pireks
BAKIR ALAŞIMLARI SANAYİ VE TİCARET A.Ş.

Personal Data Protection Policy

Personal Data Protection Policy

1. DATA PRIVACY COMMITMENT

1.1. This Personal Data Protection Policy ("Policy") outlines the principles and obligations to be followed by Pireks Copper Alloys Industry and Trade Inc. ("Company") in accordance with the provisions of the relevant legislation, primarily the Law No. 6698 on the Protection of Personal Data, while fulfilling its obligations to protect Personal Data and processing Personal Data, both within the Company and/or the principles that must be adhered to by the Company.

The Company commits to act in accordance with this Policy and the procedures to be applied in connection with it, concerning the Personal Data it holds within its own structure.

2. PURPOSE OF THE POLICY

The primary purpose of this Policy is to establish the principles regarding the methods and processes for the protection of Personal Data by the Company.

3. SCOPE OF THE POLICY

3.1. This Policy covers all activities related to the Personal Data processed by the Company and applies to these activities.

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

3.3. This Policy may be amended from time to time with the approval of the Board of Directors, if required by the KVKK Regulations or if deemed necessary by the Company's Data Controller.

4. DEFINITIONS

The definitions used in this Policy have the following meanings:

"**Explicit Consent**" refers to the consent expressed by the Data Subject, based on being informed and given freely, regarding the processing of their Personal Data.

"**Anonymization**" refers to the process of making Personal Data impossible to relate to a specific or identifiable individual, even if matched with other data.

"**Anonymized Data**" refers to data that cannot in any way be related to a natural person.

"**Personal Data**" refers to any information relating to an identified or identifiable natural person (within the scope of this Policy, the term "Personal Data" will also include the "Special Categories of Personal Data" defined below, where applicable).

"Personal Data Processing" refers to any operation performed on Personal Data, whether by automated means or non-automated means as part of a data recording system, including collection, recording, storage, preservation, modification, rearrangement, disclosure, transfer, acquisition, making accessible, classification, or restriction of use of the data.

"Committee" refers to the committee within the Company responsible for the implementation of this Policy and the procedures to be applied in accordance with the Policy (including Information Technology, Quality, Integrated Management System, Human Resources, Occupational Health and Safety, and Financial Affairs).

"**Board**" refers to the Personal Data Protection Board within the state structure.

"**Institution**" refers to the Personal Data Protection Authority within the state structure.

"**KVKK**" refers to the Law No. 6698 on the Protection of Personal Data.

"KVKK Regulations" refers to the Law No. 6698 on the Protection of Personal Data, along with other relevant legislation on data protection, binding decisions, principle decisions, rulings, instructions, and applicable international agreements issued by regulatory and supervisory authorities, courts, and other official bodies.

"KVKK Procedures" refers to the current KVKK procedures approved by the Board of Directors and enacted, which define the obligations that the Company, its employees, and the Data Controller must comply with under this Policy.

"Special Categories of Personal Data" refers to data regarding a person's race, ethnic origin, political opinions, philosophical beliefs, religion, sect or other beliefs, appearance, membership in associations, foundations or trade unions, health, sexual life, criminal convictions and security measures, as well as biometric and genetic data.

"Deletion or Erasure" refers to the process of making Personal Data inaccessible and irretrievable for the relevant users, ensuring it cannot be used again.

"Data Inventory" refers to the inventory containing information such as the processes and methods of Personal Data Processing, the purposes of Personal Data Processing, data categories, third parties to whom Personal Data is transferred, etc., regarding 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, based on authorization received from the Data Controller.

"Data Subject" refers to all natural persons whose Personal Data is processed by the Company or on behalf of the Company.

"Data Controller" refers to the natural or legal person who determines the purposes and means of processing Personal Data and manages the place where the data is systematically stored (data recording system).

"Destruction" refers to the process of making Personal Data irretrievable, inaccessible, and unusable by anyone in any way.

1. PRINCIPLES OF PERSONAL DATA PROCESSING

1.1. Processing of Personal Data in Compliance with the Law and Principles of Integrity

Personal Data is processed by the Company in accordance with the law, the principles of integrity, and based on the principle of proportionality.

