Policy on Protection, Storage and Destruction of Personal Data

Contents

1. Scope and Purpose of Policy on Protection, Storage and Destruction of Personal Data

As ALİ RIZA YILMAZ İNŞAAT VE TİCARET ANONİM ŞİRKETİ (hereinafter referred to as "COMPANY" registered at the Istanbul Trade Registry Office with the registry number 167899 and residing at Imrahor Cad.No.82 Beyoglu/Istanbul, we attach great importance to ensuring the confidentiality and security of personal data of natural persons in accordance with the Law No:6698 on Protection of Personal Data.

In accordance with this Policy on Storage and Destruction of Personal Data (hereinafter referred to as "Policy"), Law No.6698 on Personal Data Protection ("PDP" or "Law") and Regulations on Deletion, Destruction or Anonymization of Personal Data (hereinafter referred to as "Regulation"), which entered into force after being published in the Official Gazette on 28 October 2017 and which constitutes the secondary regulation of the Law; the Policy hereby has been drafted for the following purposes;

- To fulfill our obligations
- Methods and legal reasons for collecting personal data,
- The personal data of which groups of people are processed (Data subject Categorization),
- In which category the personal data of data subjects are processed (Data Categories) and sample data types,
- For what purposes the relevant personal data are used,
- Technical and administrative measures taken to ensure the security of personal data,
- To whom and for what purposes personal data can be transferred,
- Personal data sharing with public institutions and organizations and official authorities,
- Storage periods and destruction processes of personal data,
- This Policy was prepared by the COMPANY as a data controller in order to inform the data subjects about the deletion, destruction and anonymization processes, as well as the principles of determining the maximum storage period required for the purpose of processing your personal data.

This Policy sets the rules and policies to be applied by the COMPANY for employees, employee candidates, interns, references of the employee candidates, people to be contacted in case of emergency, tenants, customers, potential customers, suppliers, customers who receive accommodation services and persons given power of attorney regarding the processing of personal data and the rights of the data subject.

This Policy on Protection, Storage and Destruction of Personal Data, which has been issued in accordance with the Law is made available to natural persons (hereinafter referred to as "data subject") whose personal data are processed.

2. Definitions:

Explicit Consent: Consent about a specific subject based on information and expressed in free will.

Recipient group: The category of natural or legal persons to whom personal data is transferred by the data controller,

Relevant user: Any person who processes personal data in accordance with the authority and order received within the data controller institution or from the data controller, except the person or unit responsible for the technical storage, protection and backup of the data,

Destruction: Deletion, destruction or anonymization of personal data,

Law: Law No. 6698 on Protection of Personal Data dated 24/3/2016 ,

Recording Medium: Any media in which the personal data that is wholly or partially automatic or acquired by non-automatic means provided that it is a part of any data recording system are located,

Personal Information: Any information related to the identified or identifiable real persons,

Processing of Personal Data: All kinds of processes performed on personal data including obtaining, recording, storing, keeping, changing, re-arranging, disclosure, transmission, acquisition, making available, classification or prevention of use in whole or in part, automatically or in non-automatic ways, being part of any data recording system,

Anonymization of personal data: Anonymization of personal data implies that personal data cannot be associated with any particular or identifiable real person in any way even when the personal data is paired with other data,

Deletion of personal data: Deletion of personal data means making personal data inaccessible and unavailable in any way for Relevant Users,

Destruction of Personal Data: Process of making personal data inaccessible, recoverable and unusable by anyone,

Board: Personal Data Protection Board,

Sensitive personal data: Information about security measures with biometric and genetic data of people with respect to race, ethnicity, political thought, philosophical belief, religion, sect or other beliefs, appearance and clothing, membership to an association, foundation or trade union, medical condition, sexual life, criminal conviction.

Registry: The data controllers registry kept by the Personal Data Protection Authority,

Periodic destruction: The deletion, destruction or anonymization process to be carried out ex officio at recurring intervals specified in the personal data storage and disposal policy in case all the conditions for processing personal data included in the law are eliminated,

Data subject/Contact person: The real person whose personal data is processed,

Data Recording System: Recording system in which personal data is processed by organizing according to certain criteria,

Data controller: It refers to real or legal person responsible for identifying the purposes and means of personal data processing and installing and managing data recording system,

Regulation: Regulation on the Deletion, Destruction or Anonymization of Personal Data published in the Official Gazette on October 28, 2017.

