and takes the necessary measures accordingly. In this context, data on all categories of people are tried to be kept up to date.

C) Processing For Specific, Explicit and Legitimate Purposes

Data Controller clearly and precisely determines the purpose of processing personal data, which is legitimate and lawful. Data Controller processes the personal data relevant with the service it offers and as much as is necessary for them.

D) Being Relevant with, Limited to and Proportionate to the Purposes for Which They Are Processed

Data Controller processes personal data in a manner convenient for the realization of the specified purposes and avoids the processing of personal data that is not related to or needed for the realization of the purpose. In this context, processes are constantly reviewed and the principle of **"data minimization"** is tried to be implemented.

E) Retaining For the Period Stipulated by Relevant Legislation or the Purpose for Which They Are Processed

Data Controller retains personal data only for the period specified in the relevant legislation or required for the purpose for which they are processed. In this context, Data Controller first determines whether a period of time is foreseen for the storage of personal data in the relevant legislation, acts in accordance with this period if a period is specified, takes into account the legal and penalty statute of limitations and stores personal data for the period required for the purpose for which they are processed. Personal data is deleted, destroyed or anonymized in accordance with Data Controller's **"Personal Data Storage and Destruction"** policy in case of expiration or elimination of reasons requiring processing.

2. Rules For Processing of General Personal Data

The protection of personal data is a Constitutional right and fundamental rights and freedoms may be limited only by law, subject to the reasons specified in the relevant articles of the Constitution, without interfering their essence. In accordance with the third paragraph of Article 20 of the Constitution, personal data may only be processed in the cases stipulated in the law or with the explicit consent of the person. Data Controller processes personal data only without the explicit consent of the Data Subject if the following conditions exist;

a) Explicit stipulation in law,

b) It is necessary for the protection of life or physical integrity of the person himself/herself or of any other person, who is unable to express his/her consent due to the practical imposibility or whose consent is not deemed legally valid.

c) The requirement of processing of personal data of the parties to the contract, provided that it is directly related to the establishment or performance of a contract,

d) It is necessary for compliance with a legal obligation to which the data controller is subject

e) Personal data have been made public by the data subjecthimself/herself,

f) Data processing is necessary for the establishment, exercise or protection of any right,

g) When it is compulsory to process the data for the data controller's legitimate interests, provided that not harming fundamental rights and freedoms of the data subject

In the absence of the above conditions, Data Controller requests the explicit consent of the data subject which is based on free will and information. Especially in the field of Human Resources and working relations, taking into account the dependency relationship of the employee, it is based primarily on the reasons for compliance with the law that are not consensual, but in case of these reasons, explicit consent is applied. In contrast, in activities such as marketing, processing activities are carried out on the basis of the consent of the data subject. However, in all cases where personal data is processed, people are necessarily "**clarified**" and data processing activities are carried out.

3. Rules For Processing of Sensitive Data

In the processing of personal data determined as **"sensitive"** in the Law, it is acted in accordance with the regulations stipulated in the Law by Data Controller. In Article 6 of the Law, a number of personal data that risk causing victimization or discrimination of individuals when processed unlawfully are designated as "sensitive" and attention and sensitivity should be displayed while processing this data. These are data related to race, ethnicity, political opinion, philosophical belief, religion, sect or other beliefs, appearance and clothing, association, foundation or trade union membership, health, sexual life, criminal conviction and security measures, and the biometric and genetic data. Your sensitive personal data are processed by Data Controller in accordance with the Law in the following cases provided that the necessary measures are taken:

- ✓ sensitive personal data other than the health and sex life of the data subject, in cases stipulated in the law or based on the explicit consent of data subject if he/she has,
- ✓ sensitive personal data concerning health and sexual life of the data subject may only be processed by the persons subject to secrecy obligation or competent public institutions and organizations or with the explicit consent of the data subject for the purposes of protection of public health, operation of preventive medicine, medical diagnosis, treatment and nursing services, planning and management of health-care services as well as their financing.

- ✓Regardless of the reason, general data processing principles are always taken into account in the processing processes and compliance with these principles is ensured (Law a. 4; see Section 2, I, 1 above).

4. Clarification and Informing the Persons Concerned Whose Data Is Processed

In accordance with Article 10 of the Law, Data Controller clarifies the data subject during obtaining personal data. In this context, clarification is made about the purpose for which personal data will be processed to the Data Subject whose data is processed, to whom and for what purpose the processed personal data can be transferred, the method of collecting personal data and its legal reasons and the rights of the Data Subject whose personal data is processed.Also, in article 11 of the Law, "Requesting Information" is listed among the rights of the Data Subject whose personal data has been processed, and in this context, the necessary information is provided in case the Data subject whose personal data is processed requests information in accordance with articles 20 of the Constitution and article 11 of the Law

II. TRANSFER OF PERSONAL DATA

Data Controller can transfer the personal data and sensitive personal data of the Data Subject whose personal data is processed to third parties by taking the necessary security measures for lawful purposes of processing personal data. Accordingly, Data Controller acts in accordance with the regulations stipulated in Article 8 of the Law.

