1. PURPOSE

This policy has been prepared in order to determine the procedures and principles regarding the processing of personal data of natural persons in accordance with the Constitution of the Republic of Turkey and the International Conventions on human rights to which our country is a party and the relevant legislation, especially the Law No. 6698 on the Protection of Personal Data ("KVKK"), and the deletion, destruction or anonymization in the event that all processing conditions are eliminated.
We carry out transactions regarding the processing, storage and transfer of all personal data we obtain during our activities in accordance with the Policy on Processing and Protection of Personal Data ("Policy"). The protection of personal data and the observance of the fundamental rights and freedoms of natural persons whose personal data are collected is the basic principle of our policy regarding the processing of personal data. For this reason, we carry out all our activities where personal data is processed by observing the protection of privacy of private life, confidentiality of communication, freedom of thought and belief, and the right to use effective legal remedies. For the protection of personal data, we take all administrative and technical protection measures required by the nature of the relevant data in accordance with the legislation and current technology. This Policy explains the methods we follow regarding the processing, storage, transfer, deletion and deletion or anonymization of personal data shared during our commercial or social responsibility and similar activities within the framework of the principles mentioned in the KVKK.

DEFINITIONS

Network : A network is a structure in which multiple computers are connected to each other for various reasons such as information sharing, software and hardware sharing, centralized management and ease of support. Network devices : Devices used to create network structures.

Anonymization: Making personal data impossible to be associated with an identified or identifiable natural person under any circumstances, even by matching with other data.

Information security : Means preventing unauthorized or unauthorized access, use, modification, disclosure, destruction, alteration or damage to information.

Cloud system : A cloud system is a system model that users can access over a network to protect and manage data remotely.

DDos : A cyber-attack that overloads the system more than it can handle and makes it unable to respond.

DDos Mitigator: Service provided to prevent a DDos attack

Direct identifiers: Identifiers that, by themselves, directly reveal, disclose and make distinguishable the person with whom they are associated,

Indirect identifiers : Identifiers that, in combination with other identifiers, reveal, disclose and make distinguishable the person with whom they are associated,

Relevant person: The natural person whose personal data is processed,

Relevant user: Natural or legal persons who process personal data within the organization of the data controller or in accordance with the authorization and instruction received from the data controller, except for the person or unit responsible for the technical storage, protection and backup of the data,

Destruction : Deletion, destruction or anonymization of personal data,

KVKK : Law on the Protection of Personal Data dated 24.3.2016 and numbered 6698,

Blackout : Processes such as crossing out, painting and icing the entirety of personal data in a way that cannot be associated with an identified or identifiable natural person,

Recording medium : Any medium containing personal data that is fully or partially automated or processed by non-automated means, provided that it is part of any data recording system,

Personal data retention and destruction policy: The policy on which data controllers base the process of determining the maximum period necessary for the purpose for which personal data are processed and the process of deletion, destruction and anonymization,

Correlation : A method of assessing the relationship between two variables.

Log : Documents that record the process performed on computers.

Masking : Operations such as deleting, crossing out, coloring and starring certain areas of personal data in a way that cannot be associated with an identified or identifiable natural person,

Optical media : Optical media are storage media that hold content in digital form and are written and read by a laser.

Data recording system: A recording system in which personal data is structured and processed according to certain criteria.

Zeroday : Software and hardware flaws that are previously unknown or undetected but contain vulnerabilities that could lead to serious attacks.

2. RECORDING MEDIA

Personal data belonging to the data subjects are securely stored by A-plas (hereinafter referred to as the "Company") in the environments listed in the table below in accordance with the relevant legislation, especially the provisions of the KVKK, and within the framework of international data security principles.

