ARKAS HOLDING A.S.
PERSONAL DATA RETENTION AND DESTRUCTION POLICY
6.11.2019 / Version No: 1

TABLE OF CONTENTS

1. **Purpose**
2. **Definitions**
3. **Scope**
4. **Reasons for Personal Data Retention and Destruction**
5. **Recording Media**
6. **Retention and Destruction Periods, Periodic Destruction**
7. **Destruction**
8. **Technical and Administrative Measures Taken for the Retention and Processing of Personal Data**
9. **Application**
10. **Storing the Policy**
11. **Policy Breach and Breach Inspection**

ANNEX-A / Table of Data Retention and Destruction Periods
ANNEX-B / Table of Persons Involved in Data Retention and Destruction Processes

ARKAS HOLDING A.S.
PERSONAL DATA RETENTION AND DESTRUCTION POLICY
6.11.2019 / Version No: 1

1. Purpose

1.1. This Personal Data Retention and Destruction Policy (Policy) is prepared in accordance with the personal data processing inventory of the data controller (Company) within the framework of Article 5 of the "Regulation on Erasure, Disposal or Anonymization of Personal Data".

1.2. This Policy sets out the principles for the Company's personal data retention and destruction in order to ensure compliance with the Law and secondary legislation which the Company is subject to.

1.3. This Policy has been prepared to determine the procedures and principles about what needs to be done concerning the personal data retention and destruction activities carried out by the Company.

1.4. This Policy complies with the following principles set out in the Personal Data Protection Law (Law) no. 6698. Principles of processing personal data:

- Lawfulness and fairness
- Being accurate and kept up to date when necessary
- Being processed for specified, explicit and legitimate purposes
- Being relevant, limited and proportionate to the purposes for which they are processed
- Being stored for the period laid down by relevant legislation or the period required for the purpose for which the personal data are processed.

1.5. This Policy applies to all physical and electronic documents/environments, including originals and copies, issued within the framework of the Company's activities.

1.6. Applicable legislation may require the Company to keep certain records for certain periods. Failure to comply with these retention periods may expose the Company to penalties and sanctions, prevent the enforcement of justice, cause legal evidence to lose its evidence property and/or significantly damage the Company's position in legal proceedings. Therefore, the Policy;

1.6.1. Includes an "ANNEX-A / Table of Data Retention and Destruction Periods " prepared within the scope of the applicable legislation and specifying the processes and specific retention periods.

1.6.2. Additionally, an "ANNEX-B / Table of Persons Involved in Data Retention and Destruction Processes" that defines which persons/departments are relevant and responsible within the Company for data retention and destruction processes and that specifies the duties of these persons/departments, is included in the Policy.

1.7. Company employees are obliged to fully understand and implement this Policy.

2. Definitions

The terms listed below have the definitions stated herein unless they are proper nouns or defined differently elsewhere within this policy:

Explicit Consent	Freely given, specific and informed consent.
Recipient Group	Category of natural or legal persons to which the personal data are transferred by the Data Controller.
Active Records	Records that are in use for the administration, management and operations of the Company.
Inactive Records	Records that are currently not in-use but are in retention period as they might be processed later.
Anonymization	Making personal data impossible to be associated with any identified or identifiable natural person in any way even when the personal data is paired with other data.
Employee	Natural persons employed by the Data Controller.
Demagnetization	Exposing magnetic media to a very high magnetic field through a special device and the destruction of the data by making them unreadable.
Electronic Environment	Environment that requires minimum human intervention and that uses logical or arithmetic processes to make operations such as changing, deleting, recovering or transferring the data automatically or partially automatically.
Non-Electronic Environment	Environment connected to a data recording system that needs to be operated manually but that makes access and interpretation easier.
Physical disposal (*For Electronic Data*)	Disposal of optical and magnetic media by physical means such as melting, burning, or pulverizing.
Service Providers	Natural and legal entities engaged in commercial activities to sell products or services to the Data Controller as well as the real and legal entities that are intermediaries for providing these services.
Two-stage Authentication	Two stage authentication system that uses the combination of the username and password of the person as well as an external authentication system (mobile phone, personal question, cryptographic key, etc.).
Secondary Legislation	Any regulation, circular, communiqué, policy decision or any similar administrative decision or general opinion issued or taken by the Personal Data Protection Board pursuant to the Law.

