ANGST PFİSTER GELİŞMİŞ TEKNİK ÇÖZÜMLER A.Ş.

PERSONAL DATA STORAGE AND EXTERMINATION POLICY

APTR

PERSONAL DATA STORAGE AND EXTERMINATION POLICY

ARTICLE 1 – PURPOSE OF THE POLICY

The personal data processing and ensuring the effective exercise of the rights in accordance with T.C. Constitution, International Conventions, Law on the Personal Data Protection No. 6698 ("***PDP Law***") and other relevant legislation of the current and potential customers, suppliers, employees and job applicants, our BoD members, our guests and the other firms' employees, shareholders or the other third parties to whom we work with is a significant issue for Angst Pfister Gelişmiş Teknik Çözümler A.Ş. (hereinafter referred to as the "***Company***" or "***APTR***") which is one of the leading suppliers of leading OEM and Tier-1 automotive companies as a leading vibration prevention and sealing solutions provider, co-design and manufacturing partner, primarily in the automotive sector.

This Personal Data Storage and Extermination Policy ("***Policy***"), has been prepared in order to determine the procedures and principles regarding the storage and extermination of personal data within the Company and its affiliates. APTR's activities and transactions relating to the storage and extermination of personal data processed shall be carried out in accordance with this Policy.

ARTICLE 2 – SCOPE OF THE POLICY

The provisions of this Policy includes any and all personal data processing of the personal data processing and protection of the current and potential customers, suppliers, employees and job applicants, our BoD members, our guests and the other firms' employees, shareholders or the other third parties to whom we work with, within our Company by fully or partially through automatic means or provided that the process is a part of any data registry system, through non-automatic means or all data registry environment where personal data managed by our company.

ARTICLE 3 – DEFINITIONS

Explicit Consent	Refers to the freely given, specific and informed consent.
Receiving Group	Refers to the category of natural or legal person to whom personal data is transmitted by the data controller.
Anonymisation	Refers to rendering personal data impossible to link with an identified or identifiable natural person, even though matching them with other data.
Electronic Media	Refers to environments in which personal data can be created, read, modified and written with electronic devices.
Non-electronic Media	Refers to other environments that all written, printed, visual, etc. out of electronic media.
Extermination	Refers to erasure, destruction or anonymisation of personal data.
Law	Refers to Law on the Personal Data Protection No. 6698.

Personal Data	Refers to all and any information relating to an identified or identifiable natural person (e.g. name-surname, ID no, e-mail, address, date of birth, credit card number etc.).
Personal Data Processing	Refers to any operation performed upon personal data such as collection, recording, storage, retention, alteration, re-organization, disclosure, transferring, taking over, making retrievable, classification or preventing the use thereof, fully or partially through automatic means or provided that the process is a part of any data registry system, through non-automatic means.
Data Subject	Refers to all real persons processing personal data (e.g. customers, suppliers, employees, guests etc.)
Personal Data Storage Environment	Refers to any environment in which personal data is processed that is completely or partially automated or processed by non-automated means provided that it is part of any data recording system.
Board	Refers to Personal Data Protection Board.
Customers	Refers to the real or legal persons that APTR provides goods and services within the scope of its activities.
Sensitive Personal Data	The personal data regarding the race, ethnic origin, political opinion, philosophical belief, religion, sect or other belief, clothing, membership to associations, foundations or trade-unions, health, sexual life, convictions and security measures, and the biometric and genetic data are deemed to be sensitive personal data.
Periodic Extermination	Refers to the process of erasuring, destroying or anonymising at the repeated intervals specified in the personal data storage and extermination policy In the event that all the conditions for processing the personal data contained in the law are eliminated.
Policy	Refers to Personal Data Storage and Extermination Policy.
Supplier	Refers to a natural or legal person providing goods and services under a specific contract with APTR.
Data Processor	Refers to the natural or legal person who processes personal data on behalf of the Data Controller.
Data Registry System	Refers to the registry system in which personal data is structured and processed according to certain criteria.
Data Processor	

	Refers to the real or legal person who processes personal data based on the authority granted by and on behalf of the data controller. For example, the suppliers who have been submitted information for employee candidates.
Regulations	Refers to the Regulation on Erasure, Destruction or Anonymisation of Personal Data published in the Official Gazette dated 28.10.2017.

ARTICLE 4 – FUNDAMENTAL PRINCIPLES

This Policy is a guiding legislation that sets forth the principles and procedures of the rules stipulated under the PDP Law and other related regulation. Our company shall analyse the data processing activities conducted by taking this Policy as a guideline, and shall determine all necessary actions and take all necessary administrative and technical measures within this scope.