ELECTRONIC MEDIA	NON-ELECTRONIC MEDIA
Servers (Domain, backup, e-mail (Exchange), database, web, file sharing, etc.) ✓ Software (office software, portal, ERP, pdks) ✓ Information security devices (security, log file, antivirus, etc.) ✓ Personal computers (desktop, laptop) ✓ Mobile devices (phones, tablets, etc.) ✓ Optical discs (CD, DVD etc.) ✓ Removable memories (USB, Memory Card, etc.) ✓ Printer, scanner, photocopier ✓ Removable memories (USB, Memory Card, etc.) ✓ Printer, scanner, copier	✓ Paper ✓ Manual data recording systems (questionnaire forms, visitor logbook) ✓ Written, printed, visual media

3. STORAGE OF PERSONAL DATA

3.1. Environments where Personal Data are Stored

The Company stores personal data processed by fully automatic or partially automatic means or by non-automatic means, provided that they are part of any data recording system, in the following environments in accordance with the law:

Electronic Media:

✓ Physical and Virtual Servers
✓ Software
✓ Information Security Devices
✓ Institutional Computer Internal Disk
✓ Mobile Devices
✓ External Memory (USB, External Hard Disk, etc.)
✓ Printer, Scanner, Copier

Physical Environment:

✓ Printed Document / Copy / Document
✓ Office Space
✓ Common Archive

3.2. Ensuring the Security of Environments Where Personal Data is Stored

The Company takes the necessary technical and administrative measures in accordance with the technological possibilities and the cost of implementation in order to store personal data in secure environments and to prevent the destruction, loss or alteration of personal data for unlawful purposes.

3.2.1. Administrative and Technical Measures

Data Security Measure
Network security and application security are ensured.
Closed system network is used for personal data transfers through the network.
Security measures are taken within the scope of procurement, development and maintenance of information technology systems.
There are disciplinary regulations for employees that include data security provisions.
Training and awareness raising activities on data security are carried out for employees at regular intervals.
Authorization matrix has been created for employees.
Access logs are kept regularly.

Corporate policies on access, information security, use, storage and disposal have been prepared and implemented.
Data masking measures are applied when necessary.
Confidentiality commitments are made.
Employees who are reassigned or leave their jobs are de-authorized in this area.
Up-to-date anti-virus systems are used.
Firewalls are used.

Data Security Measure
The signed contracts contain data security provisions.
Extra security measures are taken for personal data transferred via paper and the relevant document is sent in the format of a confidential document.
Personal data security policies and procedures have been determined.
Personal data security issues are reported quickly.
Necessary security measures are taken regarding entry and exit to physical environments containing personal data.
Physical environments containing personal data are secured against external risks (fire, flood, etc.).
The security of environments containing personal data is ensured.
Personal data is minimized as much as possible.
Personal data is backed up and the security of backed up personal data is also ensured.
User account management and authorization control system are implemented and monitored.
Internal periodic and/or random audits are conducted and commissioned.
Log records are kept without user intervention.
Existing risks and threats have been identified.

Data Security Measure
If sensitive personal data is to be sent via electronic mail, it is sent encrypted and using a KEP or corporate mail account.
Intrusion detection and prevention systems are used.
Penetration test is applied.
Cyber security measures have been taken and their implementation is constantly monitored.
Encryption is performed.
Sensitive personal data transferred on portable memory sticks, CDs and DVDs are encrypted.
Data processing service providers are periodically audited on data security.

4. LEGAL AND TECHNICAL REASONS FOR THE STORAGE AND DESTRUCTION OF PERSONAL DATA

4.1. Reasons for Retention of Personal Data

4.1.1. Legal Grounds for Retention of Personal Data

Personal data by the Company;

✓ In order for the Company to fulfill its legal responsibilities that have arisen or may arise and in accordance with the measures and/or periods prescribed by law,

✓ Data that is foreseen to be deleted and/or anonymized; in a way that is not ready for access ("live") in backup/archive and similar environments for business continuity, prevention of data loss and data protection purposes,

✓ Data to be destroyed by deletion, destruction or anonymization immediately after the purpose of processing ceases to exist and at the latest until the next periodic destruction date,

It will continue to hide.