Data Subject	Natural person whose personal data are being processed.
Related Users	Any persons, except for the persons or units responsible for the technical storage, protection, and backup of the data, who works and process personal data as part of Data Controller's organization or who process data by the power given by the Data Controller.
Disposal	Any or all of the erasure, destruction and/or anonymization processes.
The Law	Personal Data Protection Law No. 6698.
Dimming/Masking	Crossing out, painting, icing, starring, etc. of all the personal data so that they cannot be associated with any identified or identifiable natural person.
Recording Media	All kinds of environments in which personal data are obtained by fully or partially automated means so long as being part of any data recording system and processed by non-automated means
Personal Data	Any information related to an identified or identifiable natural person.
Registered Electronic Mail (REM)	Electronic mail address which provides legal evidence regarding the use of electronic messages, including their transmission and delivery.
Personal Data Processing Inventory	Personal data processing activities of the Data Controller in accordance with the business processes; the inventory created by associating the personal data with the purposes of processing, the legal reasons, the category of data, the group of recipients transferred and the group of data subject, detailing the retention periods required for the purposes for which the personal data are processed, the personal data envisaged to be transferred to foreign countries and the measures taken regarding data security.
Board	Personal Data Protection Board.
Authority	Personal Data Protection Authority.
PDP Advisory Group	Employees of the company that execute the Law compliance project and provide consultancy services after the completion of the

	compliance project within the company.
Special Categories of Personal Data	Personal data relating to the race, ethnic origin, political opinion, philosophical belief, religion, religious sect or other belief, appearance, membership to associations, foundations or trade-unions, data concerning health, sexual life, criminal convictions and security measures, and the biometric and genetic data.
Periodic Disposal	Process of erasing, disposing of or anonymizing the personal data stored in the Personal Data Retention and Destruction Policy when the requirements regarding the retention of the personal data in the Law are cease to be applicable.
Policy	Personal Data Retention and Destruction Policy.
Table of data retention and destruction periods	"Table of Data Retention and Destruction Periods" in Annex A.
SFTP	A file transfer protocol that transfers files by using the cryptographic network protocol SSH.
Erasure	Making personal data inaccessible and unavailable to all the related users in any way.
The Company	Refers to the Data Controller.
Overwriting	Interception of old data recovery by writing arbitrary data consisting of 0 and 1 at least seven times on magnetic media and rewritable optical media.
VERBİS	Data Controllers' Registry (VERBİS) is an information system where data controllers are obliged to register and declare information about data processing activities.
Data Processor	Means the natural or legal person who processes personal data on behalf of the data controller upon its authorization.
Data Recording System	It refers to the recording system where personal data is processed according to certain criteria.
Data Controller	Means 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 filing system.
Data Controllers' Contact Person (DCCP)	It refers to the natural person assigned and notified during registry by the data inventory responsible for natural and legal entities established in Türkiye and by the data controller's representative for real and legal entities not established in Türkiye in order to ensure communication with the Authority in relation to the obligations under the Law and secondary regulations to be issued based on this Law.
Data Inventory Responsible	Refers to the employee appointed by the Data Controller that creates the personal data inventory of the Company in accordance with the Law, keeps it up to date and communicates the necessary changes to the Data Controllers' Contact Person.
Disposal	Means the process of making personal data inaccessible, irrecoverable and unavailable to anyone.
Regulation	Refers to the Regulation on Erasure, Disposal or Anonymization of Personal Data that was published in the Official Gazette on October 28, 2017 and entered into force on January 1, 2018.

Definitions not included herein shall be used as defined in the Law and regulations.

3. Scope

3.1. This Policy applies to the entire Company and regulates the necessary obligations. Personal data relating to all natural persons whose personal data are processed by the Company are within the scope of this Policy. This Policy shall apply to all recording environments in which personal data owned or managed by the Company are processed and to all data processing activities.

3.2. When the Company processes personal data as the Data Controller, it complies with the regulations stated in this Policy.

3.3. In the event that the Company processes personal data on behalf of another Data Processor, the Company shall comply with the regulations stated in this Policy and, if applicable, also with the regulations on all kinds of contracts executed with such third party, provided that they not contradictory to the Policy.

3.4. The relevant department manager, Data Controllers' Contact Person, and Data Inventory Responsible are responsible for the implementation of the Policy and ensuring compliance with the Policy.

4. Reasons for Personal Data Retention and Destruction

4.1. According to:

- Tax Procedural Law No. 213,
- Enforcement and Bankruptcy Law No. 2004,
- Labour Law no. 4857
- Turkish Criminal Code No. 5237,
- Social Security Council Law no. 5510,
- Law No. 5651 on the Regulation of Broadcasts on the Internet and the Fight Against Crimes Through These Broadcasts,
- Turkish Commercial Code No. 6201
- Code of Obligations no. 6098
- Occupational Health and Safety Law no. 6331,
- The Personal Data Protection Law no. 6698, other legislative provisions published as per and not limited to the relevant regulations,

And for the reasons stated below:

- During the inspections conducted by the Ministry of Labour and SSI Inspectors,
- For statistical studies,
- Also for submitting in court and expert reviews,
- Upon request by local law enforcement forces and organized industrial directorates,

Our company can obtain, process store and when necessary dispose personal data.