In all of these processes, our Company is aware that the personal data processed in order to ensure legal compliance of our Company, must comply with the general principles and provisions under the PDP Law and other related legislation. In this regard, the fundamental principles for personal data processing within the scope of the article 4 of the PDP Law are as follows:

The following principles shall be complied with when processing personal data:

- Being in conformity with the law and good faith,
- Being accurate and if necessary, up to date,
- Being processed for specified, explicit, and legitimate purposes,
- Being relevant, limited and proportionate to the purposes for which data are processed,
- Being stored only for the time designated by relevant legislation or necessitated by the purpose for which data are collected.

Within the framework of this context, all above-mentioned principles shall be taken into consideration by our Company while all personal data processing activities to be made such as collection, recording, storage, retention, alteration, re-organization, disclosure, transferring, taking over, making retrievable, classification, preventing the use or exterminating thereof of the personal data.

ARTICLE 5 – PERSONAL DATA STORAGE ENVIRONMENTS

APTR stores personal data securely in electronic and non-electronic environments in accordance with the law.

- Local server
- Cloud
- Software
- Computers, Mobile Devices
- Drives
- Portable memory
- Printer, scanner, copier
- Department file cabinets
- Archive

ARTICLE 6 – STORAGE AND EXTERMINATION OF PERSONAL DATA

Personal data of the current and potential customers, suppliers, employees and job applicants, our BoD members, our guests and the other firms' employees, shareholders or the other third parties are stored and exterminated by our Company in accordance with the law.

The processed personal data shall be stored in accordance with the condition of being relevant, limited and proportionate to the purposes for which they are processed and kept for the period foreseen in the relevant legislation or required for the purpose stipulated in Article 4 of the Law.

ARTICLE 7 – PROCESSING REQUIREMENTS FOR STORAGE

APTR stores the processed personal data within the scope of its activities for the following purposes.

- Provision of employment and workforce needs, carry out application process and selection and placement processes of employee candidates.
- Fulfill the obligations arising from the employment contract and legislation for the employees.
- Carry out side benefits and interests processes for the employees.
- Carry out human resources processes.
- Carry out training activities.
- Ensure the security of physical space.
- Ensure the legal or technical security of the persons in business relationship with our company.
- Ensure the fulfillment of legal obligations as required by legal regulations.
- Provide contact with natural or legal persons that have business relations with APTR.
- Perform works and transactions within the framework of contracts and protocols signed within the scope of supply or sale of goods or services.
- Carry out finance and accounting transactions.
- Follow and carry out legal affairs.
- Carry out occupational health and safety activities.
- Carry out logistics activities.
- Inform authorized persons, institutions and organizations.
- Carry out the necessary works for commercial or operational activities and conduct the business processes related to.

ARTICLE 8 – REQUIREMENTS FOR EXTERMINATION

Personal data shall be erased, destructed or anonymised by APTR, ex officio or upon demand by the data subject in the following situations;

- Disappearance of reasons which require the process or storage.
- Withdrawal of explicit consent if the personal data is processed subject to the explicit consent requirement.
- Amendment or abolition of the relevant legislation provisions which constitute the basis for the processing of personal data.
- The maximum period of time required to keep personal data has passed or absence of any requirement to justify storing personal data for longer periods of time.
- Complain to the Board and request is approved; in case of APTR rejects the application made by the person concerned with the request to erasure, destruct or anonymise his/her personal data, he/she finds the answer inadequate or APTR does not respond within the period stipulated in the Law.

ARTICLE 9 – NECESSARY TECHNICAL AND ORGANISATIONAL MEASURES

APTR shall take all necessary technical and organizational measures for storing personal data in a secure way, preventing it from being processed and accessed illegally and exterminated of it in accordance with the article 12 of the Law and other related provisions.

9.1. Organizational Measures

- Employee awareness trainings are organized on data security periodically.
- Employees are signed a commitment to confidentiality and protection of personal data related to the activities carried out by APTR.
- Personal data processing inventory has been prepared.
- Policies and procedures for personal data protection and storage and extermination have been adopted.
- Signed contracts contain data security provisions.
- The obligation of inform data subject before processing is fulfilled.
- Internal periodic audits are conducted.
- Trainings were provided for and confidential agreements were signed with the employees involved in sensitive personal data processing processes. The authorities of the employees who have access to the data were determined.

