ELELE DÖŞEME
SANAYİ ve TİCARET A.Ş.

PERSONAL DATA PROCESSING AND

PROTECTION POLICY

INTRODUCTION

*We, as **ELELE DÖŞEME SANAYİ ve TİCARET A.Ş.,***

operating in the subsidiary automotive industry sector for many years and providing service to our clients,

We are aware of our responsibility for the security and legal protection of personal data that is regulated as a constitutional right and we attach utmost importance to the confidentiality and security of your personal data processed within our company.

Accordingly, we have been founding systems related to operating any kind of activities that are necessary for alignment with all legislation, especially with the Turkish Personal Data Protection Law no. 6698, and have been examining the operability of these systems meticulously.

In light of all these explanations "Personal Data Processing and Protection Policy "is amended by our company and entered into force that regulates the obligations stipulated under the scope of Personal Data Protection Law no. 6698 and the relevant principles and procedures to be applied within this scope.

CONTENTS

PART 1: INTRODUCTION

1.1. Definitions and Abbreviations:

Explicit Consent	This means freely expressed consent that is related to a specific subject and based on information.
Constitution	This refers to the Turkish Constitution published in the Official Gazette with the journal number of 17863 (repeated) on November 9, 1982
Anonymization	This refers to rendering personal data by no means identified or identifiable with a natural person even by linking with other data
Communique on Obligation to Inform	This refers to Communique on the Principles and Procedures for Fulfilment of Information Obligation which is published in the Official Gazette with the journal number of 30356 on March 10, 2018
Data Recording Medium	It is any kind of place where personal data is processed completely or partially automatically or by non-automatic means, provided that being part of any data recording system.
Personal Data	This refers to all and any information relating to an identified or identifiable natural person (e.g. name-surname, ID no, e-mail, address, date of birth, credit card number etc.).
Processing of Personal Data	This refers to any operation which is performed upon personal data such as collection, recording, storage, preservation, alteration, adaptation, disclosure, transfer, retrieval, making available for collection, categorization or blocking its use by wholly or partly automatic means or otherwise than by automatic means which form part of a filing system.
Data Subject(s)	This refers to natural persons whose personal data are processed. These persons may include but not limited to employees, customers, business partners, shareholders, officials, potential customers, prospective employees, trainees, visitors, suppliers, corporate employees, and other third parties with whom the Company has business relationships.
Deletion of Personal Data	The deletion of personal data is; rendering personal data non-accessible and non-reusable to the relevant users.
Regulation on Destruction	This refers to the Regulation on the Deletion, Destruction or Anonymization of Personal Data published in the Official Gazette with the journal number of 30224 on October 28, 2017 and entered into force as of 1 January 2018.
Destruction of Personal Data	The process of making personal data inaccessible, non-retrievable and non re-usable by anyone.
PDPA/ the Board	This refers to the Personal Data Protection Authority.
PDP Law	This stands for Personal Data Protection Law that is published in the Official Gazette with the journal number of 29677 on April 7, 2016.
Sensitive Personal Data	Data relating to race, ethnic origin, political opinions, philosophical beliefs, religion, sect or other beliefs, appearance and dressing, membership of association, foundation or trade-union, health, sexual life, criminal conviction and security measures, and biometrics and genetics are sensitive personal data..
Periodic Destruction	This refers to the process of deletion, destruction or anonymization to be performed exofficio and at repeated intervals in the event that all the processing conditions of the personal data in the law are eliminated.

Policy	This refers to Personal Data Processing and Protection Policy belonging to Elele Döşeme Sanayi ve Ticaret A.Ş.
(our) Company "ELELE"	This refers to Elele Döşeme Sanayi ve Ticaret A.Ş.
Data Processor	Refers to a real or legal person outside the organization of the Data Controller who process personal data on his behalf based on the authority given by the Data Controller. These individuals are a separate real or legal person who processes personal data within the framework of the instructions given to her and is authorized by the Data Controller by a contract.
Data Controller	This refers to the real or legal person who determines the purposes and means of the processing of personal data, and who is responsible for establishment and management of the filing system.
Communique on Application to Data Controller	refers to Communiqué on Procedures and Principles of Application to the Data Controller published in the Official Gazette with the journal number of 30356 on March 10, 2018.
By-law on Data Controllers Registry	refers to the by-law published in the Official Gazette with the journal number of 30286 on December 30, 2017.