3. Data Subject Categorization

The COMPANY groups the data subjects whose personal data is processed as follows, and these groups of individuals may be expanded in the light of the process and legal reasons specified in this policy.

i. Customers
ii. Potential Customers
iii. Suppliers
iv. Lessees
v. Accommodation Service Customers
vi. Employees
vii. Interns

viii. Employee Candidates

ix. References to Employee Candidate

x. Third Persons Given Power of Attorney

xi. Contact Information in Emergency Situations

a. Data Categories and Sample Data Types

No	Data Subject	Data Category	Data Types
1.	**Customer**	**Id Info**	Name-Surname, Gender, TR Identity Number, TR Identity Information (ID serial number, family order number etc.), Date of Birth, Place of Birth, Marital Status, Nationality, Religion (former ID), Passport Number, Signature
		Contact Details	Address (home/work), Email, Phone / Mobile Phone
		Financial Information (Customer Transaction)	Bank Account Information, IBAN Number, Payment Information, Check Copies
		Professional Experience	Industrial Information, Work Place and Title Information
		Visual and Audio Records	Camera Recording In Case of Coming to the Company
		Legal Procedure and Compliance Information	Tax Board, Signature Circular
2.	**Potential Customers (Business Cards)**	**Id Info**	Name & Surname
		Contact	E-mail Address
		Professional Experience	Workplace and Title
3.	**Suppliers**	**Id Info**	Name-Surname, Gender, TR Identity Number, TR Identity Information (ID serial number, family order number etc.), Date of Birth, Place of Birth, Marital Status, Nationality, Religion, Passport Number, Signature, Name and Surname of the Supplier Employee (for invoice delivery)
		Contact Details	Address, Email, Phone / Mobile Phone, Supplier Employee's Mobile Phone Number (for invoice delivery)
		Financial Information	Bank Account Information, IBAN Number, Payment Information, Check Copies
		Business Info	Industrial Information, Work Place and Title Information
		Legal Procedure and Compliance Information	Signature Circular, Tax Plate, Certificate of Activity, Trade Registry Gazette
		Visual and Audio Records	Camera Recording In Case of Coming to the Company in Person
4.	**Lessees**	**Id Info**	Name Surname, TR Identity Number, Signature
		Contact Details	Certificate of residence, address,
		Legal Action	Authorized Signatory List
		Visual and Audio Records	Camera Recording In Case of Coming to the Company in Person
5.	**Customers Receiving Accommodation Service**	**Id Info**	Full Name, TR Identity Number, Passport Number, Mother's Name, Father's Name, Gender, Date of Birth, Full Name of the Persons with whom s/he comes, Signature
		Contact Details	Mobile Phone Number, E-Mail Address, Address, Country-City Information, Zip Code,
		Finance Information	Room Fee, Payment Method, Total Amount Paid
		Customer Transaction	Credit Card Number, Credit Card Expiry Date, Security Code
		Other information	Whether to ask for Room Cleaning or Breakfast, Membership Information, License Plate Information, if available, referred room type, room number, check-in and check-out dates, flight information, departure time, number of days for accommodation, number of people to arrive
6.	**Employees**	**Id Info**	Full Name, Gender, TR Identity Number, TR Identity Information (ID serial number, family order number, etc.), Date of Birth, Place of Birth, Marital Status, Nationality, Religion, Signature, Certificate of Identity Registration (if any, of their children), Passport number
		Contact Details	Address, E-mail, Telephone/Mobile Phone, Certificate of Residence
		Financial Information	Bank Account Information, IBAN Number,
		Visual and Audio Records	Video Recording and Photo, Passport Photo, Camera Recording
		Personal Files	Curriculum Vitae, Foreign Language Knowledge, Computer Skills Information, consent of the parents if under 18, military service status information, discount letter from the Revenue Administration for those benefiting from disability discount, work permit card or photocopy for foreigners, Turkish Employment Agency document, former convict and application registration document for disabled workers, AGI form, Employment Contract, Professional Seniority
		Professional Experience Information	Journeyman's Certificate, Hygiene Certificate, Diploma Information, Foreign Language Knowledge, Certificates, Letter of Recommendation and Course Participation Certificates, If any, In-Service Training Information, Graduation Information, Vocational Qualification Certificates, information on the prior workplace, salary information, department s/he worked and Title, References
		Other information	Information on Number of Children, Performance Evaluation Results, If Provided any Training, Place/Time/Subject Information of Training, Upper Body and Lower Body Size