1.2. Necessary Measures to Ensure Personal Data is Accurate and, When Necessary, Up to Date

The Company takes all necessary measures to ensure that Personal Data is complete, accurate, and up to date, and updates the relevant Personal Data upon request from the Data Subject to make changes to their Personal Data.

1.3. Processing of Personal Data for Specific, Legitimate, and Clear Purposes

Before processing Personal Data, the Company determines the purposes for which the Personal Data will be processed. In this context, the Data Subject is informed in accordance with the KVKK Regulations, and, where necessary, Explicit Consent is obtained.

1.4. Data Must Be Relevant, Limited, and Proportionate to the Purpose for Which They Are Processed

The Company processes Personal Data only for purposes within the scope of the KVKK Regulations, in exceptional cases (Article 5.2 and Article 6.3 of the KVKK), or in accordance with the purpose for which Explicit Consent is obtained from the Data Subject (Article 5.1 and Article 6.2 of the KVKK), and in compliance with the principle of proportionality.

1.5. Retention of Personal Data Only for as Long as Necessary and Its Deletion Afterwards

1.5.1. The Company retains Personal Data for as long as necessary for the intended purpose. If the Company wishes to retain Personal Data for a period longer than the duration required by the KVKK Regulations or the purpose of Personal Data Processing, the Company will comply with the obligations specified in the KVKK Regulations.

1.5.2. After the period required for the purpose of Personal Data Processing has ended, the Personal Data will be Deleted, Destroyed, or Anonymized. In this case, the Company ensures that the third parties to whom Personal Data has been transferred also delete, destroy, or anonymize the Personal Data.

1.5.3. The Data Controller is responsible for managing the processes of Deletion, Destruction, and Anonymization. If necessary, a procedure will be created by the Data Controller.

2. PROCESSING OF PERSONAL DATA

Personal Data may only be processed by the Company within the procedures and principles outlined below.

2.1. Explicit Consent

2.1.1. Personal Data is processed after the completion of the information provided to the Data Subjects as part of fulfilling the obligation of informing them, and upon the Data Subjects' Explicit Consent.

2.1.2. Prior to obtaining Explicit Consent under the obligation to inform, the Data Subjects are notified of their rights.

2.1.3. The Explicit Consent of the Data Subject is obtained through methods compliant with the KVKK Regulations. Explicit Consents are stored by the Company in a way that is verifiable and for the duration required under the KVKK Regulations.

2.1.4. The Data Controller is responsible for ensuring the fulfillment of the obligation to inform and, when necessary, obtaining and retaining Explicit Consent for all Personal Data Processing processes. All employees in departments processing Personal Data are required to comply with the instructions of the Data Controller, this Policy, and the KVKK Procedures annexed to this Policy.

2.2. Processing of Personal Data Without Obtaining Explicit Consent

2.2.1. In cases where the processing of Personal Data without Explicit Consent is allowed under the KVKK Regulations (Article 5.2 and Article 6.3 of the KVKK), the Company may process Personal Data without obtaining the Data Subject's Explicit Consent. In such cases, the Company will process Personal Data within the limits set by the KVKK Regulations. In this context:

2.2.1.1. Personal Data may be processed by the Company without Explicit Consent for the protection of the life or physical integrity of the Data Subject, or another person, in situations where the Data Subject is unable to provide consent due to practical impossibility or where their consent is not legally valid.

2.2.1.2. If the processing of Personal Data is directly related to the establishment, performance, enforcement, or termination of a contract, the Personal Data of the parties to the contract may be processed by the Company without the Explicit Consent of the Data Subjects.

2.2.1.3. If the processing of Personal Data is mandatory for the Company to fulfill its legal obligations, the Company may process Personal Data without the Explicit Consent of the Data Subjects.

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

2.2.1.5. If processing Personal Data without Explicit Consent is the only way to establish, use, or protect a right, Personal Data may be processed by the Company, with the knowledge of the Data Controller, without Explicit Consent.

2.2.1.6. If processing Personal Data is necessary for the legitimate interests of the Company, without harming the fundamental rights and freedoms of the Data Subject, Personal Data may be processed by the Company without Explicit Consent.