1.2. Purpose and the Scope of the Policy:

Protection of personal data is a field that ELELE gives utmost effort for acting in compliance with all legislation in force. In the scope of this ELELE Personal Data Protection and Processing Policy ("Policy"), the principles adopted in conducting the activities of personal data processing by our Company and the fundamental principles adopted in terms of compliance of our company's activities of personal data processing with the regulations in the Personal Data Protection Law no.6698 ("Law") are explained, thus, our Company provides required transparency by informing data subjects. With full awareness of our responsibility in this context, your personal data is processed and protected under this Policy.

The main purpose of this Policy is to explain the activities of personal data processing that are conducted legally within our Company and to inform Data Subjects about personal data processed by our Company. Accordingly, our aim is to provide transparency by informing persons whose personal data are processed by our Company, especially our employee candidates, visitors, shareholders of the company, potential customers and suppliers and the third parties.

The provisions of this Policy includes any and all personal data of the Company's shareholders, our hired employees and employee candidates, our visitors, current and potential clients or suppliers, or other third parties that are processed within our company and its subsidiary by fully or partially through automatic means; or provided that the process is a part of any data registry system through non-automatic means.

1.3. The Implementation of the Policy and Relevant Legislation:

The relevant legal regulations in force regarding the processing and protection of personal data will primarily find an application. If there is a discrepancy between the current legislation and the Policy, our Company accepts that the current legislation will apply. The policy is regulated by embodying the regulations introduced by relevant legislation within the scope of Company practices.

1.4. Enforcement of the Policy:

This Policy has entered into force on the date of its publication. In case of the wholly or partially change of provisions of the Policy, the date of enforcement will be updated.

This Policy is published on https://www.elelefoam.com/ and is made available to data subjects on demand of the data subjects.

PART 2: GENERAL PROVISIONS OF PERSONAL DATA PROTECTION

2.1. Security of the Personal Data:

According to Article 12 of the PDP Law, our Company takes necessary measures to prevent the illegal evaluation, access, transfer of personal data or the security vulnerability may occur in other ways, with respect to the nature of the protecting data. In this scope, our Company takes administrative measures, conducts audits and making audits done aimed at providing required security level, in compliance with the guides published by PDPA.

2.2. The Fundamental Principles:

Our company is aware that the personal data that is processed to ensure legal compliance must comply with the general principles and provisions set out in the Constitution, the PDP Law, and other relevant legislation. In this regard, the fundamental principles of all personal data processing activities are always taken into consideration within the scope of Article 4 of the PDP Law:

a. Processing lawfully and conformity with rules of bona fides: In the processing of personal data, our Company acts under the principles outlined in the legal regulations and the general rules of bona fides and honesty.

b. Principle of accuracy and being up to date, where necessary: Our Company establishes and applies the systems to ensure accuracy and recency of personal data processed by taking into account the fundamental rights and the legitimate interests of the data subjects.

c. Principle of being processed for specified, explicit, and legitimate purposes: Before and during the processing of personal data, our Company processes personal data toward legal purposes that set forth clearly and within the framework of legal and contractual purposes.

d. Principle of being relevant with, limited to and proportionate to the purposes for which they are processed: The personal data processed is limited to that is adequate, appropriate and necessary concerning legal regulations, contractual provisions and purposes set forth by the Company policy. Within the framework of this basic principle, our company has minimized the processing of personal data.

e. Principle of being retained for the period of time stipulated by relevant legislation or the purpose for which they are processed: ELELE has determined the retention period within the scope of Article 9 of the By-law on Data Controllers Registry. In this regard, the following issues are taken into consideration when determining the storage periods:

- The period generally accepted in the sector which ELELE operates,
- The period that requires processing of personal data in the relevant data category and to continue legal relationship with the data subject,
- The period to be valid for the legitimate interest to be obtained by ELELE in accordance with lawfulness and fairness, depending on the purpose of processing relevant data category,
- The period in which the risks, costs and responsibilities arising from the storage of the relevant data category depending on the purpose of processing shall continue legally,
- Whether maximum storage period to be determined is appropriate to keep the relevant data category accurate and up-to-date where necessary,
- Time period in which the data controller is obliged to retain personal data given in the relevant data category pursuant to its legal obligation,
- Period of limitation determined by the data controller for assertion of a right relating to personal data in the relevant data category.