1. Principles of Transfer of Personal Data

For legitimate and lawful personal data processing purposes, Data Controller may transfer personal data to third parties based on one or more of the personal data processing conditions specified in Article 5 of the Law listed below and limitedly:

Based on the explicit consent of the Data Subject whose personal data has been processed; or

- ✓ If there is a clear regulation in the law regarding the transfer of personal data,
- ✓If it is mandatory for the protection of the life or physical integrity of the data subject or of any other person, or the data subject is unable to express his consent due to practical impossibility or legal validity is not granted for his consent;
- ✓Provided that it is directly related to the establishment or performance of an agreement, if it is necessary to transfer personal data of the parties to the agreement,
- ✓ If the transfer of personal data is mandatory in order for data controller to fulfil its legal obligation,
- ✓ If the personal data has been made public by the Data subject himself,
- ✓ If the transfer of personal data is mandatory for the establishment, exercise or protection of a right,
- ✓If personal data transfer is mandatory for the legitimate interests of Data Controller, provided that the personal data does not harm the fundamental rights and freedoms of the Data Subject then it is transferred.

Regardless of the reason, general data processing principles are always taken into account in the transfer processes and compliance with these principles is ensured (Law a. 4; see Section 2, I, 1 above).

2. Transfer of Sensitive Personal Data

Data Controller, by taking the necessary care, taking the necessary security precautions and adequate measures prescribed by the Personal Data Protection Board ("Board"); for legitimate and lawful personal data processing purposes, can transfer the sensitive personal data of the Data Subject whose personal data is processed to third parties in the following cases.

- Based on the explicit consent of the Data Subject if he has or,
- If the Data Subject does not have explicit consent;
  - ✓ Sensitive personal data other than concerning health and sex life of the Data Subject (race, ethnic origin, political opinion, philosophical belief, religion, religious sect or other belief, appearance, membership to associations, foundations or trade-unions, data concerning health, sexual life, criminal convictions and security measures are biometric and genetic data) in cases stipulated by the Law,
  - ✓ Sensitive personal data concerning health and sexual life of the Data Subject may only be processed by the persons subject to secrecy obligation or competent public institutions and organizations, for the purposes of protection of public health, operation of preventive medicine, medical diagnosis, treatment and nursing services, planning and management of health-care services as well as their financing.

3. Transfer of Personal Data Abroad

Data Controller can transfer the personal data andsensitive personal data of the Data Subject whose personal data is processed to third parties by taking the necessary security measures for lawful purposes of processing personal data. By Data Controller personal data are transferred to foreign countries declared by the Board to have adequate protection (“Foreign Countries With Adequate Protection”) or in the absence of adequate protection, it is transferred to foreign countries where data controllers in Turkey and related foreign countries have committed adequate protection in writing and where the PDP Board has permission ("Foreign Country with Data Controller Committed to Adequate Protection"). Accordingly, Data Controller acts in accordance with the regulations stipulated in Article 9 of the Law.

If the Data Subject whose personal data has been processed for legitimate and lawful personal data processing purposes has an explicit consent or if the Data Subject whose personal data is processed does not have explicit consent, Data Controller may transfer personal data to Foreign Countries with Adequate Protection or with Data Controller Committed to Adequate Protection if one of the following conditions exists:

- ✓ If there is a clear regulation in the law regarding the transfer of personal data,
- ✓ If it is mandatory for the protection of the life or physical integrity of the Data Subject whose personal data has been processed or of any other person, or the Data Subject whose personal data has been processed is unable to express his consent due to practical imposibility or legal

validity is not granted for his consent;

- ✓ Provided that it is directly related to the establishment or performance of an agreement, if it is necessary to transfer personal data of the parties to the agreement,
- ✓ If the transfer of personal data is mandatory in order for Data Controller to fulfil its legal obligation,
- ✓ If the personal data has been made public by the Data Subject himself,
- ✓ If the transfer of personal data is mandatory for the establishment, exercise or protection of a right,
- ✓ If personal data transfer is mandatory for the legitimate interests of Data Controller, provided that the personal data does not harm the fundamental rights and freedoms of the data subject.

4. Purposes of Transfer of Personal Data by Data Controller and Categories of Persons Transferred

A) Purpose of Data Transfer

Data transfer is carried out for purposes such as; to ensure the fulfilment of the activities and establishment purposes of Data Controller, to ensure that the services provided by Data Controller from the supplier as outsourced and necessary to fulfil the commercial activities of Data Controller are provided to Data Controller, to ensure the execution of the human resources and employment policies of Data Controller, to fulfil the obligations of Data Controller within the framework of the occupational health and safety and to ensure that necessary measures are taken.

B) Persons To Whom Data Is Transferred

In accordance with article 8 and 9 of the Law of Data Controllercan transfer **personal data** to the following categories of persons:

AUTHORIZED PUBLIC ORGANIZATIONS	Public institutions and organizations authorized to receive information and documents from Data Controller	Data sharing is carried out according to the provisions of the relevant legislation.
AUTHORIZED PRIVATE LEGAL PERSONS	Private legal persons authorized to receive information and documents from Data Controller	Data sharing is carried out limited to the purpose requested by the relevant private legal persons within their legal authority.
CLIENTS	Persons or institutions served by the Data Controller.	Within the scope of the service received by our clients, limited data sharing is made in order to carry out the activities of the Data Controller.

SUPPLIER	Parties that provide services to Data Controller while carrying out the commercial activities of Data Controller	Data sharing is carried out limited to ensure that the services outsourced by Data Controller from the supplier and necessary for the performance of Data Controller's commercial activities are provided to Data Controller

In the transfers carried out by Data Controller, it is acted in accordance with the principles and rules set forth in this Policy.