3. PROCESSING OF SPECIAL CATEGORIES OF PERSONAL DATA

3.1. Special Categories of Personal Data may only be processed if the Data Subject has provided Explicit Consent or if the processing is explicitly required by law for Special Categories of Personal Data other than data related to sexual life and personal health.

3.2. Personal Data related to health and sexual life may be processed without Explicit Consent only for the protection of public health, preventive medicine, medical diagnosis, treatment and care services, and the planning and management of healthcare services and financing. Therefore, until otherwise specified in the KVKK Regulations, personal health data and data related to sexual life may only be processed under Explicit Consent or by the Company's doctors, who are bound by confidentiality obligations.

3.3. When processing Special Categories of Personal Data, the measures determined by the Board are taken.

3.4. In any case where the processing of Special Categories of Personal Data is required, the relevant employee informs the Data Controller.

3.5. If it is unclear whether a data is Special Categories of Personal Data, the relevant department consults the Data Controller for guidance.

4. DELETION, DESTRUCTION, AND ANONYMIZATION OF PERSONAL DATA

4.1. When the legitimate purpose for processing Personal Data no longer exists, the relevant Personal Data will be Deleted, Destroyed, or Anonymized. The Data Controller will monitor the cases where Personal Data must be Deleted, Destroyed, or Anonymized.

4.2. The Data Controller is responsible for managing the processes of Deletion, Destruction, and Anonymization. If necessary, a procedure will be created by the Data Controller.

4.3. The Company does not retain Personal Data with the intention of using it in the future.

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

The Company may transfer Personal Data to a third party, whether a real or legal person ("Contractor"), in compliance with the KVKK Regulations. In such cases, the Company ensures that the third parties to whom the Personal Data is transferred also comply with this Policy. In this context, necessary protective provisions are added to the contracts concluded with the third party. The clause to be added to the contracts with the third parties to whom Personal Data is transferred is obtained from the Data Controller. Each employee is required to follow the process outlined in this Policy in the event of a Personal Data transfer. If the third party to whom Personal Data has been transferred requests changes to the clause provided by the Data Controller, the situation must immediately be reported by the employee to the Data Controller.

5.1. Transfer of Personal Data to Third Parties in Turkey

5.1.1. Personal Data may be transferred to third parties in Turkey by the Company without Explicit Consent in exceptional cases specified in Articles 5.2 and 6.3 of the KVKK, or with the Explicit Consent of the Data Subject in other cases (Articles 5.1 and 6.2 of the KVKK).

5.1.2. The Company employees and the Data Controller are jointly responsible for ensuring that the transfer of Personal Data to third parties in Turkey is in compliance with the KVKK Regulations.

5.2. Transfer to Third Parties Abroad

5.2.1. Personal Data may be transferred to third parties located abroad by the Company without Explicit Consent in exceptional cases specified in Articles 5.2 and 6.3 of the KVKK, or with the Explicit Consent of the Data Subject in other cases (Articles 5.1 and 6.2 of the KVKK).

6. THE COMPANY'S OBLIGATION TO INFORM

6.1. In accordance with Article 10 of the KVKK, the Company informs the Data Subjects before processing their Personal Data. In this context, the Company fulfills the Obligation to Inform at the time of obtaining the Personal Data. The notification to be made to the Data Subjects under the Obligation to Inform includes the following elements in sequence:

6.1.1. The identity of the Data Controller and, if applicable, their representative,

6.1.2. The purposes for which the Personal Data will be processed,

6.1.3. To whom and for what purposes the processed Personal Data may be transferred,

6.1.4. The method of collecting the Personal Data and the legal basis for it,

6.1.5. The rights of the Data Subjects.

6.1.6. In accordance with Article 20 of the Constitution of the Republic of Turkey and Article 11 of the KVKK, the Company provides the necessary information to the Data Subject if they request it.

6.1.7. If requested by the Data Subjects, the Company will inform the Data Subject of the Personal Data it processes related to them.

