

1. PURPOSE

The right of every individual to request the protection of personal data about him/her is a sacred right arising from the Constitution. As ASEN ALUMINUM INDUSTRY AND TRADE INC. ("ASEN"), we consider fulfilling the requirements of this right as one of our most valuable duties. For this reason, we attach importance to the processing and protection of your personal data in accordance with the law.

As a result of the importance we attach to the protection of personal data, the Corporate Personal Data Protection Policy has been prepared to determine the principles and procedures we apply while processing and protecting personal data.

2. SCOPE

The Policy covers all kinds of operations performed on all personal data managed by ASEN, such as obtaining, recording, storing, preserving, changing, rearranging, disclosing, transferring, taking over, making available, classifying or preventing the use of all personal data data by fully or partially automatic means or non-automatic means provided that it is a part of any data recording system.

The Policy is related to all processed personal data of ASEN's partners, officials, customers, employees, supplier officials and employees and third parties.

ASEN may amend the Policy in order to comply with the legislation and the decisions of the Personal Data Protection Authority and to better protect personal data.

3. DEFINITIONS

TLDR	Description
Buyer Group	The category of natural or legal person to whom personal data is transferred by the data controller.
Explicit Consent	Consent regarding a specific subject, based on information and expressed with free will.
Anonymization	Making personal data incapable of being associated with an identified or identifiable natural person in any way, even by matching it with other data.
Contact Person	The natural person whose personal data is processed.
Relevant User	Except for the person or unit responsible for the technical storage, protection and backup of data, they are the persons who process personal data within the data controller organization or in line with the authorization and instruction received from the data controller.
Destruction	Deletion, destruction or anonymization of personal data.
Law/KVKK	Law No. 6698 on the Protection of Personal Data.

Recording Media	Any environment where personal data is processed by fully or partially automatic means or by non-automatic means, provided that it is a part of any data recording system.
Personal Data	Any information relating to an identified or identifiable natural person.
Data Inventory	The personal data processing activities carried out by data controllers depending on their business processes; The inventory they create by associating the purposes and legal reason for processing personal data, the data category, the recipient group to which it is transferred and the data subject group and details the maximum retention period required for the purposes for which personal data is processed, the personal data envisaged to be transferred to foreign countries and the measures taken regarding data security.
Personal Data Processing	Any operation performed on personal data such as obtaining, recording, storing, preserving, changing, rearranging, disclosing, transferring, taking over, making available, classifying or preventing the use of personal data by fully or partially automatic means or non-automatic means provided that it is a part of any data recording system.
Commission	The Personal Data Protection Commission established by ASEN to manage the Policy and other related procedures and to ensure the enforcement of the Policy.
Board	Personal Data Protection Board.
Institution	Personal Data Protection Authority
Special Categories of Personal Data	Data related to race, ethnic origin, political opinion, philosophical belief, religion, sect or other beliefs, appearance, membership to associations, foundations or unions, health, sexual life, criminal convictions and security measures, and biometric and genetic data.
Periodic Destruction	In the event that all of the conditions for processing personal data in the Law disappear, the deletion, destruction or anonymization process specified in the personal data storage and destruction policy and to be carried out ex officio at repeated intervals.
Politics	Personal Data Protection Policy
Data Processor	A natural or legal person who processes personal data on behalf of the data controller based on the authority granted by the data controller.
Data Controller	A natural or legal person who determines the purposes and means of processing personal data and is responsible for the establishment and management of the data recording system.

4. GENERAL PRINCIPLES

ASEN checks the compliance of the data to be processed in the preparation phase of each workflow that requires new personal data processing with the following principles. Workflows that are not eligible will not be implemented.

While ASEN processes personal data;

1. It obeys the law and the rules of honesty.
2. It makes sure that personal data is accurate and up-to-date when necessary.
3. It pays attention to the fact that the purpose of processing is specific, clear and legitimate.
4. It checks that the processed data is related to the purpose of processing, that it is processed as limited to the extent that it should be processed, and that it is proportionate.
5. It retains the data only as long as it is stipulated in the relevant legislation or necessary for the purpose of processing, and destroys it when the purpose of processing disappears.