4.2. Processing purposes that require the storage of personal data are; executing human resources processes, conducting communication activities, ensuring the company's security, conducting statistical studies, performing works and processes arising from signed contracts and protocols, fulfilling legal obligations as required or obliged by legal regulations, contacting natural/legal persons that are in business relationship with the company, ensuring the execution of occupational health and safety processes, executing information systems processes, keeping visitor, camera and meeting records, processing customer data, managing procurement processes, carrying out accounting and finance processes, following up travel processes, processing mail, cargo and shipment records.

5. Recording Media

5.1. Physical Records

5.1.1. It consists of physical recording systems such as written records, printed media and manual data (survey forms, visitor log book), physical records, and records on paper, photos, and contracts, such as paper, microfiches and similar media.

5.1.2. Active records and records that need to be accessed easily may be stored in the Company's office environment.

5.1.3. Inactive records are sent to the Company's archives.

5.2. Electronical Records

5.2.1. Personal data present in many environments, including audio recordings, photographs,

videos, and visual and audio environments, may be stored in secure electronic environments in an accurate and up to date manner accessible by the persons who are required to process the personal data and the unauthorized access to those environments and processing of the data by third parties must be prevented. Examples of electronic environments;

- Servers (Domain, backup, email, database, web, file sharing, etc.),
- Software (office software, portal, etc.),
- Information security devices (firewall, attack detection, blocking, log file, anti-virus, etc.),
- Backup cartridges,
- Personal computers (Desktop, Laptop),
- Mobile devices (phone, tablet, etc.),
- Optical discs (CD, DVD, etc.),
- Removable memory (USB, memory card, etc.),
- Other electronic data recording environments such as a printer, scanner, copier, etc.

5.2.2. Adequate protection measures should be taken, processes should be created and implemented by the Company to ensure that electronic records are protected against loss, alteration, unauthorized disposal, unauthorized access in storage processes, and to ensure that they are complete, accurate and legible.

6. Retention and Destruction Periods, Periodic Destruction

6.1. ANNEX-A provides retention and destruction periods as well as the required specific processes. ANNEX-B provides information as to the responsible parties in those processes and the duties of these persons/departments.

6.2. In the context of this Policy, the retention calendar begins at the end of the calendar year in which the listing was created. All records that have expired are disposed of twice a year. The first periodic disposal shall be carried out at the end of the calendar year and the second shall be carried out at the end of June each year and the period between the Periodic Destructions shall not exceed six months in any case. Once the personal data processing period ceases, the related data shall be disposed of within the closest destruction period. (For example, if a record was created in March 2010 and had to be kept for seven years, the Record is to be disposed of on June 30, 2017; if that record had been created in November 2010, it would have to be disposed of on December 31, 2017.)

7. Destruction

7.1. Records must be destructed of in the following cases.

7.1.1. The actions to be taken in case of the realization of any of the following conditions and when the personal data are to be disposed of are determined by the Senior Management, Data Controller’s Contact Person and Personal Data Protection Advisory Group according to the conditions of the physical event and the provisions of the Law, Regulations and Secondary Legislation .

- When the Data Subject requests the disposal of his/her personal data, provided that all the requirements for processing personal data cease to be applicable,
- When the Data Subject has withdrawn his/her explicit consent to the processing of his/her personal data,
- When the requirements and/or purposes for processing or storing personal data cease to be applicable,
- In case of amendment or invasion of the provisions of the relevant legislation constituting the basis for the processing of personal data,
- When the Authority duly requests the destruction of personal data,
- When the retention period of personal data ends, the data are disposed of.

7.1.2. If the conditions for processing personal data are still applicable, when the Data Subject requests the disposal of his/her personal data, this request may be rejected by a written justification to be prepared by the Data Controllers' Contact Person. This written justification shall be sent to the Data Subject within 30 (thirty) days from the date of notification of the request. If all the requirements for processing personal data have ceased to be applicable, the Personal Data subject to the request shall be disposed of. In this context, the request of the Data Subject shall be concluded within at the latest 30 (thirty) days as of the date of notification and the Data Subject shall be informed.