Personal data processed within the framework of the Company's activities are retained for the period stipulated

in the relevant legislation. In this context, personal data;

✓ Law No. 6698 on the Protection of Personal Data

✓ Turkish Code of Obligations No. 6098,
✓ Law No. 5510 on Social Security and General Health Insurance,
✓ Law No. 6331 on Occupational Health and Safety,
✓ Law No. 4982 on Access to Information,
✓ Law No. 5115 on Identity Notification,
✓ Labor Law No. 4857,
✓ Law No. 2004 on Execution and Bankruptcy,
✓ Law No. 5434 on Retirement Health,
✓ Law No. 2828 on Social Services
✓ Regulation No. 25369 on Health and Safety Measures to be Taken in Workplace Buildings and Annexes,
✓ Regulation No. 24015 on Archive Services
✓ Law No. 5651 on the Regulation of Publications on the Internet and Combating Crimes Committed through These Publications,
✓ Other legislation.
They are retained for the retention periods stipulated under other secondary regulations in force pursuant to these laws.

4.2. Reasons Requiring Destruction of Personal Data

Personal data;
• Amendment or abolition of the relevant legislation provisions that constitute the basis for processing,
• The purpose requiring processing or storage disappears,
• In cases where the processing of personal data takes place only on the basis of explicit consent, the data subject's withdrawal of explicit consent,
• Pursuant to Article 11 of the Law, the Company accepts the application made by the data subject for the deletion and destruction of his/her personal data within the framework of his/her rights,
• In cases where the Company rejects the application made by the data subject with the request for the deletion, destruction or anonymization of his/her personal data, finds the answer insufficient or does not respond within the period stipulated in the Law; to file a complaint to the Board and this request is approved by the Board,
• In the event that the maximum period required for the retention of personal data has expired and there are no conditions that justify the retention of personal data for a longer period of time, the personal data shall be deleted, destroyed or deleted, destroyed or anonymized ex officio by the Company or upon the request of the relevant person.

4.2.1. Legal Grounds for Destruction of Personal Data
Personal data by the Company;

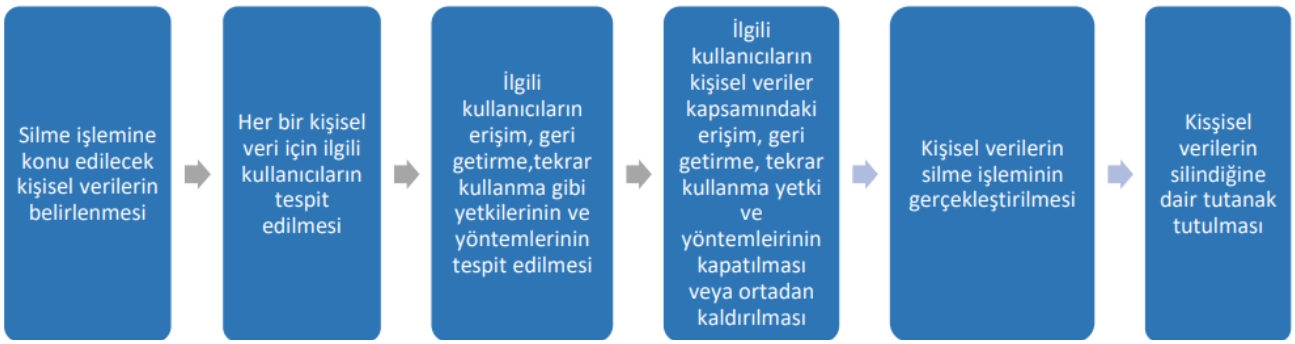
✓ The disappearance of the purposes requiring the processing of Personal Data and the reasons requiring its storage, the amendment or abolition of the provisions of the relevant legislation,
✓ In cases where the processing of Personal Data takes place only on the basis of explicit consent, the person concerned withdraws his/her explicit consent,
✓ The relevant person requests the destruction of his/her personal data by using his/her rights specified in Article 11 of the KVKK and the application made is accepted by the Company,
✓ The maximum period of time required for the retention of Personal Data has expired,

✓ Your personal data will be destroyed if there are no circumstances that justify keeping the personal data for a longer period of time.

5. DELETION OF PERSONAL DATA

Deletion of personal data is the process of making personal data inaccessible and non-reusable in any way for the relevant users. The Company is obliged to take all necessary technical and administrative measures to ensure
that deleted personal data is inaccessible and non-reusable for the relevant users.