III. PERSONAL DATA CATEGORIZATIONS

The persons whose data are processed by Data Controller and the data processed within this scope are categorized as follows;

PERSON CATEGORIZATION

EMPLOYEE CANDIDATE	Natural persons who have applied for a job to Data Controller or who have opened their resume and related information to Data Controller's review in any way
EMPLOYEE	Natural persons working in Data Controller
PARTNER	Natural persons who are partner of Data Controller

POTENTIAL CLIENT	Natural persons who have requested to use Data Controller's services or interested in themor who have been considered as they have this interest on them accordance with the rules of good faith.
TRAINEE/STUDENT	People who are undergoing training in Data Controller and internship/training students
SUPPLIER EMPLOYEE	Natural persons working in the institutions with which Data Controller has any business relationship (including but not limited to business partners, suppliers)
SUPPLIER OFFICIAL	Natural persons who are shareholders and officials of the institutions with which Data Controller has business relationship
PARENT/GUARDIAN/ REPRESENTATIVE	Natural persons whose personal data is processed as a parent, guardian or representative.
VISITOR	Natural persons who have entered the physical campuses owned by Data Controller for various purposes or who have visited our websites
OTHER	Third-party natural persons associated with Data Controller to ensure the security of commercial transactions between the aforementioned parties or to protect the rights of the persons mentioned and afford advantage (e.g. Family Members and relatives)

DATA CATEGORIZATION

IDENTITY INFORMATION	Information contained in documents such as Driver's License, ID Card, Residence, Passport, Attorney's ID, Marriage Certificate clearly belonging to an identified or identifiable natural person; processed in a partially or fully automated manner or in a non-automated manner as part of the data recording system
CONTACT DETAILS	Information such as telephone number, address, e-mail information clearly belonging to an identified or identifiable natural person; processed in a partially or fully automated manner or in a non-automated manner as part of the data recording system

LOCATION INFORMATION	Information such as address, location information of data subject clearly belonging to an identified or identifiable natural person; processed in a partially or fully automated manner or in a non-automated manner as part of the data recording system
PERSONNEL INFORMATION	Any personal data processed to obtain information that will be the basis for the formation of personal rights of our employees or individuals who are in a working relationship with Data Controller clearly belonging to an identified or identifiable natural person; processed in a partially or fully automated manner or in a non-automated manner as part of the data recording system
LEGAL PROCESS AND COMPLIANCE INFORMATION	Your personal data processed for the determination, follow-up of our legal receivables and rights and performance of our debts, as well as compliance with our legal obligations and Data Controller's policies clearly belonging to an identified or identifiable natural person; processed in a partially or fully automated manner or in a non-automated manner as part of the data recording system
CUSTOMER TRANSACTION INFORMATION	Information such as records of the use of our products and services and instructions and requests of the customer for the use of the products and services, clearly belonging to an identified or identifiable natural person and included in the data recording system
PHYSICAL SPACE SAFETY INFORMATION	Personal data relating to records and documents obtained at the entrance to the physical space and during the stay within the physical space clearly belonging to an identified or identifiable natural person and included in the data recording system
TRANSACTION SECURITY INFORMATION	Personal data processed to ensure technical, administrative, legal and commercial security while carrying out activities clearly belonging to an identified or identifiable natural person and included in the data recording system
RISK MANAGEMENT INFORMATION	In order to manage our commercial, technical and administrative risks personal data processed through methods used in these areas in accordance with generally accepted legal, commercial practice rules and with good faith clearly belonging to an identified or identifiable natural person and included in the data recording system

FINANCIAL INFORMATION	Personal data processed related to information, documents and records showing all kinds of financial results created according to the type of legal relationship that Data Controller has established with the data subject clearly belonging to an identified or identifiable natural person; processed in a partially or fully automated manner or in a non-automated manner as part of the data recording system
PERFORMANCE AND CAREER DEVELOPMENT INFORMATION (PROFESSIONAL EXPERIENCE INFORMATION)	Personal data processed for the purpose of measuring the performance of our employees or natural persons in working relationship with Data Controller and planning and executing their career development within the scope of Data Controller's human resources policy clearly belonging to an identified or identifiable natural person; processed in a partially or fully automated manner or in a non-automated manner as part of the data recording system
MARKETING INFORMATION	Personal data processed to customize and market our products and services in accordance with the usage habits, likes and needs of the data subject, as well as reports and evaluations created as a result of these processing results clearly belonging to an identified or identifiable natural person; processed in a partially or fully automated manner or in a non-automated manner as part of the data recording system
VISUAL/AUDIAL INFORMATION	Personal data clearly belonging to an identified or identifiable natural person; processed in a partially or fully automated manner or in a non-automated manner as part of the data recording system; e.g. photo and camera recordings (except recordings that are included within the scope of physical space security information), audio recordings and data contained in documents that are copies of documents containing personal data
SENSITIVE DATA II	Association, foundation, criminal conviction and security measures,

SECTION 3: LEGAL BASIS AND PURPOSES OF PROCESSING PERSONAL DATA

I. LEGAL BASIS FOR PROCESSING PERSONAL DATA

1. Reasons for Legal Compliance

A) Having the Explicit Consent of the Data Subject

One of the conditions for processing personal data is the explicit consent of the data subject. The explicit consent of the data subject should be declared related to a particular subject, on the basis of information and with free will.