2.3. Protection of Sensitive Personal Data:

Special importance is attributed to Sensitive Personal Data by law because of the risk of causing victimhood or discrimination when processed illegally. These data are personal data relating to race, ethnic origin, political opinions, philosophical beliefs, religion, sect or other beliefs, appearance and dressing, membership of association, foundation or trade-union, health, sexual life, criminal conviction and security measures, and biometrics and genetics.

It is treated sensitively in the protection of personal data which is defined as “sensitive personal data” by law and processed in accordance with the law. In this regard, technical and administrative measures taken for the protection of personal data are being implemented carefully and necessary audits provided within ELELE.

2.4. Raising Awareness and Supervisor of Departments Regarding Protection and Processing of Personal Data

ELELE provides the necessary education to provide illegal processing of and illegal access to personal data and to raise awareness towards storing personal data. Several systems have founded for raising awareness towards the protection of personal data and where necessary, we work with the consultants in this matter. Accordingly, our Company has been giving pieces of training and seminars to its employees for implementation of PDP Law, up-dating, and renewing its educations in parallel to related regulation.

PART 3: THE ISSUES RELATED TO PROCESSING OF PERSONAL DATA

3.1. Conditions of Processing of Personal Data:

Except for data subject giving her/his explicit consent, the basis of the activity of personal data processing may be either one or more than one of the conditions below:

i. **Explicit consent of data subject**: One of the conditions of processing personal data is the explicit consent of data owner. The explicit consent of data subject should be expressed freely, related to a specific subject, and based on information.

In case of the presence of the conditions of personal data processing, personal data can be processed without a requirement of explicit consent of data subject.

ii. **It is expressly permitted by any law**: If the personal data of the data owner is expressly stipulated by the Law, in other words, if there is a provision regarding personal data processing in related law, this data processing condition exists.

iii. **Inability to Obtain Explicit Consent of Data Subject due to Physical:** The personal data of the data owner can be processed when it is necessary to protect the life or physical integrity of the data owner or another person where the data owner is physically or legally incapable of giving consent or his/her consent.

iv. **Direct Relation to the Execution or Performance of the Contract**:. This condition counted as fulfilled when it is necessary to process the personal data provided that the processing is directly related to the execution or performance of the contract.

v. **Fulfilling Legal Obligations of the Company**: Personal data of the data owner can be processed when it is compulsory for our Company to fulfil its legal obligations.

vi. **Disclosure of Personal Data by Personal Data Owner**: If the relevant information is revealed to the public by the data owner herself/himself, the related personal data can be processed as limited by the purpose of disclosure.

vii. **Obligatory Data Processing for the Institution or Protection of a Right:** The personal data of the data owner shall be processed when it is compulsory for the institution, usage, or protection of a right.

viii. **It is Obligatory for the Legitimate Interests of our Company:** The personal data of the data owner can be processed if it is necessary for the legitimate interests of our Company, provided that no harm is done to the fundamental rights and freedoms of the data owner.

3.2. Processing of Sensitive Personal Data

Sensitive personal data processed by our Company in line with the principles set out in this Policy and by taking all necessary administrative and technical precautions, including the methods to be determined by the Board, in the following circumstances:

3.2.1. *Personal data other than relating to health and sexual life of the data owner may be processed without obtaining explicit consent of the data owner in the circumstances stipulated by the Laws, in other words, if there is a clear provision regarding the processing of personal data in the law that the activity is subject to. Otherwise, for processing of the sensitive personal data, explicit consent of the data owner is taken.*

3.2.2. *Personal data concerning the health and sexual life may be processed in order to protect public health, protective medicine, medical diagnosis, treatment and maintenance services, plan and manage health services and finance, by persons or authorized institutions and organizations who are under the confidential obligation. Otherwise, for processing of the sensitive personal data, explicit consent of the data owner is taken.*

3.3. Informing of the Data Subject:

ELELE informs the Data Subjects in line with Article 10 of the Law and secondary legislation. In this scope, our Company informs data subjects on the identity of the controller, the purpose of data processing, to whom and for what purposes the processed data may be transferred, the method and legal reason of collection of personal data, and the rights of data subjects regarding processing of personal data.