		Health Information	Information on any Disease that will Restrict Doing Business, Physical Disability Status, Blood Type Card, Health Check Report For Kitchen Workers,
		Legal Action Information	Letter About Employees Received From Judicial and Administrative Authorities
7.	**Interns**	**Identity Information**	Full Name, Gender, TR Identity Number, TR Identity Information (ID serial number, family order number, etc.), Date of Birth, Place of Birth, Marital Status, Nationality, Religion, Signature, Certificate of Identity Registration, Passport number
		Contact Information	Certificate of Residence, Address, E-mail, Telephone / Mobile Phone
		Health Information	Health Report, Physical Disability Status, Blood Type Card
		Visual and Audio Records	Photo/Video, Camera Recording
		Professional Experience	Hygiene Certificate, Diploma Information, Foreign Language Knowledge, Certificates, In-Service Training Information, Graduation Information, Vocational Qualification Certificates, Letter of Recommendation and Course Participation Certificates, if any, References
		Personnel Information	Curriculum Vitae, Foreign Language Knowledge, Computer Skills Information, consent of the parents if under 18, military service status information, discount letter from the Revenue Administration for those benefiting from disability discount, work permit card or photocopy for foreigners, Turkish Employment Agency document, former convict and application registration document for disabled workers,
		Other information	If Provided with any Training, Place/Time/Subject Information of Training, Upper Body and Lower Body Size
		Financial Information	Bank Account Information, IBAN Number,
8.	**Employee Candidates**	**Id Info**	Name- Surname, Date of Birth and Place of Birth, Signature
		Contact Details	Address, Phone, Email Address
		Personal Files	Resume Information, Military Status Information
		Professional Experience Information	Diploma Information, Foreign Language Knowledge, Certificates, Information on Courses Participated, In-Service Training Information, Graduation Information, Previous Work Experience, Computer Program Information, Computer Programs Information, Department of Application
		Visual Records	Camera Recording In Case of Coming to the Company in Person
		Other information	Salary Expectation
9.	**Reference to an Employee Candidate / Employee / Intern**	**ID**	Name & Surname
		Contact	Work Place, Title, Phone Number
		Visual Recording	Camera Recording In Case of Coming to the Company in Person
10.	**Third Persons Given Power of Attorney**	**Identity Information**	Name-Surname, Gender, TR Identity Number, TR Identity Information (ID serial number, family order number etc.), Date of Birth, Place of Birth, Marital Status, Nationality, Religion, Passport Number, Sample Signature
		Contact Details	Address, Phone, Email Address
		Professional Experience Information	Industrial Information, Work Place and Title Information
		Visual Records	Camera Recording In Case of Coming to the Company in Person
11.	**Contact Information in Emergency Situations**	**Identity Information**	Full Name
		Contact Information	Phone Number, Address

4. Explanations Regarding the Reasons Requiring the Storage and Destruction of Personal Data

a. Processing Purposes Requiring the Storage of Personal Data

Personal data are used by the COMPANY for the following purposes;

- Carrying out the application and placement process by evaluating the qualifications of employee candidates and interns
- Fulfillment of Obligations Arising From Employment Contracts and Legislation for Employees/Interns
- Execution of Vested Benefit and Interest Processes for Employees
- Conducting necessary activities by our respective business units and performing related business processes in order to carry out commercial activities by the Company;
- Planning and/or Execution of Business Continuity Activities
- Execution of Customer Relationship Management Processes
- Follow-up of Company Financial and Accounting Affairs
- Planning and/or Execution of External and Internal Training Activities
- Management of Relations with Business Partners and/or Suppliers
- Planning and Execution of the Sales Process of Products and/or Services
- Execution of Contract Signing Processes
- Planning and Execution of Customer Relationship Management Processes
- Planning and Execution of Market Research Activities for the Sales and Marketing of Products and Services,