B) Explicit Stipulation in Law

The personal data of the data subject may be processed in accordance with the law if explicitly stipulated in the law. *For example, reporting the identification of our employees to the competent authorities in accordance with the Identification Reporting Legislation.*

C) Failure to Obtain Explicit Consent of the Data subject Due to Actual Impossibility

The personal data of the data subject may be processed if it is mandatory to process the personal data of the person for the protection of the life or physical integrity of the person himself or of any other person, who is unable to express his consent due to actual impossibility or legal validity cannot granted for his consent; *For example, sharing the blood type information of the unconscious employee with the physician.*

D) Being Directly Related to the Establishment or Performance of the Agreement

If it is directly related to the establishment or performance of an agreement, it is possible to process personal data in cases where it is necessary to process the personal data of the parties to the agreement.

E) Fulfilling the Data Controller's Legal Obligation

The personal data of the data subject may be processed if processing is mandatory in order for Data Controller to fulfil its legal obligations as a data controller.

F) Data Subject's Making His / Her Personal Data Public

If the data subject has made his personal data public, the relevant Personal data may be processed.

G) If Data Processing Is Mandatory for the Establishment, Exercise or Protection of a Right

If data processing is mandatory for the establishment, exercise or protection of a right, the personal data of the data subject may be processed.

H) Data Processing is Mandatory for the Legitimate Interest of Data Controller

The personal data of the data subject may be processed if it is mandatory for the legitimate interests

of Data Controller to process data, provided that it does not harm the fundamental rights and freedoms of the data subject.

2. Processing of Sensitive Data and Reasons for Legal Compliance

By Data Controller sensitive data can only be processed if the data subject does not have explicit consent, provided that adequate measures are taken to be determined by the Board, only in cases stipulated in the law. Regardless of the reason, general data processing principles are always taken into account in the processing processes and compliance with these principles is ensured (Law a. 4; see Section 2, I, 1 above).

II. PURPOSES OF PROCESSING PERSONAL DATA

Data Controller processes personal data for purposes and conditions limited to personal data processing conditions specified in paragraph 2 of article 5 and paragraph 3 of article 6 of the Law. In the data processing process, the above-mentioned legal grounds are taken into account, and if there are no other reasons for compliance with the law, the consent of the relevant person is requested. Here, in accordance with the article 4 of the Law, a general audit of the principles is carried out, first of all, it is necessary that the data processing activity generally complies with the principles of compliance with the law. The consent of the relevant person is obtained "explicitly, based on information and free will".

Personal data are processed by Data Controller especially for the following purposes;

- As an employer, personal data of **EMPLOYEES, STUDENTS AND INTERNS** (employees in broad term) and their **PARENT/CUSTODIAN AND REPRESENTATIVES** must be processed in order to fulfil the mutual obligations arising from the employment contract. In this context, we process and store employees' personal data; in accordance with the law and rules of good faith, accurate and up to date when necessary; for specific, clear and legitimate purposes; in a limited and measured manner, in connection with the purpose. In this context, in line with the purposes necessary for the employees to be employed in accordance with the law, the establishment, performance and expiration of the employment contract processes are carried out in accordance with the law, the legitimate interests of the Data Controller, the cases clearly stipulated in the law, the fulfilment of legal obligations related to employee employment, data processing is mandatory for the establishment, exercise and protection of a right in case of legal follow-up and in cases other than these, the explicit consent that will be requested from employees, based on information and expressed with the free will of the employees constitutes the legal basis for the processing of personal data.
- Within the scope of the activities required by the Data Controller's field of activity, the legitimate interests of the employer require the processing of the personal data of the employees. As a matter of fact, the personal data of employees can be processed for reasons such as preventing abuses, preventing theft, ensuring general safety or occupational health and safety. However, in this case, great care is taken not to harm the fundamental rights and freedoms of employees.

- Employees' race, ethnicity, political thought, philosophical belief, religion, sect or other beliefs, appearance and clothing, as well as biometric and genetic data are not included in the personal data processed unless they are explicitly stipulated in the law as a rule, and if an exceptional practice is to be performed, the requirements are carefully evaluated before processing personal data.

- The Data Controller has control and supervision on information communication tools (telephone, mobile phones, computers, internet). The Law No. 5651 and the legitimate interests of Data Controller constitute the legal basis of such practices.
- In addition to our employees, our visitors and other persons who connect to the Internet through the Data Controller's system may also be included in the data processing. That processing activity is also based on the legitimate interests of the Data Controller, and is carried out in a way that it does not harm the fundamental rights and freedoms of the employees..
- Personal data of **EMPLOYEE RELATIVES AND FAMILY MEMBERS** are also processed for the connection and communication in emergency processes (for example, notification in case of an accident), fulfilment of legal obligations such as minimum living allowance, and employee relationship processes.
- In accordance with; Labor Law No. 4857, Code of Obligations No. 6098 article 419, Law and relevant legislations, Data Controller is processing personal information of EMPLOYEE CANDIDATES who apply for a job such as name, address, date of birth, e-mail address, telephone number and other contact information, CV, cover letter, past or relevant work experience or other experience, educational background, transcript, language test results or supporting or explanatory documents related to the job application, records of information obtained during the interview, by means of video conference, telephone of face-to-face interviews, references that specified in job applications. In the context of employee candidacy, it is highly recommended that the candidate refrains from stating any especially sensitive data and any personal data that is not directly related to his/her competencies. if that the CV and other written documents given contains those kinds of data, those parts should be blacked out first then submitted to the Data Controller. In In addition, for PERSONAL DATA (name, surname, telephone, e-mail, etc.) of the REFERENCE PERSON/PERSONS, which are included in the CV of the candidate and whose data are processed in this process, candidate should know that it is candidate's responsibility to inform the person in question and to obtain their explicit consent(s) then it should be conveyed to the Data Controller.
- Personal data of the SUPPLIER AND ITS EMPLOYEES can also be processed by the Data Controller. As a matter of fact, in the Law No. 6331, the documents and information that need to be checked regarding the occupational health and safety of the employees coming from another workplace have been specified to the main employer. Accordingly, the processing of personal data of workers working under the supplier is based on the legitimate interests of the Data Controller, primarily for the requirements of those legal regulations and the fulfilment of legal obligations. The personal data of SERVICE RECEIVING PERSONS OR THEIR AUTHORITIES are also processed within the scope of the commercial activity and legal relationship with the data subject.
- Personal Data is also processed in our Relevant Units for the purpose of:
  1. Execution of emergency management processes
  2. Execution of information security processes
  3. Execution of Employee Candidate / Intern / Student Selection and Placement Processes
  4. Execution of Application Processes of Employee Candidates
  5. Execution of Employee Satisfaction and Loyalty Processes
  6. Fulfillment of Employment and Legislation Obligations for Employees
  7. Execution of Benefits and Benefits Processes for Employees
  8. Execution of audit/ethical activities
  9. Execution of training activities
  10. Execution of access authorizations