7.1.3. The Company selects the appropriate method of disposal by consulting to the Data Controllers' Contact Person and the Personal Data Protection Advisory Group. If requested by the data subject, the company explains the reason for choosing the appropriate method. The explanation of this reason shall be made by the Data Controllers' Contact Person and shall be communicated to the Data Subject at his/her request in accordance with the Law, Regulation, and secondary legislation.

7.1.4. If all the requirements for processing Personal Data have ceased to be applicable and the personal data subject to the request has been transferred to the third party, this situation shall be notified to the third party and the necessary procedures regarding disposal shall be followed up as per the Regulation before the third party.

7.2. Disposal of Records is done by making personal data inaccessible, irrecoverable and unavailable to anyone. In order to destroy personal data, it is necessary to identify all copies of the data and to ensure that the data cannot be accessed, recovered and reused in any way. The disposal of personal data shall be carried out by the Company upon receipt of the disposal decision signed by the Data Controllers' Contact Person. The Data Controllers' Contact Person informs the persons responsible for the disposal activity as to the reason for their disposal.

7.2.1. Electronic Records;

- Electronic records can also be disposed of by de-magnetization, physical disposal and overwriting.
- Storage environments within network devices (switch, router, etc.) are fixed. Products often have a delete command, but they often do not have an automatic command to destroy data. Data are disposed of by using one or more methods such as de-magnetization, physical disposal, overwriting.

- In flash-based hard drives with ATA (SATA, PATA, etc.), SCSI (SCSI Express etc.) interfaces that contain personal data, the data are disposed of by using the disposal command if supported, or, if not supported, by using one or more of the manufacturer's recommended disposal methods or de-magnetization, physical disposal and overwriting methods.
- Fixed memory areas on portable smartphones have delete commands, but most do not have disposal commands. By using one or more methods of de-magnetization, physical disposal, overwriting, data are disposed of.
- Personal data in data storage environments such as CD's and DVD's are disposed by physical disposal methods such as incineration, fragmentation and melting.
- For items with removable recording media such as the printer, fingerprint locked entrance system etc. that contain personal data, the appropriate disposal method is selected according to the nature of the item after verifying that all recording media has been removed.

7.2.2. *Physical logs* are disposed of by paper disposal or clipping machines in incomprehensible size (if possible by vertical and horizontal disintegration) or by other methods that make it impossible to be read (e.g. by cutting the record into small pieces that cannot be assembled, or by burning the physical log in a suitable environment, etc.).

7.2.3. For *cloud systems*; databases used for storing personal data in these systems are encrypted using cryptographic methods, and where possible, individual encryption keys are used for individual data, especially for each cloud that is serviced. Once the cloud information service relationship has ended, all copies of the encryption keys required to make personal data available are disposed of.

7.2.4. For *failed devices or devices undergone maintenance*, the process of disposing of personal data contained in these devices is carried out as follows:

- Prior to the transfer of the relevant devices to third parties such as manufacturer, dealer, service point for maintenance, repair operations, the disposal of the personal data in them is conducted by the method deemed appropriate by the Company,
- When disposal is not possible or feasible, the data storage media is removed and stored, and other failed parts are sent to third parties such as manufacturers, dealers and service points,
- Necessary measures are taken in order to prevent external maintenance staff who come in for repairing purposes from copying personal data out of the institution,

Employees may seek advice from the Data Controllers' Contact Person on how to dispose the records and the above-mentioned methods of disposal.

7.3. Erasing Process

7.3.1. Personal data is made inaccessible and unavailable to the users involved in any way. The process to be followed in the process of erasure of personal data is as follows:

- Identifying the personal data for erasure,
- Identifying the users involved for each individual data by using the access authorization and control matrix or similar system,

- Identifying the rights and methods of the users involved, such as access, retrieval, reuse, etc.,
- Ending and eliminating access, retrieval, reuse rights and methods of users involved in the personal data

7.3.2. *Personal data on the servers of applications using cloud servers (Office 365, etc.):* erasure process is performed by the system administrator by removing the access authorization of the relevant users whose required personal data storage period on the servers expires.

7.3.3. *Personal data in physical logs:* Documents with personal data, that are held in the physical environment, whose retention periods have expired shall be disposed of or rendered inaccessible and unavailable in any way by the department manager that is in charge of the document's archive.

7.3.4. *Personal data on company servers*: When the retention period of the personal data on the company servers expires, the system administrator removes the access authorization of the relevant users and deletes the process. When performing this operation, if the user is also a system administrator, the system administrator privileges of that person must be removed or another method of disposal must be performed.

7.3.5. *Personal data contained in portable media environments such as flash disk, external HDD etc.* are stored encrypted and stored in secure environments with encryption keys allowing access authority only to the system administrator.