- Execution of Training / Event / Organization Processes
- Planning and Execution of Marketing Processes of Products and/or Services,
- Following Legal Affairs and Fulfilling Legal Responsibilities
- Planning and Execution of the Operational Activities Required to ensure that the Company's Activities are carried out in compliance with the Company Procedures and/or Relevant Legislation
- Providing Information to Authorized Institutions Based on Legislation

b. Reasons Requiring the Destruction of Personal Data

Pursuant to the Regulation, the personal data of the data subjects are destroyed by the COMPANY, either directly or upon request, in the following cases:

a) Amendment or abolition of relevant legislative provisions that constitute the basis for the processing or storage of personal data,
b) The disappearance of the purpose that requires the processing or storage of personal data,
c) The disappearance of conditions that require the processing of personal data in Articles 5 and 6 of the Law.
d) In cases where the processing of personal data takes place only in accordance with the explicit consent condition, the relevant person's withdrawal of his/her consent,
e) Accepting the application of the relevant person regarding the deletion, destruction or anonymization of his/her personal data within the framework of the rights of Article 11 of the Law in paragraphs 2 (e) and (f) by the data controller,
f) In cases where the data controller rejects the application made by the relevant person on the request of deletion, destruction or anonymization of his/her personal data, or his response is found inadequate, or does not respond within the period stipulated by the Law; existence of complain to the Board and approval of this request by the Board,
g) Although the maximum time requiring personal data to be stored has passed, the non-existence of any conditions to justify storing personal data for longer.

5. Technical and Administrative Measures Taken To Ensure the Security of Personal Data

The COMPANY undertakes to take all necessary technical and administrative measures and show due diligence to ensure the confidentiality, integrity and security of your personal data. In this context, it takes the necessary precautions to prevent the misuse, illegal processing, unauthorized access to data, disclosure, alteration or destruction of personal data.

The COMPANY takes the following technical and administrative measures to prevent unlawful access to the personal data it processes, to prevent unlawful processing of these data and to ensure the protection of personal data:

a. Administrative Measures Taken:

Administrative measures taken for personal data;

- Awareness trainings are provided to employees.
- Written commitment on confidentiality is received from employees.
- The employees are enlightened and have them signed the Information Statement.
- The Information Statement signed by the customers is stored in their files.
- Employees are informed about the Policy on Storage and Destruction of Personal Data, and updated versions are shared via e-mail so that they are always accessible.
- Written documents are kept in lockers.
- The data in the computer environment is encrypted and access is allowed only by authorized persons.

Administrative measures taken for Sensitive Personal Data,

In addition to the administrative measures taken for Personal Data,

- Regular trainings on data security are provided to employees involved in the processing of sensitive personal data.
- Extra security measures are taken in the environments where the data is processed and stored, and only authorized persons have access them.
- The phrase "classified documents" is added to be transferred on paper.

b. Technical Measures Taken:

Technical measures taken for personal data;

- Network security and application security are ensured.
- Key management is implemented.
- Security measures are taken within the scope of supply, development and maintenance of information technology systems.
- The security of personal data stored in the cloud is ensured.
- There are disciplinary regulations that include data security provisions for employees.

- Training and awareness activities are carried out at certain intervals on data security for employees.
- Access logs are maintained regularly.
- Corporate policies on access, information security, usage, retention and disposal have been prepared and implemented.
- Letters of undertaking on confidentiality are prepared.
- The authorities of the employees who have been subject to change of duty or left jobs are revoked regarding their previous duties.
- Current anti-virus systems and firewalls are used.
- Firewalls are implemented.
- The signed contracts contain the provisions on data security.
- Necessary security precautions are taken for entering and exiting physical environments containing personal data.
- The security of environments containing personal data against external risks is ensured.
- Security of environments containing personal data is ensured.
- Personal data is reduced as much as possible.
- Log records are maintained in such a way that there is no user intervention.

Technical measures taken for sensitive personal data:

In addition to the technical measures taken,

- A separate systematic, manageable and sustainable policy and procedure are set for the security of sensitive personal data.
- Regular training is provided in topics such as the Law and related regulations and security of sensitive personal data,
- Confidentiality agreements are made.
- The authorities of the employees who have been subject to change of duty or left jobs regarding their previous duties are immediately revoked.
- It is ensured that sufficient security measures are taken according to the nature of the medium in which the Sensitive Personal Data are stored (against electricity leaks, fire, flood, theft etc.).
- Physical security of these environments is provided and unauthorized entries and exits are prevented. In case data is required to be transferred via paper media, necessary measures are taken against risks such as theft, loss of documents or unauthorized disclosure, and the documents are sent in the form of "classified documents".