11. Execution of activities in accordance with the legislation
12. Execution of finance and accounting affairs
13. Execution of loyalty processes to company/products/services
14. Ensuring physical space safety
15. Execution of assignment processes
16. Monitoring and execution of legal affairs
17. Execution of internal audit/investigation/intelligence activities
18. Execution of communication activities
19. Planning Human Resources Processes
20. Execution / Supervision of Business Activities
21. Execution of Occupational Health / Safety Activities
22. Receiving and Evaluating Suggestions for Improvement of Business Processes
23. Execution of Business Continuity Activities
24. Execution of Service Procurement Processes
25. Execution of After-Service Sale Support Services
26. Execution of Service Sales Processes
27. Execution of Service and Operation Processes
28. Execution of customer relations processes
29. Execution of activities aimed at customer satisfaction
30. Organization and activity management
31. Execution of performance evaluation processes
32. Execution of risk management processes
33. Execution of storage and archival activities
34. Execution of contract processes
35. Execution of sponsorship activities
36. Execution of strategic planning activities
37. Follow-up of requests / complaints
38. Ensuring the safety of movable goods and resources
39. Execution of Wage Policy
40. Ensuring the security of data controller operations
41. Execution of Talent / Career Development Activities
42. Providing information to authorized persons, institutions and organizations
43. Execution of management activities
44. Creating and tracking visitor records

- For occupational health and safety, general safety and product safety purposes, the camera monitoring activity in the workplace is carried out taking into account the legitimate interests of Data Controller, provided not to harm the fundamental rights and freedoms of our visitors, the persons whose data is processed in this context and especially the employees.

3. SECTION: STORAGE, DELETION, DESTRUCTION AND ANONYMIZATION OF PERSONAL DATA

Although it has been processed in accordance with the provisions of the relevant law as set forth in Article 138 of the Turkish Penal Code and article 7 of this Law, personal data are deleted, destroyed or anonymized at the request of the data subject or at Data Controller's own discretion in case the reasons requiring its processing eliminated.

I. STORAGE OF PERSONAL DATA AND STORAGE PERIODS

Data Controller stores the personal data for the period specified in the relevant legislation if stipulated in the relevant laws and legislation. If no period of time has been regulated in the legislation on how long personal data required to be stored, the personal data is processed for a period of time which are determined by taking into account the statute of limitations/impairment periods that may arise within the scope of the legal relationship.

II. DELETION, DESTRUCTION AND ANONYMIZATION OF PERSONAL DATA

Although it has been processed in accordance with the provisions of the relevant law as set forth in Article 138 of the Turkish Penal Code and article 7 of Law, personal data are deleted, destroyed or anonymized at the request of the data subject or at Data Controller's own discretion in case the reasons requiring its processing eliminated. In this context, Data Controller fulfils its relevant obligation in line with the methods described in this section.

1. Deletion of Personal Data

A) Deletion Operation of Personal Data

Although it has been processed in accordance with the provisions of the relevant law personal data may be deleted at the request of the data subject or at Data Controller's own discretion in case the reasons requiring its processing eliminated. The deletion of personal data is the process of making personal data inaccessible and nonreusable in any way **for the relevant users**. Data Controller takes all necessary technical and administrative measures to ensure that the deleted personal data is inaccessible and nonreusable for the relevant users.

B) Deletion Process of Personal Data

The process to be followed in the process of deleting personal data is as follows:

- Determination of personal data that will be the subject of deletion.
- Identification of relevant users for each personal data using an access authorization and control matrix or similar system.
- Identification of the authorizations and methods of the relevant users such as access, restore, reuse.
- Closing and eliminating the access, restore, reuse authorizations and methods of the relevant users within the scope of personal data.

C) Deletion Methods of Personal Data

Since personal data can be stored in various recording media, it is deleted with methods compatible with the recording media.

2. Destruction of Personal Data

A) Destruction Operation of Personal Data

Although it has been processed in accordance with the provisions of the relevant law personal data may be destroyed at the request of the data subject or at Data Controller's own discretion in case the reasons requiring its processing eliminated.

The destruction of personal data **is the process of making personal data inaccessible, nonreturnable and nonreusable by anyone in any way**. Data Controller takes all necessary technical and administrative measures related to the destruction of personal data.

B) Destruction Methods of Personal Data

In order to destroy personal data, all copies of the data are identified and the systems in which the data are located are destroyed one by one.