3.4. Transfer of Personal Data:

By taking necessary security precautions regarding the legal personal data processing purposes, our Company is able to transfer the personal data and sensitive personal data of Data Subject to third parties(third party companies, public and private authorities, natural persons). Our Company acts in line with the regulations foreseen in Article 8 and Article 9 of the Law.

3.4.1 **Transfer of personal data abroad**: In the presence of one or more than one of the following conditions, by the necessary care is shown and all security precautions are taken including the ones foreseen by Authority, personal data may be transferred to third parties by our Company:

- Explicit consent of the Data Subject,
- It is clearly provided for by the laws that the activities of transfer or personal data,
- The transfer of personal data by the Company is necessary and directly related to the conclusion or fulfilment of a contract
- The transfer of personal data is obligatory for the legitimate interests of our Company,
- Provided that the personal data is revealed to the public by the data owner herself/himself, the transfer of the related personal data limited by the purpose of disclosure by our Company,
- The transfer of the personal data of data owner is compulsory for the institution, usage, or protection of a right of the Company, data owner or third party,
- The transfer of the personal data is necessary for the legitimate interests of the Company provided that no harm is done to the fundamental rights and freedoms of the data owner.
- The transfer of the personal data is obligatory to protect the life or physical integrity of the data owner or another person where the data owner is physically or legally incapable of giving consent or his/her consent.

In addition to provisions above, personal data may be transferred to foreign countries that are announced as having an adequate level of protection by PDP Authority ("Safe Country") in the presence of conditions above. In case of an adequate level of protection does not exist, personal data may be transferred to foreign countries("Foreign Country that has a Data Controller who Undertakes the Adequate Level of Protection")that the data controllers undertake the adequate level of protection in written and has a permit from the Authority, in line with the data transfer conditions foreseen in the legislation.

In case of the list of Safe Countries is not announced, personal data may be transferred by either the explicit consent of Data Subject is taken or the undertaking of the Company in the foreign country signed by Data Subject is submitted to Authority's permit.

3.4.2 **Transfer of Sensitive Personal Data:** Special categories of personal data may be transferred by our Company in line with the provisions on this Policy, by taking all necessary precautions including the methods that Authority specified and in the presence of the following conditions:

(i) **Personal data other than relating to health and sexual life** may be transferred without obtaining explicit consent of the data owner in the circumstances stipulated by the Laws, in other words, if there is a clear provision regarding the transfer of personal data in the law that the activity is subject to. Otherwise, explicit consent of the data owner is taken.

(ii) **Personal data relating to health and sexual life** may be transferred in order to protect public health, protective medicine, medical diagnosis, treatment and maintenance services, plan and manage health services and finance, by persons or authorized institutions and organizations who are under the confidential obligation. Otherwise, explicit consent of the data owner is taken.

In addition to provisions above, personal data may be transferred to Safe Countries in the presence of any of the conditions above. In case of the absence of an adequate level of protection, personal data may be transferred to Foreign Countries that have a Data Controller who Undertakes the Adequate Level of Protection, in line with the transfer conditions on the legislation.

3.5. Informing of the Data Subject regarding Transfer:

ELELE informs the Data Subjects regarding the transfer of their personal data pursuant to Article 10 of the Law and secondary legislation. In this scope, our Company informs data subjects on the identity of the controller, the purpose of data transfer, to whom and for what purposes the data may be transferred, the method and legal reason of collection of personal data, and the rights of data subjects regarding transfer of personal data.

PART 4: PURPOSES OF PERSONAL DATA PROCESSING

Our Company processes personal data limited to conditions and towards purposes below in frame of the conditions in Article 5 and 6 of the PDP Law.

