PERSONAL DATA PROTECTION POLICY

1. COMMITMENT TO DATA CONFIDENTIALITY

1.1. The Policy on Protection of Personal Data ("Policy") sets out the principles to be complied with by Polat Metal İnş.İth.İhr.San.ve Tic.Ltd.Şti. ("Company") within the Company and/or by the Company while fulfilling its obligations to protect Personal Data and processing Personal Data in accordance with the provisions of the relevant legislation, in particular the Law No. 6698 on the Protection of Personal Data.

1.2. The Company undertakes to act in accordance with this Policy and the procedures to be implemented in accordance with the Policy in terms of Personal Data within its own organization.

2. PURPOSE OF THE POLICY

To determine the principles regarding the methods and processes for the processing and protection of Personal Data by the Company.

3. SCOPE OF THE POLICY

3.1. It covers all activities regarding Personal Data processed by the Company and applies to such activities.

3.2. Does not apply to data that does not qualify as Personal Data

3.3. It may be amended from time to time with the approval of the General Manager if required by the KVKK regulations or if deemed necessary by the Company's Data Controller Contact Person or the Data Protection Committee. In case of any incompatibility between the KVKK regulations and the Policy, the KVKK regulations shall prevail.

4. DEFINITIONS

The definitions used in the Policy have the following meanings;

"Explicit Consent" refers to consent based on information on a specific subject and expressed with free will.

"Anonymization" means making Personal Data impossible to be associated with an identified or identifiable natural person under any circumstances, even by matching with other data.

"Disclosure Obligation" refers to the obligation of the Data Controller or the person authorized by the Data Controller to provide information to the Data Subject within the scope of Article 10 of the KVKK during the acquisition of Personal Data.

"Personal Data" means any information relating to an identified or identifiable natural person (within the scope of the Policy

"Personal Data" shall also include, to the extent appropriate, 'Sensitive Personal Data' as defined below).

“Personal Data Processing” means any operation performed on Personal Data such as obtaining, recording, storing, preserving, modifying, reorganizing, disclosing, transferring, taking over, making available, classifying or preventing the use of Personal Data by fully or partially automatic means or by non-automatic means provided that it is part of any data recording system.

“Data Protection Committee” refers to the committee responsible for the fulfillment of the KVKK Policies and the procedures to be implemented in accordance with the KVKK Policies.

“Board” refers to the Personal Data Protection Board.

“Institution” refers to the Personal Data Protection Authority.

“KVKK” refers to the Personal Data Protection Law No. 6698.

“KVKK Regulations” refers to the Law No. 6698 on the Protection of Personal Data and other relevant legislation on the protection of Personal Data, binding decisions, principle decisions, provisions, instructions issued by regulatory and supervisory authorities, courts and other official authorities, and applicable international agreements and any other legislation for the protection of data.

“KVKK Policies” refers to the policies issued by the Company on the protection of Personal Data. “KVKK Procedures” refers to the procedures that determine the obligations that the Company, employees and the Committee must comply with within the scope of KVKK policies.

“Sensitive Personal Data” refers to data relating to race, ethnic origin, political opinions, philosophical beliefs, religion, sect or other beliefs, appearance and dress, membership of associations, foundations or trade unions, health, sexual life, criminal convictions and security measures, and biometric and genetic data.

“Deletion/Deletion or Destruction” refers to the irreversible destruction or destruction of Personal Data.

“Data Inventory” refers to the inventory containing information such as Personal Data Processing processes and methods, Personal Data Processing purposes, data category, third parties to whom Personal Data is transferred, etc. for the Company's Personal Data Processing activities.

“Data Processor” refers to the natural or legal person who processes Personal Data on behalf of the Data Controller by being authorized by the Data Controller.

“Data Subject” refers to all natural persons whose Personal Data are processed by or on behalf of the Company.

“Data Controller” refers to the person who processes Personal Data by specifying the purposes and ways of Processing, establishing the data recording system and the natural or legal person responsible for its management.

“Data Controller Contact Person” The person appointed by the senior management who manages the Company's relations with the Institution refers to.

“Data Controllers Registry Information System (VERBIS)” Data controllers are required to apply to the Registry and other relevant by the Presidency of the Personal Data Protection Authority, which can be accessed over the internet, which they will use in transactions information system created and managed.