7.3.6. *The personal data in the databases* are erased by means of database commands ("delete", etc.). If the relevant user is also a database administrator, it is necessary to remove the database administrator privileges of the data subject or to perform another method of disposal.

7.4. Anonymization

7.4.1. Anonymization means removing or changing all direct and/or indirect identifiers in a dataset, preventing the identification of that person or making the data lose the ability to be distinguishable within a group so that the data cannot be associated with a real person.

Data that cannot be associated with a specific individual as a result of these processes are considered anonymized data. In other words, the anonymized data used to be information that identified a natural person before this process was performed, but after this process, it cannot be associated with the data subject and the data's connection with the person is severed.

The purpose of anonymization is to sever the link between the data and the person it identifies. Anonymization takes place when the data obtained as a result of the implementation of anonymization methods such as grouping, masking, derivation, generalization, randomization and non-automation cannot be related to a particular person.

Some of the anonymization methods that can be applied are listed below:

7.4.2. Anonymization methods that do not cause value irregularity: In methods that do not cause value irregularity, a change or addition or subtraction is not applied to each of the values of data in the cluster, but instead changes are made to the entire rows or columns in the cluster. Thus, the data is modified globally, while the values in the fields maintain their original state. Some of the anonymization methods that do not provide value irregularity are described with the following examples:

7.4.2.1. *Variables Removal*: It is an anonymization method provided by removing one or more of the variables completely from the table. In such a case, the entire column in the table will be completely removed. This method can be used for reasons such as the variable being a high-level descriptor, the absence of a more appropriate solution, the variable being too sensitive of a data to be disclosed to the public or not serving analytical purposes. For example, removing the “religion" column completely from a table containing people's age, gender, zip code, income and religion data.

7.4.2.2. *Registry Removal:* In this method, anonymity is strengthened by removing a line containing singularity in the dataset and the possibility of producing assumptions about the dataset is reduced. Usually excluded listings are listings that have no common value with other listings and are easily guessed by those who have an idea of the dataset. For example, in a dataset containing survey results, if only one person from any sector was included in the survey, in such a case, the exclusion of only the “sector” variable from all survey results.

7.4.2.3. *Regional Concealment:* Regional concealment aims to make the dataset safer and reduce the risk of predictability. If the combination created by the values of a particular record creates a very rarely visible situation and this situation is likely to cause that person to become distinguishable in the relevant community, the value that created the exception is changed to “unknown”. For example, considering that a table indicates the disease status according to age, gender, and occupation since the record with age=3 in this table belongs to a child, it creates an exceptional situation and increases the risk of predictability and making assumptions about the child's family. For this reason, if the age digit of the said listing is changed to “unknown” by the regional concealment method, the risk of predictability for the dataset will be reduced.

7.4.2.4. *Generalization:* It is the process of converting the relevant personal data from a special value to a more general value. It is the most commonly used method when producing cumulative reports and in operations carried out over total figures. The resulting new values indicate the total values or statistics of a group that makes it impossible to access a natural person. For example, if a person with TR identification number 12345678901 purchases a product from the e-commerce platform and also purchases another related product, it can be concluded that xx% of the purchasers of the first product from the e-commerce platform also purchase the second product by using the generalization method in the anonymization process.

7.4.2.5. *Upper and Lower Limit Coding:* The upper and lower limit coding method is obtained by defining a category for a given variable and combining the values remaining in the grouping created by this category. Generally, low or high values in each variable are gathered and

advanced by making a new definition of these values. For example; instead of reflecting the annual income of the individuals in a table, by determining the lower limit as 100,000, the upper limit as 120,000; values less than and equal to 100,000 TL can be grouped as "low", values between 100,000 and 120,000 can be grouped as “medium", and values greater than 120,000 and equal values can be grouped as “high".

7.4.2.6. *Global Coding:* The global coding method is a grouping method used in datasets that do not contain numerical values or have values that cannot be numerically sorted, and it is not possible to apply upper and lower limit coding. It is usually used when certain values are cumulative and make it easier to make predictions and assumptions. All Records in the dataset are replaced by this new definition by creating a common and new group for the selected values. For example, if the number of women in a single unit in a data set is stacked in two categories in the vocational variable (for example, if the majority of women in that set are architects or engineers), a single category can be obtained from the combination of the two categories (instead of the categories “architect" and “engineer” separately, a category called "architect or engineer” can be produced).