- Conduct of Emergency Management Processes
- Conduct Of İnformation Security Processes
- Conduct of Employee Candidate / Trainee / Student Selection Procedures
- Conduct of Application Processes of Employee Candidates
- Conduct of Employee Satisfaction and Loyalty Processes
- Conduct of Contractual and Regulatory Obligations for Employees
- Conduct of Side Benefits and Profits for Employees
- Conduct of Supervision /Ethical Activities
- Conduct of Educational Activities
- Conduct of Access Authorization
- Conduct of Appropriate Implementation of Activities İn Line with The Legislation
- Conduct of Financial and Accounting Works
- Supply of the physical space Security
- Conduct of the assignment process
- Following-up and execution of legal affairs
- Conduct of Communication Activities
- Planning Human Resources Processes
- Conduct and control of business activities
- Execution of Occupational Health / Safety Activities
- Conduct of Business Sustainability Activities
- Conduct of Logistics Activities
- Conduct of Purchasing Activities of Products / Services
- Conduct of Selling Activities of Products/Services
- Conduct of Product/ Service Producing and Operation Processes
- Conduct of Customer Relationship Management Processes
- Conduct of Activities for Customer Satisfaction
- Conduct of Organization and Activities
- Conduct of Marketing Analysis Studies
- Conduct of Risk Management Processes
- Conduct of Storing and Archiving Activities
- Conduct of Contractual Processes
- Conduct of Strategic Planning Activities
- Conduct of Supply Chain Management Processes
- Conduct of Wage Policy
- Foreign Personnel Work and Residence Permit Procedures
- Informing the Authorized Persons, Institutions and Organisations
- Conduct of Management Activities
- Building and Tracking of Visitor Records
- Employer's obligation to care in selecting employees
- the safety of life and property of people working in the company

In case of absence of processing conditions stipulated into the Article 3/1; the Company obtains the explicit consents of Data Subjects to process personal data.

PART 5: SECURITY OF PERSONAL DATA

Pursuant to Article 12 of the PDP Law, our Company is obliged to take all necessary technical and administrative precautions to prevent the illegal processing and access of personal data and to ensure the proper security level in order to ensure the protection of personal data.

All personal data processed within ELELE is kept strictly confidential and access to such data is limited. No personal data that is not covered by the legal processing conditions in accordance with Article 5 and 8 of the PDP Law is shared with third parties.

In case of determination of a violation of the law/good faith by obtaining personal data by third parties, ELELE is obliged to notify the data subject about this issue as soon as possible and to the PDP Authority, when necessary.

Applicable technical and administrative measures are taken immediately by determining the loss caused by the violation of security of personal data, the possibility of occurrence of risks that may arise regarding data protection and the risk of security violation of personal data processed by our Company. While detecting these risks, it is primarily considered that

(i) Whether the personal data is special categorised or not,
(ii) The level of privacy required by its feature and
(iii) The nature and quantity of the damage that may occur in the case of data security breach.

After the identification and determination of the priority of these risks, control methods and alternative solutions regarding reducing or elimination of such risks are considered toward the principles of cost, applicability and utility, the necessary technical and administrative measures are planned and put into practice.

5.1. Technical Measures

Technical measures taken regarding the personal data processed by our Company are listed below:

- ✓ With the leaking(penetration) tests, the necessary measures are taken by revealing risks, threats and if any, security vulnerabilities oriented our information systems in the Organization.
- ✓ Risks and threats are being constantly watched that may affect the sustainability of information systems with the analysis done by information security incident management in real-time.
- ✓ Access to information systems and authorization of users is done through security policies over the access and authority matrix and the corporate active directory.
- ✓ Necessary precautions are taken for the physical security of the company's information systems equipment, software, and data.
- ✓ To ensure the security of information systems against environmental threats, hardware (access control system that provides only authorized personnel access to the system room, 24/7 monitoring system, ensuring the physical security of the edge switches forming the local area network, fire extinguishing system, air conditioning system etc.) and software (firewalls, attack prevention systems, network access control, systems that prevent harmful software, etc.) measures are taken.
- ✓ Risks for illegal processing of personal data are identified, technical measures are taken to ensure compliance with these risks, and technical controls are made for the measures taken.
- ✓ By establishing access procedures within the company, reporting and analysis studies on access to personal data are carried out.
- ✓ Access to personal data storage areas is recorded and improper access or attempts to access are kept under control.
- ✓ The company takes the necessary precautions to make the deleted personal data inaccessible and non-reusable for the users concerned.
- ✓ If the personal data are obtained illegally by others, an appropriate system and infrastructure have been established by the Company to report this to data subject and the Board.
- ✓ Appropriate security patches are installed by following security gaps and information systems are kept up to date.
- ✓ Strong passwords are used in electronic environments where personal data are processed.
- ✓ Secure record keeping(logging) systems are used in electronic environments where personal data are processed.
- ✓ Data backup programs are used to ensure that personal data are stored securely.
- ✓ Access to personal data stored in electronic or non-electronic environments is restricted by access principles.
- ✓ Efforts are underway to switch to secure protocol (HTTPS) implementation in accessing the Company's website.
- ✓ A separate policy has been determined for the security of special categories of personal data
- ✓ Special categories of personal data security trainings were given to employees involved in special personal data processing processes, confidentiality agreements were made, and the powers of users who have access to data were defined.
- ✓ Electronic environments where special categories of personal data are processed, stored and / or accessed are kept by using cryptographic methods, cryptographic keys are kept in secure environments, all transaction records are logged, security updates of the environments are constantly monitored, regularly performing the necessary security tests and the recording of test results are provided.
- ✓ Adequate security measures are taken in physical environments where special categories of personal data are processed, stored and / or accessed, and unauthorized entries and exits are prevented by ensuring physical security.
- ✓ If special categories of personal data should be transferred via e-mail, it is transmitted in an encrypted form via corporate e-mail address or using a KEP account. If it needs to be transferred via media such as portable memory, CD, DVD, it is encrypted with cryptographic methods and the cryptographic key is kept in a different media. If the transfer between servers in different physical environments is performed, data transfer is performed by installing VPN between servers or by sFTP method. If paper transfer is required, necessary precautions are taken against the risks such as stolen, lost or seen by unauthorized people and the document is sent in **"confidential"** format.

5.2. Administrative Measures

Administrative measures taken regarding the personal data processed by our Company are listed below:

- ✓ Company employees are informed regarding the personal data protection law and processing of personal data legally. Additionally, trainings regarding the current amendments and internal company policies on this subject may be organized, when necessary.
- ✓ All the activities carried out and being carried out within the company were analyzed in detail in all departments and as a result of this analysis, a "personal data inventory" was created. Personal data processing activities have been put forward in specific to commercial activities of the departments.
- ✓ Within the scope of the organization chart, awareness has been created in related departments that are specially determined in order to meet the legal compliance requirements within the scope of the PDP Law.
- ✓ "Everything is forbidden unless it is allowed." principle is adopted. Company employees make the necessary efforts to request the minimum level of personal data as much as possible.
- ✓ Application rules have started to be determined; The necessary administrative measures to ensure the supervision of these issues and the continuity of implementation have started to be implemented through in-house policies and information.
- ✓ Access to personal data is restricted to employees determined in line with the reason for processing of personal data. Employees will be denied access to personal data that they do not use due to their duties.
- ✓ These technical measures will be audited periodically by the Company officials within the framework of the internal audit systems determined by our Company.
- ✓ In order to improve the quality of the employees, trainings are provided on the prevention of unlawful processing of personal data, prevention of unlawful access of personal data, protection of personal data, communication techniques, technical knowledge skills, and other relevant legislation.
- ✓ Confidentiality agreements are signed to employees regarding the activities carried out by the company.
- ✓ The disciplinary procedure to be implemented for employees who do not comply with the security policies and procedures has been prepared.
- ✓ Before starting to process personal data, the Company fulfills its obligation to enlighten data subjects.
- ✓ Information security awareness trainings are provided for employees.

PART 6: RIGHT TO APPLY OF THE DATA SUBJECTS AND USAGE OF THIS RIGHT

Data subjects can benefit some rights stipulated under Article 11 of PDP Law, by applying to our Company regarding personal data that are processed within our Company. In this regard, data subjects have the rights to:

- Learn whether her/his personal data are processed,
- Request information as to processing if her/his data have been processed,
- Learn the purpose of processing of the personal data and whether data are used in accordance with their purpose,
- Know the third parties in the country or abroad to whom personal data are transferred,
- Request correction in case of personal data are processed incompletely or inaccurately,
- Request deletion or destruction of personal data,
- Request informing of third parties to whom personal data are transferred on transactions performed,
- Object to any result that is to her/his detriment by means of analysis of personal data exclusively through automated systems,
- Request compensation for the damages in case the person incurs to damages due to unlawful processing of personal data.