5. PRINCIPLES OF PERSONAL DATA PROCESSING

5.1. Processing of Personal Data in Compliance with the Law and Good Faith The Company processes Personal Data in accordance with the law and good faith and based on the principle of proportionality.

5.2. Taking Necessary Measures to Ensure that Personal Data is Accurate and Up-to-Date When Necessary The Company takes all necessary measures to ensure that Personal Data is complete, accurate and up-to-date and updates Personal Data in case the Data Subject requests changes to Personal Data within the scope of KVKK Regulations.

5.3. Processing of Personal Data for Specific, Explicit and Legitimate Purposes Before the Processing of Personal Data, the purpose for which Personal Data will be processed is determined by the Company. In this context, the Data Subject is enlightened within the scope of KVK Regulations and their Explicit Consent is obtained where necessary.

5.4. The Company processes Personal Data only in exceptional cases within the scope of KVKK regulations (Article 5.2 and Article 6.3 of KVKK) or in line with the purpose within the scope of the Explicit Consent obtained from the Data Subject (Article 5.1 and Article 6.2 of KVKK) and in accordance with the principle of proportionality. The Data Controller processes Personal Data in a manner that is conducive to the achievement of the specified purposes and avoids processing Personal Data that is not related to the achievement of the purpose or is not needed.

5.5. Retention of Personal Data for the Period Stipulated in the Relevant Legislation or Required for the Purpose for which they are Processed

5.5.1. The Company retains Personal Data for as long as necessary in accordance with the purpose. If the Company wishes to retain Personal Data for a period longer than the period stipulated in the KVKK regulations or required by the purpose of Personal Data Processing, the Company acts in accordance with the obligations specified in the KVKK regulations.

5.5.2. After the period required by the purpose of Personal Data Processing expires, Personal Data shall be deleted or anonymized. It is ensured that third parties to whom the Company transfers Personal Data also delete, destroy or anonymize Personal Data.

5.5.3. The Data Controller Contact Person and the Data Protection Committee are responsible for the operation of the Deletion, Destruction and Anonymization processes. In this context, the necessary procedure is established by the Data Controller Contact Person and the Data Protection Committee.

6. PROCESSING OF PERSONAL DATA

Personal Data may be processed by the Company only within the scope of the following procedures and principles.

6.1. Explicit Consent

6.1.1. Personal Data shall be processed after informing the Data Subjects within the framework of the fulfillment of the Disclosure Obligation and in case the Data Subjects give Explicit Consent.

6.1.2. Before obtaining Explicit Consent within the framework of the Disclosure Obligation, the Data Subjects shall be informed of their rights.

6.1.3. Explicit Consent of the Relevant Person is obtained by methods in accordance with the KVKK regulations. Explicit Consents are provably maintained by the Company for the required period of time within the scope of KVKK regulations.

6.1.4. The Data Controller Contact Person and the Data Protection Committee are obliged to ensure that the Disclosure Obligation is fulfilled in terms of all Personal Data Processing processes and that Explicit Consent is obtained when necessary and that the Explicit Consent obtained is preserved. All department employees who Process Personal Data shall be responsible for the Data Controller Contact Person and Data Protection Committee's instructions, this Policy and KVKK Procedures.

6.2. Processing of Personal Data without Explicit Consent

6.2.1 In cases where it is foreseen to Process Personal Data without Explicit Consent within the scope of KVKK regulations (Article 5.2 of KVKK), the Company may process Personal Data without obtaining the Explicit Consent of the Data Subject. In the event that Personal Data is processed in this way, the Company Processes Personal Data within the limits set by the KVKK regulations.

In this context;

6.2.1.1. Personal Data may be processed by the Company without Explicit Consent if explicitly stipulated in the laws.

6.2.1.2. Personal Data may be processed by the Company without Explicit Consent if it is mandatory for the protection of the life or physical integrity of the Data Subject or someone else other than the Data Subject who is unable to disclose his/her consent due to actual impossibility or whose consent is not legally valid.

6.2.1.3. Provided that it is directly related to the establishment or performance of a contract, Personal Data of the parties to the contract If it is necessary to process Personal Data, Personal Data may be processed by the Company without the Explicit Consent of the Data Subjects can be processed.

6.2.1.4. If the Processing of Personal Data is mandatory for the Company to fulfill its legal obligation, Personal Data may be processed by the Company without the Explicit Consent of the Data Subjects.

