PERSONAL DATA PROCESSING AND PROTECTION POLICY

I.PERSONAL DATA PROCESSING AND PROTECTION COMMITMENT

1. Principles that should be obeyed by and/or within Tüprag Metal Madencilik Sanayi ve Ticaret A.Ş. ("Company") while fulfilling data protection obligations that were carried into effect by means of Personal Data Protection Law numbered 6698 and other related legislations and additionally while processing personal data are determined in this Personal Data Processing and Protection Policy ("Policy").

2. Company undertakes to implement security level that is sufficient and reasonable for the personal data exists under its structure, to respect confidentiality of the personal data, and to comply with this Policy, and instruments, programs and processes to be applied in connection with this Policy.

3. This Policy also binds contractors in terms of the provisions it includes.

II. SCOPE OF THE POLICY

1. This Policy comprises all departments and employees of the Company.

2. This Policy shall involve all activities by which Company processes personal data, and shall be applied for all kinds of events and actions.

3. This Policy shall not be implemented for anonymized data or data that are not personal data.

4. In case new legislations necessitates, Company shall provide higher security level for personal data in compliance with these new legislations, and obey the requirements of the legislations.

5. If opinion is formed that there is a legal obstacle for implementation of this Policy by the Company, Company shall re-determine the steps to be carried out by consulting to the Board, if it is found necessary.

Definitions:

Terms used in this Policy have the following definitions;

Personal Data- It is data or data set under the structure of the Company that enable Company to determine identity of real persons directly or indirectly.

Specific Personal Data- It is general name given to the set consisting of persons' race, ethnic origin, political opinion, philosophical belief, religion, communion, if exists other beliefs, appearance, association, foundation, union membership, health, sexual life, penal conviction, genetic and biometric data.

Personal Health Data- All kinds of health information set of a real person whose identity is determined or determinable.

Data Processing- All kinds of processes realized on the data including collection, record, storage, alteration, re-arrangement, transfer, classification of personal data.

Related Person- Real persons whose personal data are processed by or on behalf of the Company.

Express Consent- It is the consent related with a certain subject, based on direct notification and obtained by free will.

Anonymized Data- Data that cannot be associated with the real person under no circumstances.

Data Processor- Real or legal persons who are authorized by data supervisor and process personal data on behalf of the data supervisor.

Data Supervisor- Real or legal person that processes personal data by stating processing purposes and processing means, and has the responsibility of establishment and management of data recording system.

Board- It is Personal Data Protection Board.

Committee- It is Tüprag Personal Data Protection Committee.

Sub-Committee- It is the unit, which is assigned by Tüprag management in the branches, and consists of personnel from Human Resources, Information Technologies, Public Relations, Occupational Health and Safety Departments and responsible for implementation and monitoring of this and other policies.

III. PRINCIPLES OF DATA PROCESSING

1. Compliance with Laws

Personal data shall be collected and processed according to the law and in good faith.

2. Specific, Legitimate and Explicit Aim

Personal data shall only be processed by expressing the legitimate purpose to the related person before collecting the data and in line with the purpose identified. Data owner shall ne informed about the purposes of data processing when obtaining his/her express consent. Cases of express consent requirement are subject to approval of the Committee.

3. Transparency

3.1. When personal data are processed, Company should make explicit and comprehensible notification to the related personal data owners for information purposes. This notification to be made shall respectively include the following:

a. identity of the data supervisor,

b. Purpose, management and legal reason of data processing;

c. With whom and with what reasons personal data can be shared,

d. Rights of the related person.

3.2. Individuals should be informed about the data kept by the Company and their rights arising from data processing.

3.3. Notifications to be made to the data owners shall be made by considering additional obligations stipulated by the legislations, if any.

3.4. Written form created by the Company shall be used to obtain express consent of the individual in line with this Policy before starting activity of data collection. Form should be considered specific to each case, and should not be filled out according to standard templates. In case of any hesitation about legitimacy of data processing procedure, Committee of the Company should be informed, and data collection activity should start upon the approval of the Committee.

3.5. If data processor is a third party, instead of the Company, third party should guarantee that it shall comply with the obligations stated above by means of a written agreement before data processing starts. Agreement text prepared by the Company should be used, and if this text is not sufficient, opinion of the Company Committee should be received.

4. Accurate and when necessary updated data

Company should take the measures required for the Personal data to be complete, accurate and updated. If data owner requests alteration in the personal data, related data should be updated. Company shall take the measures required to update the personal data correctly, and to delete them in case of a request or necessity.