Data subjects may benefit above-mentioned rights by filling in the "**Application Form**" on the website of our Company (https://www.elelefoam.com/) or by sending a petition in which your identity can be determined and includes your requests via the channels specified in the Application Form or the Statement of Application to Data Controller.

As a result of failure to comply with the application procedure stipulated in the Application Form in line with Article 13 of the PDP Law, the applications sent by the Data Subjects will not be considered.

Our company may reject the application of the applicant with the reasons in the following cases:

- Processing of personal data by judicial authorities and execution agencies regarding investigation, prosecution, adjudication or execution procedures,

- Processing of personal data for the purposes of art, history, and literature or science, or within the scope of freedom of expression, provided that national defence, national security, public safety, public order, economic safety, privacy of personal life or personal rights are not violated,
- Processing of personal data within the scope of preventive, protective and intelligence-related activities by public institutions and organizations who are assigned and authorized by law for providing national defence, national security, public safety, public order or economic safety,
- Processing of personal data for purposes such as research, planning and statistics through anonymization with official statistics,
- The requirement of processing of personal data for prevention of crime or investigation of a crime,
- Processing of personal data is necessary for prevention of crime or investigation of a crime,
- The necessity of processing of personal data, deriving from the performance of supervision or regulatory duties, or disciplinary investigation or prosecution by assigned and authorized public institutions and organizations and professional organizations with public institution status.
- Where processing of personal data is necessary for the protection of economic and financial interests of the state related to budget, tax, and financial matters,
- The request of the owner of personal data is likely to block the rights and freedoms of others,
- Requests for disproportionate effort have been made,
- If the information requested is public information.

PART 7: SPECIAL OCCASIONS OF PROCESSING OF PERSONAL DATA

7.1 Monitoring Activities with the Security Cameras:

To provide security by the Company, provided that being limited with corridors and production areas and toward following visitor's entrance and exits monitoring activities are performed at the entrance of the building and the parking area with security cameras. Information on this subject is on the signboards under cameras and our website. The monitoring activities with security cameras are performed in compliance with the Constitution, PDP Law, provisions of this Policy and general principles of law. As follows:

7.1.1 Purpose of Processing Activity:

While performing monitoring activities with the security cameras, our Company acts in line with the principles of compliance with the law and good faith, processing for specific and legitimate purposes and being connected with, limited and restrained to the purpose of processing, that is stipulated in Article 4 of PDP Law.

In order to ensure the security of the physical place, protect the production and trade secrets of the Company, provide security of company's data, provide security of the life and property of the data owner and other persons, and to protect the legitimate interests of both the data owners and the Company, the data processing is conducted by ELELE through recording to data record system automatically.

There are 73 security cameras in our Company. The right to change the number of security cameras toward our Company's requirements is reserved. Security camera recording zones are strictly limited and determined by our Company in line with the purpose of monitoring with the security cameras. Security camera recording zones are limited to areas where security risk is high such as building and facility entrances, corridors, dining hall, production areas etc. Meeting rooms, offices, restrooms and dressing rooms are excluded from the security camera recording zones.

Monitoring activities with security cameras are essential for both providing the security of our employees, our customers, our suppliers and others, and also for protecting our Company's trade secrets and customer interests, and limited to these purposes.

Towards all these purposes stated above, the security camera recording system at our Company is on record for 7 days and 24 hours.

7.1.2 Authorized Persons to Access:

Access to security camera records stored on digital media is restricted to those authorized by our Company, and the records are only viewed from their computer or monitors.

The General Manager, the Manager of the Financial and Administrative Affairs Department itself and the persons authorized by him/her are authorized to access security camera records. Security officers at the entrance of the parking area monitor live and instantaneously to ensure visitor entrance and exits.

A limited number of persons having the authorization to access the security camera records declare that they shall protect the confidentiality of the data by labour contracts, internal policies, safety regulations, and confidentiality contracts.