6.2.1.5. Personal Data made public by the Data Subject may be processed by the Company without Explicit Consent.

6.2.1.6. If the Processing of Personal Data is mandatory for the establishment, exercise or protection of a right, Personal Data may be processed by the Company without Explicit Consent.

6.2.1.7. Personal Data may be processed by the Company without Explicit Consent if data processing is mandatory for the legitimate interests of the Company, provided that it does not harm the fundamental rights and freedoms of the Data Subject

7. PROCESSING OF SPECIAL CATEGORIES OF PERSONAL DATA

7.1. Sensitive Personal Data can only be collected with the explicit consent of the Data Subject or in cases of sexual life and personal health In the event that processing is explicitly required by law in terms of Special Categories of Personal Data other than data can be processed.

7.2. Personal Data relating to health and sexual life may only be processed for the purposes of protecting public health, preventive medicine, medical diagnosis, treatment and care services, planning and management of health services and financing, confidentiality

persons under a retention obligation (e.g. Company physician) or authorized institutions and organizations without obtaining Explicit Consent.

7.3. While Processing Sensitive Personal Data, the measures determined by the Board are taken.

7.4. The Company shall ensure that employees involved in the processing of Special Categories of Personal Data,

7.4.1 Provide regular trainings on KVK Regulations and the security of Special Categories of Personal Data.

7.4.2 Will make confidentiality agreements.

7.4.3 Clearly define the scope and duration of authorization of users authorized to access Sensitive Personal Data.

7.4.4 Periodically perform authorization checks.

7.4.5 Immediately remove the authorizations of employees who change their duties or leave their jobs and allocate them to the relevant employee. will take back the inventory immediately.

7.5. In case of transfer to electronic media of Special Nature, where Special Nature Data is processed, stored and/or the electronic media through which it is accessed, the Company;

7.5.1 Preserve Sensitive Personal Data using cryptographic methods.

7.5.2 Keep cryptographic keys in secure and different environments.

7.5.3 Keep transaction records of all movements performed on Sensitive Personal Data securely. log the data.

7.5.4 Continuously follow the security updates of the environments where Special Categories of Personal Data are located, and keep track of the necessary security tests on a regular basis and record the test results.

7.5.5 If Sensitive Personal Data is accessed through a software, user authorizations of this software will carry out security tests of these software regularly, and will record the test results.

7.5.6 In case of remote access to Sensitive Personal Data, at least two-stage authentication system will provide.

7.6. In the event that Sensitive Personal Data is processed in a physical environment, the Company shall ensure that adequate security measures (against electric leakage, fire, flooding, theft, etc.) are taken according to the nature of the environment where Sensitive Personal Data is located;

7.6.1 Ensure that adequate security measures (against electric leakage, fire, flood, theft, etc.) are taken according to the nature of the environment where Sensitive Personal Data is located.

7.6.2 It shall prevent unauthorized entry and exit by ensuring the physical security of these environments.

7.7. In case of transfer of Special Categories of Personal Data, Data Controller;

7.7.1 If it is necessary to transfer Sensitive Personal Data via e-mail, it will use an encrypted corporate e-mail address or Registered Electronic Mail (“REM”) account.

7.7.2 If it is necessary to transfer Sensitive Personal Data via media such as portable memory, CD, DVD, it will encrypt it with cryptographic methods and keep the cryptographic key in different media.

7.7.3 If Special Categories of Personal Data need to be transferred between servers in different physical environments, the servers by establishing a VPN or by SFTP method.

7.7.4 In case it is necessary to transfer Sensitive Personal Data via paper media, theft of the document, will take the necessary precautions against risks such as loss or unauthorized access.

7.8. In addition to the above regulations, the Data Protection Committee and the Data Controller Contact Person shall be responsible for the processing of Special Categories of Data. In particular, Personal Data Security published by the Board on ensuring the security of Personal Data, including It will act in accordance with the KVKK regulations, including the Guide.

7.9. In any case requiring the Processing of Special Categories of Personal Data, the relevant employee shall contact the Data Controller Contact The Data Subject shall be informed.

7.10. If it is not clear whether a data is Sensitive Personal Data or not, the relevant department shall inform the Data An opinion is obtained from the Responsible Contact Person.

8. STORAGE PERIOD OF PERSONAL DATA

Personal Data are kept within the Company for the duration of the relevant legal retention periods and are kept for the period necessary for the realization of the activities related to this data and the purposes specified in this Policy.