7.4.2.7. *Sampling*: In the sampling method, instead of the entire dataset, a subset taken from the set is described or shared. This reduces the risk of generating accurate estimates of individuals because it is not known whether a person known to be included in the entire dataset is included in the sample subset disclosed or shared. Simple statistical methods are applied to determine the subset to be sampled. For example, if demographic information of people living in Istanbul province is explained or shared by anonymizing a dataset about their occupation and health status, it may be meaningful to make scans and make predictions in the relevant dataset about a person who is known to live in Istanbul. However, in the relevant dataset, only the records of the people who are registered to the population in Istanbul are left and anonymization is applied by removing the population record from the dataset of those who are registered in other provinces and the data is disclosed or shared, the malicious person accessing the data will not be able to make a reliable estimate of whether the information pertaining to the person he/she knows is in Istanbul or not because he/she will not be able to estimate whether the population record of the person he/she knows is in Istanbul.

7.4.3. Anonymization methods causing value irregularities

7.4.3.1. *Micro-Combination*: With this method, all records in the dataset are first sorted in a meaningful order and then the whole set is divided into a certain number of subsets. Then, the average value of each subset belongs to the specified variable and the value of that variable of the subset is replaced with the average value. Thus, the average value of that variable that applies to the entire dataset will not change. For example, assuming that the “25,000, 28,000, 37,000, 49,000, 56,000 and 60,000” values are in the “Income” column in a table, the first three values (25,000, 28,000, 37,000) are divided into “Group 1" and the next three values (49,000, 56,000 and 60,000) are divided into “Group 2”. Afterwards, the average of the values in Group 1 is taken ([25.000 + 28.000 + 37.000] / 3 = 30.000) and

30.000 is written on all income values for Group 1 instead of their own values. The same procedure is made for Group 2.

7.4.3.2. *Data Exchange*: The method of data exchange is the recording changes obtained by exchanging the values of a variable subset between the pairs selected from the records. This method is mainly used for variables that can be categorized and the main idea is to transform the database by changing the values of the variables between the Records pertaining to the individuals. For example; In a table showing Age, Gender, Province and Income values, the income information of the record with Age= "24", Gender= "F", Province= "Ankara" and the income information of the record with Age= "45", Gender= "M", Province= "İzmir" are exchanged with each other. Likewise, the income information of the records with Age= "35", Gender= "M", Province= "İzmir" and income information of the records with Age= "50", Gender= "M", Province= "İzmir" are exchanged with each other. Thus, although it does not reflect the reality, it will be able to give the desired statistical result.

7.4.3.3. *Noise Addition*: With this method, additions and subtractions are made to provide deteriorations to the specified extent in a selected variable. This method is mostly applied in datasets containing numerical values. Disruption is applied equally at all values. For example, if the values in the "Income" column in a table are 45,000, 15,000 and 100,000, each value can be deducted (-5,000) and reflected as 40,000, 10,000 and 95,000.

7.4.4. Anonymization Strengthening Statistical Methods

7.4.4.1. *K - Anonymity*: It has been developed to prevent the disclosure of person-specific information with specific fields in a dataset, allowing the identification of more than one person, showing unique characteristics in certain combinations. If there are multiple records of combinations created by combining some of the variables in a data set, the likelihood of identifying the persons corresponding to this combination is reduced.

7.4.4.2. *L-Variety*: L-Variety method formed by studies conducted on the deficiencies of K-anonymity takes into account the variety created by sensitive variables corresponding to the same variable combinations.

7.4.4.3. *T-Proximity:* Although the L-variety method provides variety in personal data, there are situations where the said method does not provide adequate protection because it is not interested in the content and degree of sensitivity of personal data. As such, the process of calculating the degree of sensitivity of personal data within the values and anonymizing the data set according to these sensitivity levels is called the T-proximity method.

7.5. Physical and Unowned Documents Containing Personal Data

If the owners of the physical documents that are left/forgotten on the desktops, printers and in various locations within the offices cannot be found, the employee who first notices the document must dispose of the said document in accordance with the principles of disposal of the physical logs contained in Article 6.2 of this policy.

8. Technical and Administrative Measures Taken for the Retention and Processing of Personal Data

In order to ensure the proper retention and security of Personal Data, the Company shall take physical, technical and administrative measures to prevent unauthorized alteration, possible loss, unauthorized processing or access, risks and similar damages arising from exposure to human action or natural or physical environment, by taking into account the nature and condition of personal data. In addition to these;

8.1. Necessary measures are taken by revealing the risks, threats, weaknesses and, if any, vulnerabilities for the Company's information systems with data leakage tests (pen tests).

8.2. Risks and threats that will affect the continuity of information systems are monitored as a result of real-time analyses conducted with the information security incident management.