5.1. Process of Deletion of Personal Data



5.2. Deletion of Personal Data

5.2.1. Deletion Methods According to Recording Media

Since personal data can be stored in various recording media, they must be deleted by methods appropriate to the recording media. Examples of this are given below.

a) Application-as-a-Service Type Cloud Solutions

The data in the Cloud system must be deleted by the Company by issuing a delete command. While performing
the aforementioned operation, it should be noted that the relevant users of the Company are not authorized to
restore the deleted data on the Cloud system.

b) Personal Data on Paper

Personal data on paper media must be erased by the Company using the blackout method. The blackout process
is performed by cutting out the personal data on the relevant document, where possible, and making it invisible
to the relevant users by using fixed ink in a way that cannot be reversed and cannot be read by technological solutions.

c) Office Files on the Central Serve

The file must be deleted with the delete command in the operating system or the access rights of the relevant user on the file or the directory where the file is located must be removed by the Company. While performing the aforementioned operation, it should be noted that the relevant user of the Company is not also the system administrator.

ç) Personal Data on Portable Media

Personal data on Flash-based storage media should be stored encrypted and deleted using software suitable for these media.

d) Databases

The relevant rows containing personal data should be deleted with database commands. While performing the aforementioned operation, it should be noted that the relevant user of the Company is not also the database administrator.

5.3. Destruction of Personal Data

Destruction of personal data is the process of making personal data inaccessible, unrecoverable and nonreusable by anyone in any way. The Company takes all necessary technical and administrative measures regarding the destruction of personal data.

5.3.1. Methods of Destruction of Personal Data

In order to destroy personal data, it is necessary to identify all copies of the data and destroy them one by one using one or more of the following methods depending on the type of systems in which the data is located:

a) Local Systems

One or more of the following methods can be used by the Company to destroy the data on the systems in question.

i) De-magnetization: It is the process of passing the magnetic media through a special device and exposing it to a very high magnetic field to distort the data on it in an unreadable way.

ii) Physical Destruction: The process of physically destroying optical media and magnetic media, such as melting, burning or pulverizing them. By melting, burning, pulverizing or passing the optical or magnetic media through a metal grinder, the data is rendered inaccessible. In the case of solid state disks, if overwriting or de-magnetizing is not successful, this media must also be physically destroyed.

iii) Overwriting: It is the process of writing random data consisting of 0s and 1s at least seven times on magnetic media and rewritable optical media to prevent the recovery of old data. This process is done using special software.

b) Environmental Systems

Destruction methods that can be used depending on the type of company data recording media are listed below:

i) Network devices (switches, routers, etc.): The storage media inside these devices is fixed. Most of the time, the products have a wipe command but not a destroy feature. They must be destroyed using one or more of the appropriate methods specified in paragraph "a".

ii) Flash-based media: Flash-based hard disks with ATA (SATA, PATA, etc.), SCSI (SCSI Express, etc.) interfaces must be destroyed by using the command if supported, or by using the manufacturer's recommended
destruction method if not supported, or by using one or more of the appropriate methods specified in a.

iii) Magnetic tape: These are media that store data with the help of micro magnet parts on flexible tape. It must be destroyed by exposing it to very strong magnetic environments and de-magnetizing it or by physical destruction methods such as incineration and melting.

iv) Units such as magnetic disks: These are media that store data with the help of micro-magnet parts on flexible (platters) or fixed media. They must be destroyed by exposing them to very strong magnetic environments and de-magnetizing them or by physical destruction methods such as incineration or melting.

v) Mobile phones (Sim card and fixed memory spaces): Fixed memory spaces on portable smartphones have a delete command, but most do not have a destroy command. They should be destroyed using one or more of the appropriate methods described in a.

vi) Optical disks: Data storage media such as CDs and DVDs. They must be destroyed by physical destruction methods such as incineration, fragmentation, melting.

vii) Peripherals such as printers, fingerprint door access systems whose data recording media are removable: All data recording media must be destroyed by verifying that they have been removed and using one or more of the appropriate methods specified in a according to their characteristics.