Personal Data whose purpose of use has expired and the legal retention period has expired, in accordance with Article 7 of the KVKK, the Company by the government, deleted, destroyed or anonymized.

9. DELETION, DESTRUCTION AND ANONYMIZATION OF PERSONAL DATA

9.1. When the legitimate purpose for the Processing of Personal Data no longer exists, the relevant Personal Data shall be Deleted, Destroyed or Anonymized. Situations requiring Deletion, Destruction or Anonymization of Personal Data are monitored by the Data Controller Contact Person and the Data Protection Committee.

9.2. The Data Controller Contact Person and the Data Protection Committee are responsible for the operation of the Deletion, Destruction and Anonymization processes. In this context, the necessary procedure is established by the Data Controller Contact Person and the Data Protection Committee.

9.3. All Deletion, Destruction and Anonymization activities to be performed by the Company on Personal Data Data Destruction It will be realized in accordance with the principles specified in the Procedure

10. TRANSFER OF PERSONAL DATA AND PROCESSING OF PERSONAL DATA BY THIRD PARTIES

The Company may transfer Personal Data to a third natural or legal person at home and/or abroad in accordance with the KVKK Regulations by taking the necessary measures in line with the purposes of Personal Data Processing. In this case, the Company ensures that third parties to whom it transfers Personal Data also comply with this Policy. In this context, necessary protective regulations are added to the contracts concluded with the third party. The article to be added to the contracts concluded with third parties to whom all kinds of Personal Data are transferred is obtained from the Data Controller Contact Person. Each employee is obliged to go through the process in this Policy in case of Personal Data transfer. If the third party to whom Personal Data is transferred requests a change in the article transmitted by the Data Controller Contact Person, the situation shall be immediately notifies the Data Controller Contact Person by the employee.

10.1. Transfer of Personal Data to Third Parties in Turkey

10.1.1. Personal Data may be collected without Explicit Consent in exceptional cases specified in Article 5.2 of the KVKK and Article 6.3 provided that adequate measures are taken, or in other cases, provided that the Explicit Consent of the Data Subject is obtained (Article 5.1 and Article 6.2) It may be transferred to third parties in Turkey by the Company.

10.1.2. The transfer of Personal Data to third parties in Turkey shall be in accordance with the regulations of the KVKK Company employees and the Data Controller Liaison Person are jointly and severally responsible for ensuring that the Data Controller Liaison Person

10.2. Transfer of Personal Data to Third Parties Abroad

10.2.1. Personal Data may be transferred to third parties abroad without Explicit Consent in exceptional cases specified in Article 5.2 and Article 6.3 of the LPPD or in other cases, provided that the Explicit Consent of the Data Subject is obtained (Article 5.1 and Article 6.2 of the LPPD), It may be transferred by the Company.

10.2.2. In the event that Personal Data is transferred without Explicit Consent in accordance with the KVKK regulations, it may also be one of the following conditions must exist in terms of the foreign country to which the Personal Data will be transferred;

10.2.2.1 The foreign country to which the Personal Data is transferred has the status of countries with adequate protection by the Board (please follow the Board's current list for a list),

10.2.2.2.2 If the foreign country where the transfer will take place is not included in the Board's list of safe countries By making a written commitment that the Company and the Data Controllers in the relevant country will provide adequate protection Obtaining permission from the Board.

10.2.3. Ensuring that the transfer of Personal Data to third parties abroad complies with the KVKK regulations Company employees, Data Protection Committee and Data Controller Contact Person are jointly and severally liable.

11. DISCLOSURE OBLIGATION OF THE COMPANY

11.1. In accordance with Article 10 of the KVKK, the Company shall inform the Data Subjects before the Processing of Personal Data. In this context, the Company fulfills the Disclosure Obligation during the acquisition of Personal Data. The notification to be made to the Data Subjects within the scope of the Disclosure Obligation includes the following elements respectively:

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

11.1.2. The purpose for which Personal Data will be processed,

11.1.3. To whom and for what purpose the processed Personal Data may be transferred,

11.1.4. Method and legal reason for collecting Personal Data,

11.1.5. The rights of the Data Subjects listed in Article 11 of the LPPD.

11.2. In accordance with Article 20 of the Constitution of the Republic of Turkey and Article 11 of the LPPD, the Company shall provide the necessary information in case the Data Subject requests information.

11.3. If requested by the Relevant Persons in accordance with the KVKK regulations, the Company may process the processed personal data notifies the requesting Relevant Person.