5. Data being linked, limited and measured in terms of the processing purpose

5.1. Company undertakes to collect and process data as long as it deems it necessary and it is associated with the collection purpose. If there is data in the personal data collected which are not included in the clarifying and express consent texts, and not connected with the purpose; these data shall be anonymized or deleted, and Company shall not continue to store them based on any probability of a need. When related areas cannot be deleted or anonymized, if necessary company shall request from the individuals their personal data without including the related areas.

5.2. Apart from the legal exceptions, personal data shall not be collected and/or processed by aiming to be ready for the situations that will arise in future before purpose is shaped.

5.3. Company shall implement approach of carrying out activities in line with the right of privacy and protection of personal data in a programmed manner ("privacy by design" / "privacy by default"), and shall determine required personal data during personal data processing, and eliminate or minimize unnecessary personal data.

6. Preservation of personal data as long as it is required, and their deletion afterwards

6.1. Personal data shall be kept as long as it is necessary. In case it is required to extend this time period, obligations stipulated in the related legislations or legitimate processing benefits shall be adhered. In cases nonconforming to these definitions and still require time extension, Committee should be informed about the reason of extension.

6.2. Personal data shall be deleted after the required period expires. This time shall not be extended by means of a decision to be taken by the company without abiding by the laws.

6.3. Research shall be utilized for purposes of statistics and planning after they are deleted, and if it is deemed adequate to anonymize personal data, such utilization of which shall provide benefits for the Company, opinion of Committee should be obtained.

6.4. When purpose of collecting personal data disappears and/or legal storage period expires; department holding the data physically or electronically is responsible for carrying out destruction, deletion and annihilation processes, and this department in charge is obliged to give information to other departments where these personal data are kept.

IV. SECURITY AND CONFIDENTIALITY OF PERSONAL DATA

1. Each Company employee or person working under the structure of the Company is responsible for the security of electronic devices allocated for his/her use.

2. Each Company employee or person working under the structure of the Company is responsible for security of physical files in his/her own area of responsibility.

3. Personal data and specific personal data shall be considered by the Company as confidential information. Losing confidential information, processing them unlawfully, misusing them, their access beyond authority, their alteration or annihilation without any approval should be prevented by taking the required technical and administrative measures.

4. When there are security measures stipulated by the legislation or shall be requested additionally for security of personal data; particularly Human resources Department, and all departments processing specific personal data are obliged to comply with the additional security measures and ensure continuity of these security measures.

5. If there are departments in the Company processing specific personal data, Company shall give information to these departments about significance, security and privacy conditions of the personal data they process by means of the necessary documents.

6. Health data which are specific personal data, can only be processed by individuals stated in the legislation, and authorized by the Company.

V. PERSONAL DATA PROCESSING

Personal data may only be collected, processed or used within the scope of legal foundations stated below:

1.Express Consent

1.1 Personal data shall be processed if related persons give express consent in accordance with the 3rd provision of this Policy.

1.2. Express consent should be given with free will, otherwise it shall be void.

1.3. Express consent shall be obtained from the related person in written form or in electronic medium. Additionally oral consent may also accepted if it is recorded. Such consent shall be recorded in a provable manner. Rights of the individuals shall be notified before obtaining their express consent.

1.4. Express consent shall be obtained in written form when processing of specific personal data is required.

1.5. Consent declarations shall be documented and stored as long as data is processed.

1.6. Departments processing personal data are obliged to ensure control of presence and validity of data owner's express consent while collecting personal data to be processed. If it is determined that express consent is not obtained, data processing activity shall be terminated.

2. Processing Personal Data without Obtaining Express Consent

2.1. Personal data to be processed can be processed without obtaining express consent, if they are associated with the life or body integrity of the data owner and/ or a person other than the data owner.

2.2. When it is impossible for the data owner to give consent physically or legally, personal data may be processed without the requirement of express consent.

2.3. Personal data made public by the data owner may be processed without obtaining express consent.

2.4. It is not required to receive express consent of the data owner in cases personal data processing is clearly stipulated in the laws. Such processing of data should be within the framework of limits, obligations and requirements stipulated in the laws.

2.5. Personal data may be processed without express consent in cases such as collection of matured receivables, prevention of contract violations, providing security of the Company, etc.; provided that fundamental rights and freedoms of the individuals are not infringed.

2.6. If personal data processing without obtaining express consent is the only feasible way to establish, utilize or protect a right; personal data may be processed without obtaining express consent within the knowledge of the Committee.

3. To be Mandatory for an Agreement

3.1. If condition of being directly related with the drawing up, implementation, performance or termination of a contract is provided; personal data of contracting parties may be processed without express consent of the related individuals.

3.2. Personal data may be processed without express consent with the aim to meet the requirements of the contracting parties before or during drawing up a contract.

