PERSONAL DATA RETENTION AND DISPOSAL POLICY

ARNIKON ENGINEERING LTD. (ARNIKON); In accordance with all relevant legislation, it makes the highest effort to process and store personal data in accordance with the law and to destroy it when necessary. The main purpose of this text is; Deletion, destruction or anonymization of personal data processed wholly or partially automatically or non-automatically provided that it is a part of any data recording system, pursuant to the provisions of the Law on the Protection of Personal Data No. 6689 and the Regulation on the Deletion, Destruction or Anonymization of Personal Data. information on the processes involved.

1- DEFINITIONS

• Recipient group: It is the natural or legal person category to which personal data is transferred by the data controller.

• Relevant user: Persons who process personal data within the organization of the data controller or in line with the authorization and instruction received from the data controller, excluding the person or unit responsible for technical storage, protection and backup of the data.

• Destruction: It is the deletion, destruction or anonymization of personal data.

• Recording medium: Any medium containing personal data that is fully or partially automated or processed non-automatically provided that it is a part of any data recording system.

• Personal data: Any information relating to an identified or identifiable natural person.

• Personal data processing inventory: Personal data processing activities carried out by data controllers depending on their business processes; It is the inventory that they have created by associating with the personal data processing purposes and legal reason, the data category, the transferred recipient group and the data subject group, explaining the maximum storage period required for the purposes for which personal data is processed, the personal data to be transferred to foreign countries and the measures taken regarding data security.

• Personal data retention and destruction policy: This is the policy on which data controllers base the process of determining the maximum time required for the purpose for which personal data is processed, and the process of deletion, destruction and anonymization.

• Board: It is the Personal Data Protection Board.

• Periodic destruction: It is the deletion, destruction or anonymization process that will be carried out ex officio at repetitive intervals and specified in the personal data storage and destruction policy in case all the conditions for processing personal data in the law are no longer valid.

• Registry: It is the registry of data controllers kept by the Presidency of the Personal Data Protection Authority.

• Data registration system: It is the registration system in which personal data is processed and structured according to certain criteria.

• Data controller: It is the 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.

2- AIM

This Personal Data Retention and Disposal Policy has been prepared in order to determine the procedures and principles regarding the work and transactions related to the storage and destruction activities carried out by ARNIKON.

In line with the basic principles determined by ARNIKON law; Personal data belonging to company employees, customers, and service/product providers Its Constitution has prioritized it to be processed in accordance with the Law on the Protection of Personal Data No. 6698 and the relevant regulations, and to ensure that the relevant persons use their rights effectively. Work and transactions related to the processing and protection of personal data are carried out by ARNIKON in accordance with the Policy prepared in this direction.

3- SCOPE

ARNIKON Personal Data Processing and Storage Policy; It applies to ARNIKON employees, customers, service/product providers, recording environments where data is processed, and activities for the processing of personal data.

4- RECORDING ENVIRONMENTS

ELECTRONIC ENVIRONMENTS:

Servers (Backup, e-mail, database-web, file sharing, etc.), Information security devices (Firewall, intrusion detection and prevention, log file, antivirus, etc.), Personal computers (Desktop-laptop), Mobile devices (Phone, tablet), USB, Memory Card Optical discs (Cd, DVD) printer, scanner, copier.

NON-ELECTRONIC ENVIRONMENTS:

Paper, manual data systems, written-printed-visual media.

5- REASONS FOR KEEPING PERSONAL DATA

The data controller stores the data it processes within the framework of its activities for the following purposes.

- Planning and implementation of our business strategies;
- Raising and improving our service standards and offering alternative solutions;
- Ensuring institutional functioning, planning and implementation of administrative activities;
- Performance of contracts to which it is a party;
- Ensuring the legal security of the legal relations and persons to which it is a party;
- Following all legal processes;
- Establishing relations with suppliers and managing the process;
- Establishing and securing the database;
- Duly conduct of corporate correspondence;
- Implementation and development of human resources policies;
- Planning and implementation of recruitment processes;
- Increasing the efficiency of the employees and evaluating the returns;
- Fulfillment of the obligations related to the relevant LAW and legislation;

REASONS FOR DISPOSAL OF PERSONAL DATA

Personal data is deleted, destroyed or anonymized at the request of the person concerned or ex officio in the following cases.

- Amendment or repeal of the provisions of the relevant legislation, which are the basis for processing,

- The disappearance of the purpose that requires its processing or storage,
- In cases where the processing of personal data takes place only on the basis of explicit consent, the data subject withdraws his explicit consent,

- The application made by the data controller regarding the deletion and destruction of personal data within the framework of the rights of the person concerned, pursuant to Article 11 of the Law,

- In cases where the data controller rejects the application made by the data subject to the request for the deletion, destruction or anonymization of his personal data, finds the answer insufficient or does not respond within the time stipulated in the Law; Making a complaint to the Board and this request being approved by the Board,

- The maximum period for keeping personal data has passed and there are no conditions to justify keeping personal data for a longer period of time.