11.4. It shall be responsible for ensuring that the necessary Disclosure Obligation is fulfilled before the Processing of Personal Data. The employee who follows the process, the Data Protection Committee and the Data Controller Contact Person are responsible.

11.5. In the event that the Data Processor is a third party other than the Company, the third party must undertake that the third party will act in accordance with the above-mentioned obligations with a written contract before the Personal Data Processing begins. In cases where third parties transfer Personal Data to the Company, the clause to be added to the agreements shall be written by the Data Controller

It is obtained from the Contact Person. Each employee is obliged to go through the process in this Policy in case Personal Data is transferred to the Company by a third party. In the event that the third party transferring Personal Data requests a change in the article communicated by the Data Controller Contact Person, the situation shall be immediately communicated by the employee to the Data Controller Contact Person. Notified to the contact person.

12. RIGHTS OF THE PERSON CONCERNED

12.1. The Company may respond to the following requests of the Data Subjects whose Personal Data it holds, in accordance with the KVKK responds in accordance with the regulations;

12.1.1. Learning whether Personal Data is processed by the Company,

12.1.2. To request information about the processing of Personal Data,

12.1.3. To learn the purpose of processing Personal Data and whether they are used in accordance with their purpose,

12.1.4. To know the third parties to whom Personal Data is transferred domestically or abroad,

12.1.5. To request correction of Personal Data in case of incomplete or incorrect processing by the Company,

12.1.6. In order to be evaluated within the principles of purpose, duration and legitimacy, it is necessary to Process Personal Data To request the deletion or destruction of Personal Data by the Company if the reasons disappear,

12.1.7. In the event that Personal Data is corrected, deleted or destroyed by the Company, these transactions are considered to be Personal Request notification to third parties to whom the data is transferred,

12.1.8. If the processed Personal Data is analyzed exclusively through automated systems and a result is obtained against the Relevant Person, to object to this result,

12.1.9. To request compensation for the damages in case the Personal Data is processed against the law and the Relevant Person suffers damages due to this reason.

In cases where the Relevant Persons wish to exercise their rights and/or believe that the Company has not acted within the scope of this Policy while processing Personal Data, they may submit their requests by filling out the Personal Data Application Form or by creating their own requests in a way that meets the conditions determined by the Personal Data Protection Authority, to the e-mail address given below, which may change from time to time, from the e-mail address previously notified to the Company and registered in the Company system (the e-mail address registered in the system must be checked), or with a secure electronic signature or mobile signature to the Company's cash register address or to the postal address given below, which may change from time to time, by hand or via notary, and may send them by other methods determined by the Personal Data Protection Authority that may be added to these in the future. Current application methods and application content must be confirmed by the legislation before the application.

Data Controller: Polat Metal Construction Import Export Trade Co. Ltd.

E-mail: info@polatmetal.com

Postal Address: Dilovası Organized Industrial Zone 4th Section D 4013 Street No:4 Dilovası/Gebze/KOCAELİ

12.2. If the Data Subjects submit their requests regarding the rights listed above to the Company in writing, the Company will finalize the request free of charge within thirty days at the latest, depending on the nature of the request. In the event that an additional cost arises for the finalization of the requests by the Data Controller, the fees in the tariff determined by the Personal Data Protection Board may be requested by the Data Controller.

13. DATA MANAGEMENT AND SECURITY

13.1. The Company appoints a Data Controller Contact Person and establishes a Data Protection Committee to fulfill its obligations within the scope of the KVKK Regulations, to ensure and supervise the implementation of the KVKK Procedures necessary for the implementation of this Policy, and to make recommendations regarding their operation.

13.2. All employees involved in the relevant process are responsible for the protection of Personal Data in accordance with this Policy and the KVKK Procedures.

13.3. Personal Data Processing activities are supervised by the Company with technical systems according to technological possibilities and implementation costs.

13.4. Personnel knowledgeable in technical matters regarding Personal Data Processing activities are employed.

13.5. Company employees are informed and trained regarding the protection of Personal Data and processing it in accordance with the law.

13.6. The necessary KVKK Policy is created in order to ensure that employees who need to access Personal Data in the Company have access to the said Personal Data. The Data Controller Contact Person and the Data Protection Committee are responsible for its creation and implementation.

13.7. Company employees may access Personal Data only within the authority granted to them and in accordance with the relevant Access Matrix. Any access and processing carried out by the employee in excess of their authority is against the law and is a reason for termination of the employment contract for a just cause.