VI. PROCESSING SPECIFIC PERSONAL DATA

1. Specific personal data can only be processed when express consent of the data owner is received or in case it is clearly stipulated in the laws.

2. Personal data related with health and sexual life can only be processed without obtaining express consent with the aim to protect public health, to carry out preventive medicine, medical diagnosis, treatment and care services, to plan health services and finance, and management. In case of such processing, data processor has confidentiality obligation.

3. Required measures shall be taken by the Board when processing specific personal data.

4. "Tüprag Specific Personal Data Processing Policy" shall be followed while processing specific personal data.

5. If it is not clear whether or not information is a specific personal data, opinion of the Committee shall be obtained.

VII. PROCESSING DATA OF EMPLOYEES

1. All personal data processing principles stated above shall also be applied for personal data for the Company employees.

2. Personal data of individuals applying for a job by not using CV collecting channels of the Company may be processed without their express consent with the aim to initiate work relationship.

If application received in this way is finalized negatively as a result of evaluation for a certain position, personal data of the related person shall be deleted.

3. Personal data of employees that are connected with the work relationship and execution of the agreement can be processed without obtaining express consent of the employees. In the contrary case, there should be approval of the employee, legal obligation, legitimate benefit and similar reasons. Approval of the Committee should be received for validity of the related reason.

VIII. TRANSFER OF PERSONAL DATA

1. Transfer to Third Persons in Turkey

1.1. Personal data may only be transferred to third persons in Turkey when express consent of the related person is received.

1.2. Personal data may be transferred to third persons in Turkey when at least one of the conditions stated in V.2 is effective.

1.3. Department realizing the transfer is responsible for ensuring compliance with the obligations to be fulfilled during their transfer within Turkey.

2. Transfer to Third Persons Abroad

2.1. Personal data may only be transferred to third persons abroad if express consent of the related person is obtained.

2.2. Personal data may be transferred to third persons abroad without obtaining express consent of the individual when at least one of the conditions in V.2 is valid. In addition to V.2; one of the following conditions shall also be sufficient for transfer to third persons abroad:

a. When Board determines the foreign country to which personal data is transferred and protection in the required level is provided;

b. If Board does not approve foreign country to which transfer will be realized, Company and data supervisors in the related country provide a written engagement stating that required protection shall be provided, and obtain permission of the Board.

2.3. Department realizing the transfer is responsible for ensuring compliance with the obligations to be fulfilled during transfer of the personal data to abroad.

3. Transfer of Personal Health Data

3.1. Personal health data may not be transferred to third persons without obtaining express consent of the related person.

3.2. Personal health data may be transferred to public institutions and organizations without seeking for express consent of the related person in order to protect public health, to carry out preventive medicine, medical diagnosis, treatment and care services, to plan health services and finance, and management, and when it is clearly stipulated in the laws.

3.3. When compulsory transfer of the personal health data is discussed, approval of the Committee should be received.

3.4. Department realizing the transfer is responsible for ensuring compliance with the obligations to be fulfilled during transfer of the health data.

IX. DATA PROCESSING AGREEMENTS

Company may conclude an agreement with a real or legal person ("Contractor") with the aim for personal data processing on behalf of the Company as the data processor, in this way powers to be determined by the Company shall be granted. By this agreement, Company determines aim and methods of data processing activity, and instructions for the data processing activity. Monitoring of convenience of data processing activity is under the responsibility of the Company. Data processing agreements are concluded in accordance with the obligations stated below:

1. Technical and administrative capacity of the related contractor to ensure data privacy should be taken into consideration while electing the contractor.

2. Agreement to be concluded should include obligations of the Company as data supervisor, and Contractor as data processor in written form.

3. It should be ensured that Contractor fulfills its duty completely and correctly by carrying out evaluation periodically.

4. Fulfillment of the above conditions is under the responsibility of the related department of the Company as one of the contracting party.

X. RIGHTS OF RELATED INDIVIDUALS

1. Company shall give answers to the following requests of the related persons, personal data of whom is kept, in the time period defined in the law;

a. Learning whether or not Company has processed his/her own personal data,

b. Learning which personal data Company has processed,

c. Learning whether or not Company has transferred his/her personal data,

d. Learning third persons and data supervisor of the third persons to which Company has transferred his/her personal data,

e. Learning aim of the Company to process personal data,

f. Requesting the Company to update his/her personal data,

g. Requesting the Company to anonymize, delete or annihilate his/her personal data,

h. Objecting to a result against the person himself/herself by exclusively analyzing the processed data by means of automatic systems,

i. Requesting recovery of loss arising from unlawful personal data processing.

2. When execution of rights determined in the first article require certain labor force and cost, these rights can be restricted by applying to the Committee.