3. Anonymization of Personal Data

A) Anonymization Operation of Personal Data

Anonymization of personal data is rendering personal data impossible to link with an identified or identifiable natural person, even by use of matching them with other data. Data Controller may anonymize personal data when the reasons requiring the processing of personal data processed in accordance with the law are eliminated. Anonymization of personal data is carried out by rendering it impossible to link with an identified or identifiable natural person, even by use of restoring by Data Controller or receiver groups and/or matching them with other data and use of appropriate techniques in terms of the recording environment and related field of activity. Data Controller takes all necessary technical and administrative measures for the anonymization of personal data.

Personal data anonymized in accordance with Article 28 of the Law may be processed for purposes such as research, planning and statistics. Such processing are outside the scope of the Law and the explicit consent of the data subject shall not be sought.

B) Anonymization Methods of Personal Data

Anonymization is preventing the identification of the Data subject by extracting or modifying all direct and/or indirect identifiers in a dataset or losing the ability to be distinguishable in a group or crowd in such a way that it cannot be linked to a natural person. Data that does not point to a particular person as a result of preventing or losing these features is considered anonymized data. The purpose of anonymization is to break off the link between the data and the person that this data identifies. All operations of breaking off the links that are carried out by automated or non-automated methods such as grouping, masking, derivation, generalization, randomization applied to records in the data recording system where personal data is kept are called methods of anonymization. The data obtained as a result of the application of these methods should not be able to identify a particular person.

SECTION 5: RIGHTS OF DATA SUBJECT

I. SCOPE OF THE RIGHTS OF THE DATA SUBJECTAND EXERCISE OF THESE RIGHTS

1. Rights of the Data Subject

The persons whose personal data is processed by Data Controller have the following rights:

- ✓ To learn whether the personal data are processed or not,
- ✓ To request information if the personal data are processed,
- ✓ To learn the purpose of the data processing and whether this data is used for intended

purposes,

- ✓ To know the third parties to whom his/her personal data is transferred at home or abroad,
- ✓ To request correction of personal data in case of incomplete or incorrect processing and to request the notification of the transaction made within this scope to third persons to whom the personal data are transferred,
- ✓ To request the deletion or destruction of personal data in the event that the reasons requiring their processing are eliminated, and to request the notification of the transaction made within this scope to third persons to whom the personal data are transferred, although it was processed in accordance with the provisions of Law and other relevant laws,
- ✓ To object to the processing, exclusively by automatic means, of his personal data, which leads to an unfavourable consequence for the person himself/herself,
- ✓ To request compensation for the damage arising from the unlawful processing of the personal data.

2. Exercise of the Rights of Data Subject

It is necessary and sufficient for the Data Subject to communicate their demands regarding exercising their rights mentioned above to Data Controller by using the Data Subject Application Form available on the Data Controller's website in accordance with article 13 paragraph 1 of the Law with the following methods;

In the application:
Name, surname and if the application is written, the signature, T.R. Identification Number for Turkish nationals, for foreigners; nationality, passport number or identification number, if any, the notification address or workplace address, the e-mail address based on the notification, telephone and fax number, the subject of the request, must be present. Information and documents related to the subject are added to the application.

In order for a person other than the data subject to make a request, there must be a power of attorney issued by the data subject on behalf of the applicant. In the application containing your explanations of the right you have as data subject; the matter you are requesting must be clear and understandable, the subject you are requesting is related to you or if you are acting on behalf of someone else, you must be authorized and to document your authority, the application must include identification and address information, and documents that certify your identification must be included in the application.

3. Responding to Applications

If the Data subject submits his request to the Data Controller in accordance with the prescribed procedure, Data Controller will conclude the relevant request free of charge as soon as possible and within thirty days at the latest according to the nature of the request. But if the transaction requires an additional cost, the fee in the tariff determined by the Board will be charged by Data Controller. Data Controller may request information from the Data subject in order to determine whether the applicant is the Data subject. In order to clarify the issues contained in the application of the Data subject, Data Controller may address questions to the Data subject about his application.

SECTION 6: ENSURING THE SECURITY OF PERSONAL DATA

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

Data Controller takes all necessary technical and administrative measures to ensure lawful processing of personal data. In this context,

- ✓In order to fulfil the clarification obligation of Data Controller for Persons Concerned in a complete and accurate manner, the "**Principles of Clarification in the Processing of Personal Data Policy**" has been put into effect.
- ✓Employees are informed about the protection of personal data and lawful processing of personal data.
- ✓All the activities carried out by Data Controller are analysed in detail in all business units and as a result of this analysis, personal data processing activities are revealed specific to the activities carried out by the relevant business units.
- ✓Personal data processing activities carried out by the business units of Data Controller; the requirements to be fulfilled in order to ensure compliance of these activities with the personal data processing requirements sought by law No. 6698 are determined specific to each business unit and the detail activity it carries out.
- ✓The contracts and documents governing the legal relationship between Data Controller and its employees are annotated with records imposing obligation not to process, disclose and use personal data except for the Data Controller's instructions and exceptions imposed by law and employees' awareness in this regard is created and audits are carried out.
- ✓The contracts and documents governing the legal relationship between Data Controller and the third parties that process the data for which Data Controller is responsible re annotated with records imposing obligation not to process, disclose and use personal data except for the Data Controller's instructions and exceptions imposed by law and the "**Principles of Personal Data Protection Procedures in Third Party Relations**" has been put into effect in this regard.