6. To Whom and for What Purpose the Processed Personal Data Are Transferred

The COMPANY transfers personal data to third parties only in line with the purposes specified in this Policy on Protection, Storage and Destruction of Personal Data and in accordance with Articles 8 and 9 of the Law.

In this context, personal data transfers are carried out through secure media and channels provided by the relevant third party.

In addition to the technical measures to ensure the security of the personal data subject to the transfer mentioned above; they are also legally protected thanks to the Law-compliant provisions included in our contracts considering that the counterparty of the legal relationship is a data controller or data processor.

The COMPANY pays strict attention to process your personal data in accordance with the "need to know" and "need to use" principles, by providing the necessary data minimization and taking the necessary technical and administrative security measures. Since the execution or supervision of business activities, ensuring business continuity, and the operation of digital infrastructures require continuous data flow with different stakeholders, we have to transfer the personal data we process to third parties for the purposes specified in the Information Statements for each relevant person.

7. Recording Medium:

Personal data of data subjects are stored securely by the COMPANY in accordance with the relevant legislation, in particular the provisions of the PDP Law, in the mediums listed below:

Electronic Mediums:

DLP (the system that contains usernames and passwords where domain accounts are kept),

File server (server with common files),

DHCP (service that distributes IP to computers),

Proxy (an application that records internet access, allows or blocks access),

The application that collects the logs required to be taken according to the Law No. 5651,

Backup applications and media,

Accounting application,

Database systems (environment where application data is kept),

Terminal servers (servers that enable applications to be accessed and run),

Personal Computers (Desktop, laptop)

Printer, scanner, copier

Non-Electronic Media:

Paper

Written, printed and visual media.

8. Storage of Personal Data and Destruction Times

The following criteria are used in determining the storage and destruction periods of your personal data obtained by the COMPANY in accordance with the provisions of the Law and other relevant legislation:

a) If a period is stipulated in the legislation regarding the storage of the said personal data, this period is obeyed. Following the expiry of the stated period, action is taken regarding the data within the scope of subparagraph (b).

b) In the event that the period stipulated in the legislation regarding the storage of the relevant personal data has expired or there has been no period stipulated in the relevant legislation regarding the storage of such data;

- Personal data are classified as personal data and sensitive personal data based on the definition in Article 6 of the Law on PDP. All personal data determined to be of sensitive nature are destroyed. The method to be applied in the destruction of the relevant data is determined by the quality of the data and importance of the storage in the eye of the COMPANY.
- Compliance of data storage with the principles specified in Article 4 of the Law on PDP is sought, for example; it is questioned whether the COMPANY has a legitimate purpose in storing the data. The data that is determined to be violating the principles in Article 4 of the Law on PDP if stored is deleted or destroyed.
- It is determined the data storage which of the exceptions stipulated in Article 5 and Article 6 of the Law can be considered for the data storage. Reasonable periods are determined for data storage within the framework of the exceptions determined. Data are deleted or destroyed if the said periods expire.

9. Legal Reasons Requiring Storage

The data are kept by the COMPANY in line with the periods stipulated in the legislation within the scope of its activity, especially in the legislation stated below:

- Law on Protection of Personal Data No. 6698,
- Turkish Code of Obligations No. 6098,
- Turkish Commercial Code No 6102
- Labour Law No. 4857,
- Social Security and General Health Insurance Law No. 5510,
- Law No. 5651 on Regulating Internet Broadcasting and Combating Crimes Committed Through Internet Broadcasting,
- Occupational Health and Safety Law No. 6331,
- Law No. 2634 for the Encouragement of Tourism
- Law No.17996 on the Relations of Tourism Enterprises with the Ministry, One Another and Their Customers
- Other secondary regulations in force under these laws