viii) Peripherals whose data recording medium is fixed, such as printers, fingerprint door access systems: Most of these systems have a delete command but not a destroy command. They must be destroyed using one or more of the appropriate methods specified in a.

c) Paper and Microfiche Media

Since the personal data on such media is permanently and physically written on the media, the main media must
be destroyed. When this is done, it is necessary to shred the media with paper shredding or shredding machines
into small pieces of incomprehensible size, if possible horizontally and vertically, so that they cannot be reassembled.
Personal data transferred from the original paper format to electronic media through scanning must be destroyed by using one or more of the appropriate methods specified in a, depending on the electronic media in which they are located.

d) Cloud Environment

During the storage and use of personal data in the said systems, it must be encrypted with cryptographic methods and where possible for personal data, encryption keys must be used separately, especially for each cloud solution that the Company receives service. When the cloud computing service relationship ends; all copies of the encryption keys required to make personal data usable must be destroyed.
In addition to the above-mentioned environments; The destruction of personal data contained in the Company's devices that malfunction or are sent for maintenance is carried out as follows:

i) Destruction of the personal data contained in the relevant devices by using one or more of the appropriate methods specified in a) before transferring them to third institutions such as manufacturers, sellers,

services for maintenance and repair,

ii) In cases where destruction is not possible or appropriate, dismantling and storage of data storage media, sending other defective parts to third parties such as manufacturers, vendors, service centers,

iii) Taking necessary measures to prevent personnel coming from outside for maintenance and repair purposes from copying personal data and taking them out of the organization, It is necessary

6. ANONYMIZATION

Anonymization is the removal or modification of all direct and/or indirect identifiers in a dataset, preventing the identification of the person concerned or losing the ability to be distinguishable in a group/crowd in such a way that it cannot be associated with a real person. As a result of the prevention or loss of these features, data that do not point to a specific person are considered anonymized data. In other words, anonymized data is information that identifies a real person before this process was carried out, but after this process, it has become unassociable with the person concerned and its connection with the person has been severed. The purpose of anonymization is to break the link between the data and the person identified by this data. All of the disconnection processes carried out by methods such as automatic or non-automatic grouping, masking, derivation, generalization, randomization applied to the records in the data recording system where personal data is kept are called anonymization methods. The data obtained as a result of the application of these methods should not be able to identify a specific person.

6.1. Methods of Anonymization of Personal Data

6.1.1. Anonymization methods that do not introduce value irregularity

In non-value regularization methods, no changes, additions or deletions are made to the values of the data in the cluster; instead, changes are made to all rows or columns in the cluster. Thus, while the overall data is changed, the values in the fields retain their original form.

✓ Extracting Variables
✓ Extracting Records
✓ Generalization
✓ Regional Cloaking
✓ Lower and Upper Bound Coding
✓ Global Coding
✓ Sampling

6.1.2. Forms of anonymization that provide value irregularity

Unlike the above-mentioned methods, the value-distortion methods distort the values of the dataset by changing the existing values.

✓ Micro Joining
✓ Data Exchange
✓ Noise Addition

6.1.3 Statistical methods to strengthen anonymization

In anonymized datasets, as a result of the combination of some values in the records with singular scenarios, the possibility of identifying the identity of the people in the records or deriving assumptions about their personal data may arise. For this reason, anonymity can be strengthened by minimizing the uniqueness of the records in the dataset by using various statistical methods in anonymized datasets.

✓ K-Anonymity
✓ L-Diversity
✓ T-Closeness

7. STORAGE AND DISPOSAL

7.1. Storage and Destruction Period Table

Data Category	Data Retention Period
1-Identity Personal Data	101 Years
2-Communication Personal Data	101 Years
4-Personnel Personal Data	101 Years
5-Legal Action Personal Data	10 Years
6-Customer Transaction Personal Data	101 Years
7-Physical Space Security Personal Data	2 Years
8-Transaction Security Personal Data	2 Years