5. DUTIES AND RESPONSIBILITIES

The Personal Data Protection Commission has been established within ASEN in order to manage this Policy and other related procedures regarding the processing of personal data and to ensure the enforcement of the Policy. The General Manager represents the Commission as the chairman and the members are department managers. In addition, ASEN also receives KVKK consultancy support in order to comply with the Personal Data Protection Law No. 6698 when necessary. If the commission deems it necessary, it may also invite KVKK consultants and professional experts to its meetings.

The duties and responsibilities of the Commission are stated below.

1. It meets normally every year. If conditions require it, extraordinary meetings can be held (for example, in the event of a possible data breach).
2. Discusses the issues that need to be changed/improved in the Policy.
3. It determines the issues that can be fulfilled in order to process and protect personal data in accordance with the law.
4. The Commission determines the steps that can be taken to increase KVKK awareness within the company and among its business partners.
5. It identifies the risks that may be encountered in the processing and protection of personal data and takes the necessary administrative and technical measures.
6. It provides contact with the institution and manages the relations.
7. It evaluates the requests from the Relevant Person.
8. It follows the periodic destruction processes.
9. Updates the Data Inventory.
10. It makes assignments regarding the above-mentioned issues.

6. MEASURES TAKEN FOR DATA SECURITY

ASEN takes all necessary technical and administrative measures to ensure the appropriate level of security in order to prevent the unlawful processing of personal data, to prevent unlawful access to personal data, and to ensure the protection of personal data.

6.1. Within the scope of the technical measures recommended by the Personal Data Protection Authority;**a) Ensuring Cybersecurity**

- Priority measures that can be taken to protect information technology systems containing personal data against unauthorized access threats over the internet,
- Ensuring that access to systems containing personal data is also limited, Employees are given limited access authority and access to the relevant systems by using username and password,
- To protect against malware, it is also necessary to use products such as antivirus, antispam, which regularly scan the information system network and detect dangers.

b) Monitoring Personal Data Security

- In order to prevent and prevent information processing systems from being exposed to both internal and external attacks and cybercrime or malware;
- Checking which software and services are running in information networks.
- Determining whether there is infiltration in information networks.
- Keeping a record of all users' transaction transactions (such as log records).
- Reporting security issues as quickly as possible.

c) Ensuring the Security of Environments Containing Personal Data

- Ensuring the physical security of devices containing personal data (laptop, mobile phone, flash disk, etc.) that may experience personal data security breaches,
- Sending personal data to be transferred by e-mail or mail by taking adequate precautions.
- In order to ensure the security of personal data, the protection of devices such as paper documents, servers, backup devices, CDs, DVDs and USBs containing personal data in sections/rooms with access authorization restrictions with additional security measures.
- Taking measures such as keeping these areas under lock and key when not in use and keeping entry and exit records.

d) Storage of Personal Data in the Cloud

- Managing the risks associated with the processing of personal data by cloud storage service providers.
- Evaluation and approval by the data controller whether the security measures taken by the cloud storage service provider are sufficient and appropriate.
- In this context, knowing in detail what personal data is stored in the cloud, backing it up, ensuring synchronization and applying authentication control.

e) Backup of Personal Data

- Ensuring that backed-up personal data is only accessible to the system administrator.
- Data set backups must be kept out of the network.
- Taking measures against the use of malware on data set backups.
- Ensuring the physical security of all backups.

f) Information Technology Systems Supply, Development and Maintenance

- If the devices sent to third institutions such as manufacturers, sellers, and services contain personal data because they are defective or due for maintenance, ensuring the security of personal data before sending these devices for maintenance and repair.
- Dismantling and storing the data storage media on the devices.
- Performing operations such as sending only defective parts.
- If personnel have come from outside for purposes such as maintenance and repair, preventing them from copying personal data and taking them out of the institution.

g) Regarding the Need for the Implementation of These Technical Measures, ASEN implements the following technical measures;

- Authority Matrix application.
- Authority Control application.
- Access Logs application.
- User Account Management app.
- Network Security app.
- Application Security management.
- Encryption management.
- Log Records application.
- Data Masking application.
- Backup management.
- Up-to-date Anti-Virus Systems management.
- Delete, Destroy, or Anonymize app.