7.1.3 Third Parties to Whom Personal Data is Transferred:
Security camera records are only shared with law enforcement officers and relevant judicial authorities through CD or external memory, when necessary or upon the request.

7.1.4 The Retention Period:
ELELE, keeps the security camera records for 15 day. The records are automatically deleted by the method of overwriting once in 15 days.

7.2 Website Visitors:
The personal data shared by the visitors for using our company web, by signing up with the explicit consent of data subject, to visitors' web system belonging to the Company, are processed automatically by our Company.

7.2.1. The Purpose of the Processing Activity:
While processing personal data of the visitors who use the web, our Company acts in line with the principles of compliance with the law and good faith, processing for specific and legitimate purposes and being connected with, limited and restrained to the purpose of processing, that is stipulated in Article 4 of PDP Law.

To use Company's web, the personal data of visitors are processed limited to following purposes:

- Conduct of Information Security Processes (IP adress identification and logging activities by establishing a relationship between the person's information and the transaction),
- Conducting activities in line with the legislation,
- Conduct of Supervisor/Ethic Activities,
- Conduct of Access Authorizations,
- Conduct of Risk Management Activities,

7.2.2 Authorized Persons to Access:
Access to records concerning web visitors stored in digital media is restricted to those authorized by our Company, and the records are only viewed from their computer or monitors.

The Data Processing Department Manager itself and the persons authorized by him/her are authorized to access records concerning web visitors. A limited number of persons having the authorization to access the records concerning web visitors declare that they shall protect the confidentiality of the data by labour contracts, internal policies, safety regulations, and confidentiality contracts.

7.2.3. Third Parties to Whom Personal Data is Transferred:
The mentioned personal data are kept confidential. There is no connection from outside currently, but if support is taken outside when either technical support or support regarding software toward any kind of technical information technology is required, the Company's access is possible. This access will be limited to only the resolution of the technical or software related problem to provide your connection to our visitors' web. Besides, it may be possible to share the data with judicial and administrative authorities for solving legal disputes or when requested by showing reasons due to relevant legislation.

7.2.4.The Retention Period:
ELELE, keeps the records concerning web visitors for 2 years.

PART 8: THE OBLIGATION TO REGISTER WITH THE DATA CONTROLLERS' REGISTRY

ELELE is registered to Data Controllers' Registry. The scope of the information submitted to Data Controllers' Registry, excluding the additional information and documents required by the PDPA, is stated as follows:

- ✓ Identity and address information of ELELE as data controller and of its representative, if any,
- ✓ The purposes for which personal data will be processed,
- ✓ The group(s) of people who are subject of data and explanations about data categories belonging these people,
- ✓ Receiver or groups of receivers to whom personal data may be transferred,
- ✓ Personal data which is envisaged to be transferred abroad.

- ✓ Measures taken for the security of personal data,
- ✓ The maximum storage period required for the purposes for which personal data are processed.

PART 9: DESTRUCTION OF PERSONAL DATA

Our Company stores personal data in line with the required period for purposes of processing and minimum period stipulated in relevant legislation. In this scope, in line with article 138 of the Turkish Penal Code No. 5237 and article 7 of the PDP Law, personal data is deleted, destroyed or anonymized by our company in case the reasons requiring data processing are eliminated despite being processed legally. Accordingly, a "Personal Data Retention and Destruction Policy" is prepared by our Company containing the basis and procedures of deletion, destruction or anonymization of personal data.

In line with this Destruction Policy, ELELE keeps the right of not to fulfil the request of the data subject in the event of having the right and/or obligation to keep the personal data pursuant to the relevant legislation.

PART 10: THE CONTACT PERSON

A Contact Person is assigned to fulfil the obligations as part of PDP Law and to the application of policy and procedures within Company, and to ensure that our Company communicates better with the Data Subjects and the Board. This Contact Person is published on the website.

PART 11: EXECUTION OF THE POLICY AND RELEVANT REGULATION

The legal regulations in force regarding the processing and protection of personal data are implemented within the Company. However, if there is any incompatibility or inconsistency between the legislation in force and this Policy for any reason, our Company accepts that the legislation in force will find application.

This Policy is an embodiment of the rules determined by the relevant legislation in force within the framework of ELELE practices and our Company carries out the necessary works and audit processes.