II. TECHNICAL AND ADMINISTRATIVE DATA MEASURES TAKEN IN THE PROCESSING OF SENSITIVE DATA

The law attributes special importance to a number of personal data due to the risk of causing victimization or discrimination of individuals when processed unlawfully. These are; data related to race, ethnicity, political opinion, philosophical belief, religion, sect or other beliefs, appearance and clothing, association, foundation or trade union membership, health, sexual life, criminal conviction and security measures, and the biometric and genetic data. Data Controller acts responsibly in the protection of sensitive data, which is determined as "special quality" by Law and processed lawfully. In this context, the technical and administrative measures taken by Data Controller for the protection of personal data are carefully applied in terms of sensitive data and necessary audits are carried out.

In this context,

- ✓Regular trainings are given on the law and related regulations and sensitive data issues for employees involved in the processing of sensitive data, confidentiality agreements are made, the scopes and durations of the authorization of the users authorized to access the data are clearly defined, authorization controls are carried out, the authorizations of employees who have changed duties or left their jobs are immediately removed and in this context the inventory

allocated to them by the Data Controller is being returned.

- ✓ If the environments where sensitive data are processed, stored and/or accessed are electronic environments, data are stored using cryptographic methods. Cryptographic keys are kept in safe and different environments, transaction logs of all activities performed on the data are logged securely, security updates of the environments where the data is located are monitored and necessary security tests are carried out, test results are recorded.
- ✓ If the data is accessed through a software, user authorizations are made for this software, security tests of this software are carried out regularly and test results are recorded. If remote access to data is required, at least a two-step authentication system is provided.
- ✓ If environments where sensitive data is processed, stored and/or accessed are physical environments, adequate security measures (against electrical leakage, fire, flooding, theft, etc.) are taken according to the nature of the environment in which sensitive data are located, and unauthorized entry and exit are prevented by ensuring the physical security of these environments.
- ✓ If sensitive data is to be transferred, if the data must be transferred via e-mail, it is ensured that it is transferred encrypted with the corporate e-mail address or using the Registered E-Mail (REM) account.
- ✓ If private data is transferred via physical environments,. the transfer of private data in printed form is required, necessary measures are taken against risks such as theft, loss of documents or being seen by unauthorized persons and the documents are sent in the form of "**confidential documents**".
- ✓ In addition to the above-mentioned measures, technical and administrative measures are taken into account to ensure the appropriate level of security specified in the Personal Data Security Guide published on the website of the Personal Data Protection Board.

III. TECHNICAL AND ADMINISTRATIVE MEASURES TAKEN TO PREVENT UNLAWFUL ACCESS TO PERSONAL DATA

Data Controller takes technical and administrative measures to prevent imprudent or unauthorized disclosure, access, transfer or all unlawful access of personal data in other ways.

1. Technical Measures Taken to Prevent Unlawful Access to Personal Data The main technical measures taken by Data Controller to prevent unlawful access to personal data are listed below:

A) Ensuring Cybersecurity

To ensure personal data security primarily cybersecurity products are used, but measures are not limited to this. Measures such as firewalls and gateways are taken. Unused software and services are removed from devices.

B) Software Updates

With patch management and software updates it is ensured that the software and hardware work properly and that the security measures taken for the systems are checked regularly.

C) Access Limitations

Access to systems containing personal data is also limited. In this context, employees are granted access to the extent necessary for their work and duties and their powers and responsibilities, and

access to related systems is provided by using usernames and passwords. When creating these keys and passwords, it is ensured that combinations of uppercase letters, numbers and symbols are preferred instead of numbers or sequences of letters associated with personal information that can be easily guessed. Accordingly, access authorization and control matrix is created.

D) Encryption

In addition to the use of strong keys and passwords, access limitation is carried out with methods such as limiting the number of password entry attempts, ensuring that keys and passwords are changed at regular intervals, opening the administrator account and admin authorization for use only when needed, and limiting access to employees who have been dismissed from the data controller by means of deleting the account or closing the logins without losing time.

E) Anti-Virus Software

To protect against malware, products such as anti-virus and anti-spam are also used, which regularly scan the information system network and detect hazards, and the files required are regularly scanned by keeping them up to date. If personal data is to be obtained from different websites and/or mobile application channels, connections are made via SSL or a safer way.

F) Tracking Personal Data Security

- Checking which software and services are running in information networks,
- Determining whether there is a leak in information networks or an activity that should not be,
- Regular keeping of transaction activity records of all users (such as log records),
- Reporting security issues as quickly as possible,

is carried out, an official reporting procedure is established for employees to report security vulnerabilities in systems and services or threats which take advantage of such vulnerabilities.

In cases of undesired events such as an information system crash, malicious software, decommissioning attack, missing or incorrect data entry, violations of privacy and integrity, abuse of the information system, evidences thereon are collected and stored securely

G) Ensuring the Security of the Environments Containing Personal Data

If personal data are stored on the devices or in printed form which are located in the Data Controller's premises, physical security measures are taken against threats such as theft or loss of such devices and papers. The physical environments containing personal data are protected against external risks (fire, flood etc.) by suitable methods, and the entries to / exits from such environments are controlled.

If personal data are on electronic environments, access between network components can be restricted or separated to prevent personal data security breaches.

Measures at the same level are also taken for hard copies, electronic environments and devices (laptop, mobile phone, flash disk) containing personal data belonging to the Data Controller located outside of Data Controller's premises. Personal data to be transferred by e-mail or mail are also sent carefully and with adequate measures taken.