9.2. Technical Measures

- Corporate policies on information security, access and use, storage and extermination are prepared and implemented.
- Risks and threats that will affect information systems are monitored as a result of analyzes conducted with information security incident management. Incidents of information security violations are reported and recorded. In this context, necessary measures are taken
- Network security and firewalls are provided.
- Anti-virus programs with automatic updates are used. It is regularly checked for the timeliness and availability of this program.
- Special use procedure has been established within the framework of VPN technology for users accessing the Company's computer network over the Internet.
- Log records are kept in an electronic environment.
- Access to systems containing personal data is restricted. In this context, employees are granted access rights to the extent necessary for their work and duties, access to related systems is provided by using user name and password.
- Strong passwords are used in electronic environments where personal data is processed and stored.
- Necessary security measures are taken for entering and exiting physical environments containing personal data.
- Secure logging systems are used in electronic environments where personal data are processed.
- Only authorized personnel is permitted enter the system room in order to ensure security of information systems. The system room is monitored by a 24/7 security camera. The system room is protected against environmental threats such as flood, rain and fire and appropriate measures are taken thereof.
- Data backup programs are used to ensure the safe storage of personal data. Storing information on local disks of computers is prohibited, and files and documents are stored on corporate storage devices where backup operations are performed to ensure security

- Personal data on paper is stored in lockers. Unauthorized access is prevented by providing physical security.
- Destruction of personal data on paper media is carried out with shredder.
- Necessary measures are taken to ensure that deleted personal data cannot be accessed and reused for the relevant users.
- Security is ensured in the physical environments where sensitive personal data is processed, stored or accessed.

ARTICLE 10 – PERSONAL DATA EXTERMINATION TECHNIQUES

Personal data shall be exterminated by the following techniques in cases stipulated by Law and related secondary legislation;

10.1. Erasure of Personal Data

On Server	It is deleted by the "delete" command in the operating system or by removing the access rights of the relevant users on the directory where the file is located by the system administrator.
On Software	The corresponding lines with personal data are deleted with the "delete" command. It is made inaccessible to other users (employees) except the database administrator.
On Paper	It is rendered inaccessible to other employees except the unit manager responsible for the file archive. In addition, it can be unreadable by drawing / painting / wiping and dimming.
On Portable Equipment	It is stored in a secure environment by being encrypted by the system administrator and giving access only to the system administrator.

10.2. Destruction of Personal Data

On Paper	The paper is irreversibly destructed by using the shredder machine.
On Optical/Magnetic Equipment	It is stored in a secure environment by being encrypted by the system administrator and giving access only to the system administrator. Physical destruction such as incineration, dusting is applied.

10.3. Anonymisation of Personal Data

Anonymisation of personal data is defined as rendering personal data impossible to link with an identified or identifiable natural person, even though matching them with other data.

Personal data shall be made irrelevant to identified or identifiable natural person in spite of the use of appropriate techniques in terms of the registry medium and the relevant field of activity such as retrieving and matching personal data with another data by controller, receiver or receiver groups.

ARTICLE 11- PERIOD OF STORAGE AND EXTERMINATION

Process	Storage Period	Extermination Period
Execution of human resources processes	10 Years	During the first periodic destruction period following the end of the storage period
Preparation and execution of Contracts	10 Years	During the first periodic destruction period following the end of the storage period
Execution of finance and accounting affairs	10 Years	During the first periodic destruction period following the end of the storage period
Carrying out occupational health and safety activities	10 Years	During the first periodic destruction period following the end of the storage period
Conducting information security processes	2 Years	During the first periodic destruction period following the end of the storage period
Keeping camera recordings	15 Days	Automatically deleted by overwriting
Keeping visitor records	1 Year from the end of the visit	During the first periodic destruction period following the end of the storage period
Execution of corporate law processes	5 Years	During the first periodic destruction period following the end of the storage period

** A longer period in accordance with the legislation or statute of limitations under the legislation, entitlement period, retention periods and so on for a longer period of time, the periods in the provisions of the legislation shall be considered as the maximum retention period.*

ARTICLE 12- PERIODIC EXTERMINATION TIME

Pursuant to Article 11 of the Regulation, APTR has determined the period of periodic extermination as 6 (six) months.

ARTICLE 13 – EXECUTION OF THIS POLICY

The execution date of this Policy is April 2nd, 2018. In case of amendment of all or some particular articles, the execution date of this Policy will be updating.

This Policy is submitted to physically reach of everyone whose personal data being processed by our Company through our company's website https://www.angst-pfister.com/tr, Company's Human Resources Department and security cabin that is in the entrance of our company.

Annex – Storage and Extermination Distribution of Tasks

DISTRIBUTION OF TASKS

TITLE	DEPARTMENT	TASKS
APTR HR Manager	Human Resources	Responsible for overseeing compliance with the policy, eliminating deficiencies and ensuring correct implementation.
APTR HR Manager	Human Resources	Responsible for the preparation, execution, publication and updating of the policy.
IT specialist	IT	Responsible for technical aspects of the policy.