8.3. Access to information systems and authorization of users are carried out through security policies through access and authorization matrix and corporate active directory.

8.4. Necessary measures are taken for the physical security of the company's information systems equipment, software, and data.

8.5. In order to ensure the security of information systems against environmental threats, measures are taken regarding hardware (access control system that allows only authorized personnel to enter the system room, 24/7 operating monitoring system, ensuring the physical security of the edge switches forming the local area network, fire extinguishing system, air conditioning system, etc.) and software (firewalls, attack prevention systems, network access control, systems preventing harmful software, etc.).

8.6. Risks are determined to prevent the unlawful processing of personal data; appropriate technical measures are taken for these risks and technical controls are carried out for the measures taken.

8.7. Within the company, access procedures are established and reporting and analysis activities related to the accessing of the personal data are carried out.

8.8. Access to personal data storage areas is recorded and inappropriate access or access attempts are kept under control.

8.9. The Company takes the necessary measures to make erased personal data inaccessible and unavailable to the related users.

8.10. For situations when the personal data is obtained illegally by others, an appropriate method has been established by the Authority to notify the data subject and the Board regarding this situation.

8.11. Appropriate security patches are installed by following security vulnerabilities and information systems are kept up to date.

8.12. Strong passwords are used in electronic environments where personal data are processed.

8.13. Secure recording (logging) systems are used in electronic environments where personal data are processed.

8.14. Data backup programs that ensure the safe retention of personal data are used.

8.15. Access to personal data stored in electronic or non-electronic environments is restricted according to access principles.

8.16. A separate policy has been determined for the security of special categories of personal data.

8.17. Training has been given on data security of special categories of personal data for employees involved in sensitive personal data processing processes, confidentiality agreements have been made and the authorizations of the users with access to the data have been defined.

8.18. Electronic environments where special categories of personal data are processed, stored and/or accessed are protected using cryptographic methods, cryptographic keys are kept in secure environments, all transaction records are logged, security updates of the environments are continuously monitored, necessary safety tests are performed/made regularly, and test results are recorded.

8.19. Security measures are taken for physical environments where special categories of personal data are processed, stored and/or accessed, unauthorized entry and exit are prevented.

8.20. Special categories of personal data are transferred in encrypted form via the corporate e-mail address or REM account if they are required to be transferred via e-mail. If transfer via media such as flash memory, CD, DVD is required, the data are encrypted by cryptographic methods and the cryptographic key is kept in different media. If the transfer is performed between servers in different physical environments, data transfer is performed by installing a VPN between servers or by the SFTP method. If it is necessary to transfer the document via paper format, necessary measures are taken against risks such as theft, disappearance or unauthorized persons and the document is sent in a “confidential" format.

8.21. As a minimum, security measures are taken in accordance with the Company's policies and in accordance with the practices in the field which the Company operates in.

8.22. All employees are obliged to ensure that all Personal Data they process are kept securely. Personal data may not be shared, disclosed orally, in writing or otherwise to any unauthorized third party, whether by accident or otherwise.

8.23. If employees share Personal Data in an unauthorized way and act contrary to the requirements of this Policy, this situation should be immediately notified to the Data Controllers' Contact Person. This situation may generally require a disciplinary penalty and/or may result in the termination of the employment contract with a justified reason in accordance with Article 25 of the Labour Law of the employee.

8.24. Physical copies containing Personal Data should be kept in locked cabinets or locked drawers; for electronic copies security criteria in "Information Systems General Standards and Security Policy". should be applied.

8.25. Personal Data, whether electronic or physical, may not be kept at the personnel's home, laptops, or other personal portable devices, or at other sites outside the workplace.

8.26. Employees must comply with all the safety criteria in the "Information Systems General Standards and Security Policy" in rare circumstances when it is approved by the company management that it is necessary or appropriate to keep Personal Data out of the workplace, even though , under normal circumstances, the data is not allowed to be kept in the personnel's home, laptops or other personal portable devices or other remote locations.

8.27. The employee who manages the said equipment is responsible for the data stored in portable electronic devices or erasable environments. This person is also obliged to provide the following elements:

8.27.1. To have backups of these data stored in environments where adequate security measures are taken against the likelihood of damage to the data contained in the relevant devices and environments,

8.27.2. Special categories of personal data and other sensitive data are appropriately encrypted,

8.27.3. That Special categories of personal data or other sensitive data have not been copied to portable storage devices without consulting the Data Controllers' Contact Person or Data Inventory Responsible and that the relevant encryption and protection measures have been taken in this context, and

8.27.4. Failure to leave laptops, mobile devices and computer-based recording media (such as USB devices, CDs) containing special categories of personal data and other sensitive data unattended in the office.