If employees have access to the information system network with their personal electronic devices,

adequate security measures are also taken for them.

Access control authorization and/or encryption methods are used against situations such as loss or theft of devices containing personal data. In this context, the password key is stored in the environment which is only accessible to authorized persons, and unauthorized access is prevented thereby.

Hard copy documents containing personal data are also stored in a locked environment which is only accessible to authorized persons, and unauthorized access to such documents is prevented thereby.

H) Storage of Personal Data on Cloud

Practices for storing personal data on the cloud can also be applied when necessary. In this case, the Data Controller must assess whether the security measures taken by the cloud storage service provider are also adequate and appropriate. In this context, the measures specified in the guidelines and recommendations of the Board are taken into account.

I) Procurement, Development and Maintenance of Information Technology Systems

Security requirements are taken into account by the Data Controller when determining the needs related to the procurement, development of new systems or improvement of existing systems.

J) Backup of Personal Data

If any personal data is damaged, destroyed, stolen or lost due to any reason whatsoever, the Data Contoller enables recovery by making use of the backed-up data within the shortest time possible. The backed-up personal data is only accessible to the system administrator and the data set backups are excluded from the network.

2. Administrative Measures taken to Prevent Unlawful Access to Personal Data

The main administrative measures taken by Data Controller to prevent unlawful access of personal data are listed below:

- ✓ Employees are informed and trained about technical measures to be taken to prevent unlawful access to personal data.
- ✓ Employees are informed that they cannot disclose the personal data they have learned to anyone else in violation of the provisions of the Law and cannot use it for any purpose other than for the purpose of processing, and this obligation will continue after their departure from office and necessary commitments are taken from them accordingly.
- ✓ Personal Data Protection Policies and Procedures are determined and within the scope of policies and procedures; regular checks are carried out, the checks carried out are documented and the issues that need to be improved are determined. Also, the risks that may arise for each category of personal data and how to manage security breaches are also clearly determined.
- ✓ Reducing Personal Data as Much as Possible: Personal data must be accurate and up to date, maintained for the period stipulated in the relevant legislation or required for the purpose for which they are processed However, it is evaluated that whether inaccurate, outdated and non-purpose data is still needed, and personal data that is not needed is deleted, destroyed or anonymized by the personal data storage and destruction policy.
- ✓ Managing Relationships with Data Processors: When Data Controller receives services from

data processors to meet the need for Information Technologies, when receiving services it is conducted by ensuring that the level of security provided by them is provided at least in terms of personal data of those who process such data. In this context, protective regulations regarding the protection of personal data are introduced in the agreements signed with the data processor.

IV. STORING PERSONAL DATA IN SAFE ENVIRONMENTS

Data Controller takes the necessary technical and administrative measures according to technological facilities and application cost for the storage of personal data in safe environments and to prevent destruction, loss or alteration of personal data for unlawful purposes.

1. Technical Measures Taken to Store Personal Data in Safe Environments

The main technical measures taken by Data Controller for the storage of personal data in safe environments are listed below:

- ✓ Systems suitable for technological developments are used for the storage of personal data in safe environments.
- ✓ Technical security systems are established for storage areas, technical measures taken are periodically audited by the audit mechanism determined by Data Controller, and the necessary technological solutions are provided by reassessing the issues that pose a risk.
- ✓ All necessary infrastructures are used in accordance with the law to ensure the safe storage of personal data.

2. Administrative Measures Taken to Store Personal Data in Safe Environments

The main administrative measures taken by Data Controller for the storage of personal data in safe environments are listed below:

- ✓Employees are informed about ensuring the safe storage of personal data.
- ✓In case of procurement of an external service due to technical requirements for the storage of personal data by Data Controller, provisions regarding that the persons to whom personal data are transferred will take the necessary security measures for the protection of personal data and that these measures will be ensured to be observed in their own organizations are included in the agreements concluded with the relevant companies to which the personal data are transferred in accordance with the law, and in this regard, acted in accordance with the provisions in the Data Controller's **Principles of Personal Data Protection in Third Party Relations Procedure**.

V. TRAINING

- ✓Data Controller provides its employees with the necessary trainings within the scope of Policies and Procedures and Law and Regulations on the protection of Personal Data.
- ✓ In the trainings, the definitions of Sensitive Data and the practices for its protection are specifically mentioned.

VI. AUDIT

1. Increasing The Awareness of Business Units on The Protection and Processing of Personal Data and Auditing

Data Controller provides necessary notifications to business units to raise awareness to prevent unlawful processing of personal data, unlawful access to data and to ensure the retention of data.

2. Increasing The Awareness of Business Partners and Suppliers on The Protection and Processing of Personal Data and Auditing

Data Controller provides necessary information to its business partners in order to prevent unlawful processing of personal data, to prevent unlawful access to data and to increase awareness to ensure the retention of data.

3. Audit of Measures Taken on The Protection of Personal Data

Data Controller has the right to regularly, at all times and directly audit that all employees, departments and contractors of the Data Controller are acting in accordance with these policies and Regulations on the protection of Personal Data, without any prior notice or in this context carries out the necessary routine audits or have them carried out. The results of this audit are evaluated within the scope of the internal functioning of the Data Controller and necessary activities are carried out to improve the measures taken.

Measures to be taken in the event of unauthorized disclosure of personal data; Data Controller executes the system that allows the personal data processed in accordance with Article 12 of the Law to be notified to the Data Subject and the Board as soon as possible if they are obtained by others by unlawful means.