6.2. Within the scope of the Administrative Measures Recommended by the Personal Data Protection Authority;

a) Identification of Existing Risks and Threats

- What all personal data processed by the data controller are in order to ensure the security of personal data,
- Accurately determining the probability of occurrence of risks that may arise regarding the protection of this data and the losses that will be caused in case of occurrence,
- Appropriate measures must be taken.

b) Employee Training and Awareness Activities

- To receive training on issues such as not to disclose and share personal data unlawfully.
- Conducting awareness activities for employees and creating an environment where security risks can be identified, ensuring personal data security.
- Roles and responsibilities regarding personal data security should be determined in job descriptions and employees should be aware of their roles and responsibilities in this regard.

- Acting in accordance with the principle of "Everything is Prohibited Unless Allowed" when granting access to environments containing personal data.
- Determination of Personal Data Security Policies and Procedures
- Reducing Personal Data as Much as Possible
- Management of Relations with Data Processors

Regarding the Need to Implement These Administrative Measures, ASEN implements the following administrative measures;

- Preparation of Personal Data Processing Inventory
- Corporate Policies (Antivirus, E-Mail, Physical Security, Backup, etc.)
- Contracts (Data Controller-Data Controller, / Data Controller - Data Processor Confidentiality Commitments, etc.)
- In-House Periodic and/or Random Audits
- Risk Analysis
- Employment Contract, Disciplinary Regulation (Addition of Provisions in Accordance with the Law, etc.)
- Corporate Communication (Crisis Management, Board and Relevant Person Notification Processes, etc.)
- Training and Awareness Activities (Information Security and Law)
- Notification to the Data Controllers Registry Information System (VERBIS)

7. RIGHTS OF THE RELEVANT PERSON REGARDING PERSONAL DATA

The relevant person can apply to ASEN and make a request on the following issues:

1. To learn whether their personal data is processed,
2. Requesting information if personal data has been processed,
3. To learn the purpose of processing personal data and whether they are used in accordance with their purpose,
4. To learn the third parties to whom their personal data is transferred domestically or abroad,
5. To request correction of personal data in case of incomplete or incorrect processing and to request notification of the transaction made in this context to third parties to whom personal data has been transferred,
6. Although it has been processed in accordance with the provisions of the KVKK and other relevant laws, to request the deletion, destruction or anonymization of personal data in case the reasons requiring its processing disappear and to request that the transaction made in this context be notified to third parties to whom their personal data has been transferred,
7. To object to the emergence of a result against the processed data by analyzing it exclusively through automated systems,
8. To request compensation for the damage in case of damage due to unlawful processing of personal data.

8. VIOLATION NOTIFICATIONS

ASEN employees report to the Commission any work, action or fact that they think violates the provisions of the KVKK and/or the Policy. The Commission convenes after this violation notification if it deems necessary and creates an action plan regarding the violation.

If the violation has occurred through the unlawful acquisition of personal data by others, the Commission notifies the relevant person and the Board within 72 hours within the scope of the Board's decision dated 24.01.2019 and numbered 2019/10.

9. CHANGES

Changes to the policy are prepared by the Commission and submitted to the approval of the ASEN Board of Directors. The updated Policy can be sent to employees via e-mail or published on the website.

10. REFERENCE DOCUMENTS

Law No. 6698 on the Protection of Personal Data and other legislation

11. EFFECTIVE DATE

This version of the Policy was approved by the ASEN Board of Directors on 10.02.2026 and entered into force.

H. GOKHAN ASLAN
General Manager