Data Type	Storage Period	Destruction Times
Personal Data Regarding Customers, Suppliers and Lessees	10 years after the legal relationship ends;	In the first periodic destruction period following the expiry of the storage period
Personal Data Regarding Customers Receiving Accommodation Service	5 years from the Service Provision, and Credit Card Information for 6 months from the Service Provision	In the first periodic destruction period following the expiry of the storage period
Camera Record Taken to Ensure the Security of the Physical Space	1 month	In the first periodic destruction period following the expiry of the storage period
Personal Data of Authorized Third Persons	10 years after the legal relationship ends	In the first periodic destruction period following the expiry of the storage period
CV and Personal Information Received During Job Application	2 years	In the first periodic destruction period following the expiry of the storage period
Personal Data Received Regarding Employees	10 years from the termination of the Employment Contract	In the first periodic destruction period following the expiry of the storage period
Personal Data Received Regarding Interns	2 years from the end of the internship	In the first periodic destruction period following the expiry of the storage period

All Records Regarding Accounting and Financial Transactions	10 years	In the first periodic destruction period following the expiry of the storage period

In order to exercise your rights over your personal data; you can make necessary changes, updates and/or deletions and related requests via the "Contact Form" you can access from the COMPANY's Website, and through the COMPANY's official e-mail address **www.ramadaistanbul.com** and the official phone number **"0090 0212 631 20 20"**.

10. Methods used for legal destruction of personal data

The COMPANY has established a unit ("Technical Unit") responsible for the destruction of the personal data it processes in accordance with the law. The Technical Unit ensures the deletion of personal data in a way that they can be processed only by the relevant users, and cannot be processed for all other unrelated sections.

a. Deletion of Personal Data

Deletion of personal data is the process of making personal data inaccessible and unusable for the users concerned in no way. The data controller takes all necessary technical and administrative measures to ensure that the deleted personal data are inaccessible and unusable for the relevant users.

i. Deletion Process of Personal Data

The processes followed in deleting personal data are as follows:

- Determining personal data to be deleted
- Identifying the relevant users for each personal data using an access authorization and control matrix or a similar system
- Determining the authorizations and methods of the relevant users such as access, retrieval and reuse
- Closing and eliminating the authorization and methods of access, retrieval, reuse within the scope of personal data of the relevant users

ii. Deletion Methods of Personal Data

a) Application Type Cloud-Based Solutions

In the cloud system, data is deleted by giving a delete command. While performing the said process, it is noted that the relevant user is not authorized to retrieve deleted data on the cloud system.

b) Personal Data on Paper Media

Personal data in paper media are deleted using the blackout method. The blackout process is done by cutting the personal data on the relevant documents whenever possible, and making them invisible to the relevant users by using fixed ink, which is irreversible and cannot be read with technological solutions.

c) Office Files on the Central Server

The file is deleted with the delete command in the operating system or the access rights of the relevant user on the directory where the file or file is located are removed. While performing the aforementioned operation, it is noted that the relevant user is not the system administrator at the same time.

d) Personal Data on Portable Media

Personal data in flash-based storage media is stored encrypted and deleted using software suitable for these media.

e) Databases

The relevant lines containing personal data are deleted by database commands (DELETE etc.). While performing the said operation, it is noted that the relevant user is not a database administrator at the same time.

Personal data in paper and electronic media, whose purpose of processing is completely eliminated, is destroyed or deleted in accordance with the Guidelines on Deletion, Destruction or Anonymization of Personal Data published by the Personal Data Protection Authority. All deletion and destruction operations performed by the Technical Unit are logged and recorded electronically with a time stamp. A report regarding the performance of such operations for personal data in paper media is issued and kept by the Technical Unit. Records of deletion or destruction of personal data in electronic and paper media are kept for three years. The Company uses the method of "deleting" in a way that only the relevant departments can access these data during the retention periods of personal data. If the storage period expires and there is no other purpose that requires the storage of personal data, the Company uses the anonymization method.

b. Destruction of Personal Data

Destruction of Personal Data is the process of making personal data inaccessible, irreversible and nonerasable by anyone in no way. The Company takes all necessary technical and administrative measures regarding the destruction of personal data.

i. Methods of Destruction of Personal Data

In order to destroy personal data, all copies of the data are detected and destroyed 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

The following methods are used to destroy data on these systems.