13.8. If the Company employee suspects that the security of Personal Data is not sufficiently ensured or detects such a security breach, the Company immediately notifies the Data Controller Contact Person.

13.9. Detailed Procedures for the security of Personal Data are established by the Data Controller Contact Person and the Data Protection Committee.

13.10. Each person to whom a Company device is allocated is responsible for the security of the devices allocated to their use.

13.11. Each Company employee or person working within the Company is responsible for the security of the physical files within their area of responsibility.

13.12. In the event that there are security measures requested or to be requested additionally for the security of Personal Data within the scope of the KVKK regulations, all employees are obliged to comply with additional security measures and ensure the continuity of these security measures.

13.13. Software and hardware including virus protection systems and firewalls are installed in the Company in accordance with technological developments to store Personal Data in secure environments.

13.14. Backup programs are used and adequate security measures are taken in the Company to prevent loss or damage to Personal Data.

13.15. Necessary measures will be taken to protect documents containing Personal Data with encrypted (encrypted) systems in the Company. In this context, Personal Data will not be stored in common areas and on the desktop. Files and folders containing Personal Data, etc. will not be moved to the desktop or common folder, information on Company computers will not be transferred to another device such as USB, etc., or taken out of the Company without the knowledge of the Data Controller Contact Person or the Data Protection Committee.

13.16. The Data Protection Committee, together with the Senior Management, is responsible for taking technical and administrative measures for the protection of all Personal Data within the Company, continuously monitoring developments and administrative activities, preparing the KVKK Procedures, announcing them within the Company, ensuring compliance with them and supervising them. In this context, the Data Protection Committee and the Data Controller Contact Person organize the necessary training to increase the awareness of employees.

13.17. If a department within the Company processes Special Personal Data, this department will be informed by the Data Protection Committee about the importance, security and confidentiality of the Personal Data they process, and the relevant department will act in accordance with the instructions of the Data Protection Committee. Only limited employees will

be authorized to access Special Personal Data, and their list and monitoring will be carried out by the Data Protection Committee.

13.18. All Personal Data processed within the Company is considered "Confidential Information" by the Company.

13.19. Company employees have been informed that their obligations regarding the security and confidentiality of Personal Data will continue after the termination of the employment relationship, and a commitment has been obtained from Company employees to comply with these rules.

14. TRAINING

14.1. The Company provides its employees with the necessary training on the protection of Personal Data within the scope of the Policy and KVKK Procedures and KVKK Regulations.

14.2. The definitions of Special Personal Data and practices regarding their protection are specifically addressed in the trainings.

14.3. If a Company employee accesses Personal Data physically or in a computer environment, the Company provides training to the relevant employee on such access (e.g. accessed computer programs and portals).

15. AUDIT

The Company has the right to audit the compliance of all employees, departments and contractors of the Company with this Policy and KVKK regulations on a regular basis at any time without any prior notice and conducts the necessary routine audits within this scope. The Data Protection Committee and the Data Controller Contact Person establish the Audit Procedure regarding these audits, submit it to the approval of the Senior Management and ensure the implementation of the said procedure.

16. VIOLATIONS

16.1. Each employee of the company shall report any work, transaction or action that they consider to be contrary to the procedures and principles set forth in the KVKK regulations and this Policy to the Data Protection Committee. The Data Protection Committee shall create an action plan in accordance with this Policy and the Information Security Breach Incidents Procedures.

16.2. As a result of the information provided, the Data Protection Committee prepares the notification to be made to the Relevant Person or Institution regarding the violation, taking into account the provisions of the legislation in force, especially the KVKK regulations. The Data Controller Contact Person conducts the correspondence and communication with the Institution.

18. RESPONSIBILITIES

The responsibilities within the Company are, in order, the employee, department head, Data Protection Committee and Data Controller Contact Person. In this context; the Data Protection

Committee and Data Controller Contact Person responsible for the implementation of the Policy are appointed by the Company's Board of Directors with the decision of the Board of Directors and changes are made in this context in the same way.

19. CHANGES TO BE MADE IN THE POLICY

18.1. This Policy may be changed by the Company with the approval of the Senior Management when necessary.

18.2. The Company shares the updated Policy text with its employees via e-mail so that the changes it has made to the Policy can be reviewed or makes it available to employees and Relevant Persons via the web address below.