6.2. The employee following the relevant process and the Data Controller are jointly responsible for ensuring the fulfillment of the Obligation to Inform before processing the Personal Data. In this context, if necessary, the Data Controller may create a KVKK Procedure to report each new processing process to the Data Controller.

6.3. If the Data Processor is a third party outside of the Company, the third party must commit, via a written agreement, to comply with the obligations specified above before starting to process the Personal Data. In cases where third parties transfer Personal Data to the Company, the clause to be added to the contract will be obtained from the Data Controller. Each employee is required to follow the process outlined in this Policy if Personal Data is transferred to the Company by a third party. If the third party transferring the Personal Data requests any changes to the clause provided by the Data Controller, the employee must immediately report the situation to the Data Controller.

7. RIGHTS OF DATA SUBJECTS

7.1. The Company will respond to the following requests of Data Subjects regarding their personal data in accordance with the KVKK Regulations:

7.1.1. Learn whether their Personal Data is processed by the Company,

7.1.2. Request information regarding the processing of their Personal Data,

7.1.3. Learn the purpose of processing their Personal Data and whether it is being used in accordance with its purpose,

7.1.4. Know the third parties to whom their Personal Data has been transferred, both domestically and internationally,

7.1.5. Request the correction of Personal Data that has been processed inaccurately or incompletely by the Company,

7.1.6. Request the deletion, destruction, or anonymization of Personal Data if the reasons requiring processing no longer exist, including evaluation based on purpose, duration, and legitimacy principles,

7.1.7. Request notification of the transactions made under Articles 6.1.5 and 6.1.6 to third parties to whom the Personal Data has been transferred,

7.1.8. If the Personal Data is analyzed solely by automated systems and a result is produced to the disadvantage of the Data Subject, object to this result,

7.1.9. In the event that Personal Data is processed unlawfully and the Data Subject suffers damage as a result, request compensation for the damage.

Data Subjects can submit their requests or complaints to the Data Controller by securely signing their requests with an electronic signature or by delivering a petition signed in wet ink, with identification documents attached, either by hand or via notary, to the following email address or postal address, which may change from time to time:

Data Controller: Pireks Bakır Alaşımları San. ve Tic. A.Ş.

Email: pireks@hs01.kep.tr

Post: Ömerli Mah. Murathan Sokak No: 3 Arnavutköy - İstanbul / Türkiye

Organize San. Bölgesi Gaziosmanpaşa Mah. 2. Cad. No:11 Çerkezköy/ Tekirdağ

If Data Subjects submit written requests regarding the rights listed above to the Company, the Company will resolve the request free of charge within thirty days at the latest, depending on the nature of the request. If there is an additional cost associated with the resolution of the request by the Data Controller, the fees specified in the tariff determined by the Personal Data Protection Authority may be charged by the Data Controller. The Data Controller either accepts or rejects the request, providing a justification for the rejection, and informs the concerned person in writing or electronically. If the request is accepted, the Data Controller will take the necessary action.

If the fee charged for the request is due to the fault of the Data Controller, the fee will be refunded to the concerned party.

8. DATA MANAGEMENT AND SECURITY

8.1. The Company appoints a Data Controller and ensures the creation and implementation of necessary KVK Procedures to fulfill the obligations under the KVK Regulations, to implement and monitor the application of this Policy, and to provide recommendations for the functioning of these procedures.

8.2. All employees involved in the process are jointly responsible for the protection of Personal Data in accordance with this Policy and the KVK Procedures.

8.3. Personal Data processing activities are monitored by the Company through technical systems based on technological possibilities and application costs.

8.4. Personnel knowledgeable in technical matters related to Personal Data Processing activities are employed.

8.5. Company employees are informed and trained regarding the protection of Personal Data and its lawful processing.

8.6. Employees of the Company who need access to Personal Data shall be granted access according to the relevant KVK Procedure, and the creation and implementation of this procedure are jointly the responsibility of the Data Controller.

8.7. Employees of the Company may only access Personal Data within the scope of the authority granted to them and in accordance with the relevant KVK Procedure. Any access or processing performed beyond the employee's authority is unlawful and constitutes grounds for the immediate termination of the employment contract for just cause.