3. If requesting rights defined in the first article produces an adverse effect, these rights may be restricted.

4. Related data owners can contact with the Company by using following contact information to exercise their rights.

Data Supervisor: Tüprag Metal Madencilik San. ve Tic. A.Ş.

REM address: tuprag@hs.01.kep.tr

Mail: İran Caddesi Turan Emeksiz Sk. No: 1 06700 GOP, ÇANKAYA / ANKARA

XI. CONFIDENTIALITY

All personal data processed in the Company within the scope of the law is confidential. Employees may carry out collection, processing, transfer, utilization, deletion, annihilation, destruction, anonymization activities concerning personal data only within the limits of its power. Otherwise, it is forbidden for the employees to carry out these activities. Additionally, employees may not use personal data for their own purposes or for commercial purposes.

Access of employees to personal data should be determined jointly by Department managers, Sub-Committee and Information Systems Department of the Company, and duties and obligations of the employees should be analyzed while making these determinations.

Department managers should give information to their employees about the data confidentiality at the beginning of the work.
Employees shall also be informed by the related Department manager that their confidentiality obligations shall continue even after the termination of their labor contract.

XII. SECURITY

Security of the personal data is respectively under the responsibility of the Employee, Department and Company. Personal data should be protected against deletion, unlawful processing, misuse, being put into process by unauthorized persons. These security measures comprise all personal data stored physically and electronically.

Employee should raise their concerns about security of data to the Committee via related Department manager.
If data processing activities contain security risks, processing requirement should be re-evaluated, and following the risk-benefit analysis data processing should be continued or procedure should be terminated within the knowledge of the Committee.
Company's Information Technologies Department is obliged to take technical and administrative measures to protect all personal data within the Company, and follow the developments and administrative activities continuously.

XIII. TRAINING

Company shall give training to its employees about protection of personal data, and explain their obligations on this subject. Definition and applications for protection of specific personal data shall be considered particularly in the trainings. If employee of the Company reaches the personal data physically or in computer environment, Company shall give to this employee training specific to this access (for example; computer program accessed).

XIV. CONTROL

Company shall regularly control whether or not all departments in the Company and Contractors identified by the Company act according to this Policy, and Personal Data Protection Law numbered 6698. Besides the Company, departments shall also monitor the obligations determined by this Policy.

XV. VIOLATION EVENTS

Each employee of the Company is obliged to convey an action or event that he/she thinks against the restrictions defined in the Personal Data Protection Law numbered 6698, and in this Policy to the related department managers. Department manager notifies the contradictions to the Committee. As a result of the information conveyed, Committee is obliged to make notification to the related persons or authorized organization concerning violation actions or events by taking into consideration the legislation.

XVI. LIABILITIES

Liabilities within the Company respectively belong to the employee, department and Committee. Within this context;

1. Employees are responsible for all personal data that are present in their own working area in printed form or in computer environment, and provisions defined in the law and in this Policy should be complied with for all types of processing related with these data.

2. Department managers are responsible for all personal data in printed form or in computer environment and processed by the employees in the department; and should ensure that department

works in compliance with the provisions defined in the law and in this Policy for all types of processing related with these data.

3. Managers of the departments are responsible to contribute to implementation of this Policy in their own department by realizing inspections and controls.

4. Employees in the position of a manager are responsible for the personal data processing included in their own fields, and they shall ensure that personal data is processed in accordance with the law and this Policy.

5. Departments are obliged to inform the Committee about new data processing, data deletion, uncertainty and all other similar cases related with the personal data. Responsibility shall belong to the Committee after notification is realized, unless otherwise specified.

6. Following all kinds of notifications made to the Information Technologies Department of the Company about deletion, anonymization, new data entry and all other similar subjects; Information Technologies Department of the Company is obliged to perform all related processes within the time period specified in the law and in this Policy.

7. Provisions of Personal Data Protection Law and cited Turkish Criminal Law numbered 5237 are reserved in terms of contradiction to law concerning personal data covered by this Policy.

XVII. COOPERATION WITH PERSONAL DATA PROTECTION AUTHORITY

1. Company reserves its right to make alterations and updating in this Policy in connection with the Personal Data Protection Authority.

2. Cooperation with the Personal Data protection Authority shall be carried out with the Contact Person to be assigned by the Company.

3. Company shall comply with the decisions and instructions of the Personal Data Protection Authority, and shall inform its employees about this subject.

XVIII. AMENDMENTS TO BE MADE IN THE POLICY

1. Following all kinds of official alterations to be made in the related legislation, amendment can be made in this Policy by the Company in compliance with these alterations.

2. Company shall submit this Policy in an updated form for the access of its employees over the following web address.

Related web address: www.tuprag.com.tr