Data Category	Data Retention Period
9-Risk Management Personal Data	10 Years
10-Finance Personal Data	101 Years
11-Vocational Experience Personal Data	101 Years
13-Visual and Audio Recordings Personal Data	101 Years
14-Race and Ethnicity Sensitive Personal Data	101 Years
16-Philosophical Beliefs, Religions, Sects and Other Beliefs Sensitive Personal Data	101 Years
20-Union Membership Sensitive Personal Data	101 Years
21-Health Information Sensitive Personal Data	101 Years

Data Category	Data Retention Period
23- Criminal Conviction and Security Measures Sensitive Personal Data	101 Years
24-Biometric Data Sensitive Personal Data	It is retained for the duration of the employment relationship.
26-Other Information-Military Status Personal Data	101 Years
26-Other Information-Vocational Information Personal Data	101 Years
26-Other Information-Education Information Personal Data	101 Years

7.2 Periodic Disposal

In the event that all of the conditions for processing personal data specified in the Law disappear; The Company
deletes, destroys or anonymizes the personal data whose processing conditions have disappeared through a process specified in this Personal Data Storage and Destruction Policy and to be carried out ex officio at recurring intervals.

8. DETERMINATION OF PERSONAL DATA TO BE DESTROYED

8.1. Situations Requiring Periodic Destruction

The destruction of personal data in the Company is carried out within the periods specified in the Personal Data Inventory and is carried out in periods of 6 (six) months at the latest. In the event that any of the circumstances that eliminate the conditions for processing personal data occur, the destruction process is carried out in the next destruction period for the records related to this personal data.

The Data Controller determines the personal data to be destroyed through the Personal Data Inventory and notifies the KVK Committee department representatives. The department representative determines the printed and electronic records to be destroyed.

8.2. Cases Requiring Destruction on Demand

In the applications made by the relevant person using his/her right arising from the Law or according to the request of the Personal Data Protection Authority, the destruction process is carried out within 30 days after the request is received by the Company and a response is sent to the relevant person.
For the destruction requests received through the Personal Data Request Management Process, the Data Controller examines the records to be destroyed with the relevant working group to be formed from the KVK Committee department representatives and determines the records to be destroyed within 10 (ten) days at the latest from the date of receipt of the request to the Company.

8.3. Determination of Destruction Method

In the Personal Data Inventory, according to the type, criticality and sensitivity of the environment in which the personal data to be destroyed is located, the type of destruction is decided according to the destruction methods specified in the Personal Data Protection Law. If destruction is to be carried out, the physical wastes generated after the process are disposed of in a safe and irreversible manner.

Deletion	Destruction	Anonymization
Deleted	Shredding	Anonymized
Formatting	Cremated	-
By overwriting	-	-
With magnetic field	-	-

Types of Physical Destruction	Types of Digital Destruction
Shredding	Formatting
Cremated	Anonymized
By writing on it	By writing on it
With magnetic field	Deleted

The method of destruction according to environments is exemplified below;

Environment Containing Personal Data	Destruction Type	Destruction Method
Paper	Physical Destruction	Disintegrating
CD, DVD, Floppy disk, etc.	Physical Destruction	Disintegrating
Carrier Memory, SD Card (USB)	Digital Destruction	Formatting
Database	Digital Destruction	Anonymized, Deleted
External/Internal Disk	Digital Destruction	Formatted, Fragmented
Electronic Correspondence (E-mail etc.)	Digital Destruction	Deleted

8.4. Implementation of Destruction

Personal data to be destroyed,

✓ Identified records,

✓ Teams

✓ Calendar and

✓ The method is carried out taking into account.

The Data Controller also notifies the data processing parties of the personal data to be destroyed and ensures

the destruction of the personal data in the records of the relevant parties.

8.5. Ensuring that all of the detected Personal Data is Destroyed

Data Controller; It checks that all personal data is destroyed by the PDP Committee within the planned time interval and with the records determined. After the destruction of personal data is realized, the Destruction

Team fills out the Data Destruction Form and obtains the approval of the Data Controller. This form is kept by the Data Controller for at least 10 (ten) years without prejudice to other legal obligations.

Revision No	Revision Date	Revision Content	Making the Change
0	5.11.2020	First Publication	Fatih Tosun
1	27.06.2022	The information in the document was tabulated to make it easier to understand.	Fatih Tosun