8.8. If an employee suspects that the security of Personal Data is insufficient or identifies a security breach, they must immediately report the situation to the Data Controller.

8.9. A detailed and up-to-date KVK Procedure regarding the security of Personal Data is created by the Data Controller.

8.10. Any individual provided with a Company device is responsible for the security of the device allocated to them for personal use.

8.11. Every employee or individual working within the Company is responsible for the security of physical files within their area of responsibility.

8.12. If additional security measures are required or requested under the KVK Regulations for the security of Personal Data, all employees are obligated to comply with the additional security measures and ensure their continuity.

8.13. To ensure the secure storage of Personal Data within the Company, software and hardware, including virus protection systems and firewalls, are installed in accordance with technological developments.

8.14. Backup programs are used within the Company to prevent the loss or damage of Personal Data, and adequate security measures are implemented.

8.15. Documents containing Personal Data are protected in encrypted (password-protected) systems in locked rooms outside working hours. In this context, Personal Data is not stored in common areas or on desktops. Files and folders containing Personal Data are not moved to the desktop or common folders, and information on Company computers cannot be transferred to another device such as a USB without prior written approval from the Data Controller. Personal Data cannot be taken outside of the Company.

8.16. The Committee, together with the Board of Directors, is responsible for taking technical and administrative measures to protect all Personal Data within the Company, continuously monitoring developments and administrative activities, ensuring the implementation of up-to-date KVK Procedures, submitting them to the Board of Directors for approval, announcing them within the Company after

approval, ensuring compliance, and overseeing these procedures. In this context, the Committee and Data Controller organize necessary training to increase employee awareness.

8.17. If a department within the Company processes Special Categories of Personal Data, that department is informed by the Committee about the importance, security, and confidentiality of the Personal Data they process, and the department acts in accordance with the instructions of the Committee. Access to Special Categories of Personal Data is granted only to a limited number of employees, and the list and tracking of these employees are managed by the Committee.

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

8.19. Employees of the Company are informed that their obligations regarding the security and confidentiality of Personal Data will continue even after the termination of their employment relationship, and a commitment to comply with these rules is obtained from all employees.

9. TRAINING

9.1. The Company provides necessary training to its employees regarding the protection of Personal Data in accordance with the Policy, the KVK Procedures attached, and KVKK Regulations.

9.2. The training particularly addresses the definitions and protection measures for Sensitive Personal Data.

9.3. If a company employee has physical or computer-based access to Personal Data, the Company provides training to the relevant employee regarding these accesses (e.g., the specific software programs accessed).

10. AUDIT

The Company has the right to regularly audit, without prior notice, whether all employees, departments, and contractors of the Company comply with this Policy and KVKK Regulations, and performs the necessary routine audits in this regard. The Committee and the Data Controller, if deemed necessary, will create a KVK Procedure for these audits, submit it for approval by the Board of Directors, and ensure the implementation of the said procedure.

11. BREACHES

11.1. Each employee of the Company is required to report to the Committee any work, transaction, or action they believe to be in violation of the procedures and principles outlined in the KVKK Regulations and this Policy. In this context, the Committee creates an action plan in accordance with this Policy and the KVK Procedures for the relevant breach.

11.2. Following the notifications, the Committee prepares a report to be communicated to the Data Subject or the Institution regarding the violation, considering the applicable legal provisions, including the KVKK Regulations. The Data Controller conducts correspondence and communication with the Institution.

12. RESPONSIBILITIES

The responsibilities within the Company are organized in the following order: employee, department, and Data Controller. In this context:

12.1. The Committee and the Data Controller, responsible for the implementation of the Policy, are appointed by the Board of Directors through a board decision, and any changes are made through the same process.

13. CHANGES TO THE POLICY

13.1. The Company may amend this Policy from time to time with the approval of the Board of Directors.

13.2. The Company will share the updated Policy text with its employees via email or make it available for access by employees and Data Subjects through the following website:

Relevant website: http://www.pireks.com

14. EFFECTIVE DATE OF THE POLICY

The current version of this Policy was approved by the Company's Board of Directors on 29.09.2020 and entered into force on this date.