6- ADMINISTRATIVE AND TECHNICAL MEASURES REGARDING THE STORAGE AND DISPOSAL OF PERSONAL DATA

Necessary administrative and technical measures are taken by the data controller for the safe storage of personal data, prevention of unlawful processing and access, and destruction of personal data in accordance with the law.

<u>Administrative Measures</u>

- Trainings are provided on prevention of unlawful processing of personal data, prevention of illegal access of personal data, protection of personal data, communication techniques, technical knowledge and skills, Law No. 657 and other relevant legislation in order to improve the quality of employees.

- Confidentiality agreements are signed by the employees regarding the activities carried out by the Institution.

- A disciplinary procedure has been prepared for employees who do not comply with security policies and procedures.

- Before starting to process personal data, the obligation to inform the data subjects is fulfilled by the data controller.

- Personal data processing inventory has been prepared.

- Periodic and random inspections are carried out within the institution.

- Information security trainings are provided for employees
- The security of the places where personal data is stored physically is ensured and the access authority is limited.
- Awareness of data processing service providers on data security is ensured.
- Personal data is backed up and the security of the backed up personal data is also ensured.
- Personal data is reduced as much as possible.
- The security of environments containing personal data against external risks is ensured.
- Necessary security measures are taken regarding entry and exit from environments containing personal data.
- Extra security measures are taken for personal data transferred via paper and the relevant document is sent in confidential document format.
- The authorizations of employees who have a change of job or quit their job in this field are removed.
- Confidentiality commitments are made.
- Institutional policies on access, information security, use, storage and destruction have been prepared and started to be implemented.

Technical Measures

- Encryption is done.
- Existing risks and threats have been identified.
- User account method and authorization control system are implemented and these are also followed.
- Current anti-virus systems are used.
- Network security and application security are provided.

7- DISPOSAL TECHNIQUES OF PERSONAL DATA

At the end of the storage period required for the period stipulated in the relevant legislation or for the purpose for which they are processed, the personal data is destroyed by the Data Controller ex officio or upon the application of the data subject, again in accordance with the provisions of the relevant legislation, with the following techniques.

a- Deletion of Personal Data

Data Recording Environment	Explanation
Personal Data on Servers	The system administrator removes the access authorization of the relevant users and deletes the personal data on the servers for those whose period of time has expired.
Personal Data in Electronic Media	Among the personal data in the electronic environment, the ones whose period has expired are rendered inaccessible and non-reusable for other employees (related users) except the database administrator.
Personal Data in Physical Environment	Personal data kept in the physical environment is made inaccessible and unusable in any way for other employees, except for the unit manager responsible for the document archive, for those whose period of time has expired. In addition, the process of blackening is applied by drawing/painting/erasing in a way that cannot be read.
Personal Data in Portable Media	Of the personal data kept in flash-based storage media, the expired ones are encrypted by the system administrator and the access authorization is given only to the system administrator, and they are stored in secure environments with encryption keys.

a- Destruction of Personal Data

Data Recording Environment	Explanation
Personal Data in Physical Environment	Of the personal data in the paper medium, the ones that need to be kept, which have expired, are irreversibly destroyed in the paper clipping machines.
Personal Data in Optical / Magnetic Media	The physical destruction of the personal data in optical media and magnetic media, such as melting, burning or pulverizing, is applied. In addition, magnetic media is passed through a special device and exposed to a high magnetic field, making the data on it unreadable.

8- STORAGE AND DISPOSAL TIMES

Regarding the personal data being processed by the data controller within the scope of its activities;

- The storage periods on the basis of personal data regarding all personal data within the scope of activities carried out in connection with the processes are in the Personal Data Processing Inventory;

- Storage periods on the basis of data categories are recorded in VERBIS;

- Updates are made on the said retention periods, if necessary. For personal data whose storage period has expired, ex officio deletion, destruction or anonymization is carried out by the data controller.

Process	Storage Time	Disposal Time
Human resources process	Legal action + 10 years	The first periodic disposal period following the end of the storage period
Customer Transaction	Legal action + 10 years	The first periodic disposal period following the end of the storage period

In accordance with the 11th article of the regulation, ARNIKON has determined the period of periodic destruction as 6 months. Accordingly, the periodic destruction process in June and December every year is carried out by the persons authorized by the policy by taking minutes.

8- PUBLICATION / STORAGE OF THE POLICY EFFECTIVE DATE AND UPDATES TO THE POLICY

The policy is published in two different media, with wet signature (printed paper) and electronically, and is disclosed to the public on the website. The printed paper copy is kept in the company's file.

The policy is deemed to have entered into force after its publication on the company's website. If it is decided to be revoked, old copies of the Policy with wet signatures are canceled and signed by the company's authorized signatories (with the cancellation stamp or by writing cancellation) and are kept by the company for at least 5 years. The Policy can be updated after the amendment to be made in the relevant legislation or if deemed necessary.