8.27.5. Employees may not copy and/or download documents containing personal data stored on secure Company programs to the computer they use unless necessary, and if they download and/or copy them when the purpose of processing is over, they immediately delete the said electronic copy after making sure that the document they arrange is saved to the company servers and/or relevant programs if it is to be used by the company.

9. Application

9.1. Publishing: This Policy will be provided to the employees by the Data Controller.

9.2. Effective Date: This Policy shall enter into force on release.

9.3. Amendments: Prior to any changes to this Policy, the Data Controllers' Contact Person or Data Inventory Responsible may request the changes to be applied from the Data Controller. Policy changes are made by the Data Controller.

10. Storing the Policy

The Data Controller is responsible for publishing and storing this Policy. Each department manager is responsible for the implementation of this Policy. Questions related to the implementation of this Policy should be directed to the Data Controller's Contact Person and the Data Inventory Responsible.

11. Policy Breach and Breach Inspection

11.1.1. If an employee is unable to comply with this Policy, an inspection is conducted by the department manager to determine the following. If deemed necessary, appropriate regulatory measures are taken to reduce the risk of breach by evaluating the impact of the Policy on the Company. Considering the severity of the breach, it is determined whether the employee will be subject to a disciplinary sanction (including the possibility of dismissal) included in the "Disciplinary Regulations".

11.1.2. If it is decided that the actions following the breach are appropriate, the department manager contacts the Data Controllers' Contact Person, the Upper Management and the Human Resources Directorate and takes action to implement the necessary actions.

ANNEX-A / Table Of Data Retention and Destruction Periods

PROCESS	RETENTION PERIOD	DESTRUCTION PERIOD
Conducting Occupational Health / Work Safety Activities	10 years after the termination of the business relationship	On the first periodic destruction period following the end of the retention period
Conducting Contract Processes	10 years after the termination of the business relationship	On the first periodic destruction period following the end of the retention period
Conducting Communication Activities	10 years after the termination of the business relationship	On the first periodic destruction period following the end of the retention period
Conducting Human Resources Processes	15 years after the termination of the business relationship	On the first periodic destruction period following the end of the retention period
Conducting Recruitment Processes	1 year after the end of the application process	On the first periodic destruction period following the end of the retention period
Cyber Security Incident Management	5 years after being recorded	On the first periodic destruction period following the end of the retention period
Conducting Hardware and Software Access Processes	2 years after being recorded	On the first periodic destruction period following the end of the retention period
Registration of Visitors and Meeting Participants	2 years after the end of the event	On the first periodic destruction period following the end of the retention period
Camera Records	1 year after being recorded	On the first periodic destruction period following the end of the retention period
Customer Data	10 years after the termination of the business relationship	On the first periodic destruction period following the end of the retention period
Conducting Procurement Processes	10 years after the termination of the business relationship	On the first periodic destruction period following the end of the retention period
Execution of Accounting and Finance Processes	15 years after being recorded	On the first periodic destruction period following the end of the retention period
Procedures of General Assembly and Board of Directors	10 years after being recorded	On the first periodic destruction period following the end of the retention period
Execution of Official and Legal Procedures	20 years from the termination of a legal relationship	On the first periodic destruction period following the end of the retention period
Travel Processes	1 year from the end of the trip	On the first periodic destruction period following the end of the retention period
Mail, Cargo, Shipping Records	5 years after being recorded	On the first periodic destruction period following the end of the retention period

ANNEX-B / Table of persons involved in data retention and destruction processes

All employees of the Company are liable for actively supporting the persons responsible for the implementation of the Policy and for taking the technical and administrative measures contained in this Policy.

TITLE	**DEPARTMENT**	**DUTY**
General Manager	Management	Responsible for employees to act in accordance with the policy.
PDP Advisory Group	Risk Management, Human Resources, Information Technologies, Corporate Strategies	Responsible for preparing, developing, executing, updating and publishing the Policy in relevant platforms
Data Controllers' Contact Person (DCCP)	-	He/she is responsible for the execution of the policy on behalf of the data controller.
Information Technologies Director	Information Technologies Security	Responsible for providing the technical solutions needed in the implementation of the Policy and informing the management to provide the necessary investments, executing the erasure, disposal and anonymization processes in electronic recording environments and conducting related internal audits.
Director of Human Resources	Human Resources, Administrative Affairs, Security	Responsible for the execution of the policy in accordance with his/her duties and supervising other departments' officers and employees such as Archive, Security.