- **Physical Destruction:** It is the physical destruction of optical media and magnetic media such as melting, burning or pulverizing. Data is made inaccessible by processes such as melting, burning, pulverizing or passing optical or magnetic media through a metal grinder. For solid hard disks, if the overwriting or de-magnetization process is not successful, this media is also physically destroyed.
- **Overwriting:** It is the process of preventing the recovery of old data by writing random data consisting of 0s and 1s at least seven times on magnetic media and rewritable optical media. This process is performed using special software.

b) Environmental Systems: The destruction methods that can be used depending on the media type are as follows:

- **Network devices (switches, routers, etc.):** The storage environments inside these devices are fixed. Products often have a delete command, but do not have a destruction feature. It is destroyed using one or more of the suitable methods specified in (a).
- **Flash-based environments:** Flash-based hard disks that have ATA (SATA, SSD, PATA, etc.), SCSI (SCSI Express, etc.) interface are deleted using the <block erase> command if supported, if not supported, using the manufacturer's recommended destruction method, or using one or more of the appropriate methods specified in item (a).
- **Mobile phones (Sim card and fixed memory areas):** There are delete commands in fixed memory areas on portable smartphones, but most do not have a destroy command. It is destroyed using one or more of the appropriate methods specified in item (a).
- **Environmental units such as printers with removable data recording media:** It is destroyed by using one or more of the appropriate methods specified in item (a), depending on their characteristics after verifying that all data recording media have been removed.
- **Environmental units such as printers whose data recording medium is fixed:** Most of the systems in question have a delete command, but no destroy command. It is destroyed using one or more of the appropriate methods specified in item (a).

c) Paper Media

The main medium is destroyed, as the personal data in these media is permanently and physically written on the media. While this process is being carried out, the media is divided into small pieces in an incomprehensible size, horizontally and vertically, in such a way that it cannot be put back together by shredding or shearing machines.

Personal data transferred from the original paper format to the electronic medium through scanning are destroyed by using one or more of the appropriate methods specified in item (a), depending on the electronic environment they are in.

d) Cloud Environment

When the cloud computing service relationship expires, all copies of the encryption keys required to make personal data available are destroyed. In addition to the above media, the process of destroying personal data in devices that are malfunctioning or sent for maintenance is carried out as follows:

- Destruction of the personal data contained in the relevant devices by using one or more of the appropriate methods specified in item (a) before they are transferred to third parties such as manufacturers, vendors, service points for maintenance and repair,
- Where it is not possible or feasible to destroy, the data storage media is removed and stored, and other failed parts are sent to third parties such as manufacturers, dealers and service points for maintenance and repair,
- Necessary measures are taken to prevent personnel coming outside for maintenance or repair from copying and taking personal data out of the institution.

11. Periodic destruction period

The Company destroys personal data, whose retention period has expired and does not have any other data processing purpose requiring storage of personal data, within 6 months following the expiration of the retention period.

12. Periods of deletion and destruction of personal data, if requested by the Relevant Person

When the relevant person refers to the Company and requests the deletion or destruction of his/her personal data;

a) If all the conditions for processing personal data have disappeared; the Company deletes, destroys or anonymizes the personal data subject to the request. The Company finalizes the deletion or destruction requests of the relevant persons within **"thirty days"** at the latest.

b) If all the conditions for processing personal data have disappeared and the personal data subject to the request is transferred to third parties; the Company notifies the third party of this situation and requests the deletion or destruction of the personal data in question.

If all the conditions for processing personal data have not disappeared, this request may be rejected by the Company, in accordance with the third paragraph of Article 13 of the Law by explaining the grounds for rejection and the rejection shall be notified to the relevant person in writing or electronically within thirty days at the latest.

13. Title, Unit and Job Descriptions of the Persons involved in the Storage and Destruction Processes

Title	Unit	Position
Sales & Marketing-Operations Manager	General Directorate	S/he is responsible for the Company employees to act in accordance with the Policy and to carry out the PDP process within the Company in full compliance with the relevant legislation.
Sales & Marketing-Operations Manager	General Directorate	S/he is responsible for the preparation, execution, publication and updating of the Policy in relevant environments.
General Manager of the Consultant IT Company	Information Technologies	She is responsible for providing the technical solutions needed in the implementation of the Policy.
General Manager of the Consultant IT Company	Information Technologies	S/he is responsible for ensuring internal audits.

14. Amendments to the Policy on Protection, Storage and Destruction of Personal Data

The COMPANY can always make amendments in the Policy on Protection, Storage and Destruction of Personal Data. These amendments become effective immediately upon the publication of the new amended Policy on Protection, Storage and Destruction of Personal Data. You will be informed about the amendments in this Policy on Protection, Storage and Destruction of Personal Data.