1. PURPOSE

The KVKK Personal Data Retention and Destruction Policy (“Policy”) has been prepared in order to determine the procedures and principles regarding the processes and activities related to retention and destruction carried out by Quad Plus Otomasyon Hizmetleri Ltd. Şti. (“Company”), and to establish the procedures and principles concerning the retention and destruction of personal data and special categories of personal data contained in the data recording systems in electronic and physical environments operated by the Company.

In accordance with the Turkish Personal Data Protection Law No. 6698 (“Law”), the Company has prioritized ensuring that the personal data of Company employees, employee candidates, visitors, suppliers, and customers are processed in compliance with the Constitution of the Republic of Türkiye, international conventions, the Law, and other relevant legislation, and that data subjects can effectively exercise their rights.

The processes and activities related to the retention and destruction of personal data are carried out by the Company in accordance with the Regulation prepared by the Company in this context.

2. SCOPE

Personal data belonging to Company employees, former employees, interns, employee candidates, visitors, suppliers, and customers fall within the scope of this Regulation, and this Regulation shall apply to all recording environments in which personal data owned or managed by the Company are processed, as well as to all activities related to the processing of personal data.

As a Company, our fundamental principle is that the personal data of the Company’s customers, employees, employee candidates, service providers, visitors, and other third parties are processed in compliance with the Constitution of the Republic of Türkiye, international conventions, the Turkish Personal Data Protection Law No. 6698 (“Law”), and other relevant legislation. Within this scope, ensuring that data subjects do not suffer any loss of rights and are able to exercise their rights effectively has been determined as a priority.

This Policy has been prepared in compliance with the provisions of the Law, the Regulation on the Deletion, Destruction or Anonymization of Personal Data published in the Official Gazette dated 28.10.2017 and numbered 30224 (“Regulation”), and other relevant legislation.

3. RESPONSIBILITY

The Company is responsible for the implementation of this procedure, while the Company Personal Data Management Committee is responsible for the execution of the implementation.

4. DEFINITIONS

Recipient Group: The category of natural or legal persons to whom Personal Data are transferred by the Data Controller
Explicit Consent: Consent that is related to a specific subject, based on information, and expressed by free will
Anonymization: Rendering Personal Data incapable of being associated with an identified or identifiable natural person in any way, even by matching them with other data
Employee: Employees of Quad Plus Otomasyon Hizmetleri

Electronic Environment: Environments where Personal Data can be created, read, modified, and written through electronic devices
Non-Electronic Environment: All written, printed, visual, and other environments outside electronic environments
Service Provider: A natural or legal person providing services to the Personal Data Protection Authority within the framework of a specific contract
Data Subject: The natural person whose Personal Data are processed
Relevant User: Persons who process Personal Data within the organization of the Data Controller or in accordance with the authority and instructions received from the Data Controller, excluding the person or unit responsible for the technical storage, protection, and backup of the data
Destruction: The deletion, destruction, or anonymization of Personal Data
Law: Turkish Personal Data Protection Law No. 6698
Recording Environment: Any environment where Personal Data processed fully or partially automatically, or non-automatically provided that it forms part of any data recording system, are located
Personal Data: Any information relating to an identified or identifiable natural person
Personal Data Processing Inventory: An inventory in which Data Controllers detail the Personal Data processing activities they carry out depending on their business processes by associating them with the purposes of processing Personal Data, data categories, recipient groups to whom the data are transferred, and the group of Data Subjects; and in which they specify the maximum period required for the purposes for which the Personal Data are processed, the Personal Data intended to be transferred to foreign countries, and the measures taken regarding data security (see F.191 Personal Data Inventory)
Processing of Personal Data: Any operation performed on Personal Data such as obtaining, recording, storing, retaining, altering, reorganizing, disclosing, transferring, taking over, making available, classifying, or preventing the use of Personal Data, wholly or partially by automated means or by non-automated means provided that it forms part of a data recording system
Policy: KVKK Personal Data Retention and Destruction Policy
Special Categories of Personal Data: Data relating to a person's race, ethnic origin, political opinion, philosophical belief, religion, sect or other beliefs, appearance and dress, membership of associations, foundations or trade unions, health, sexual life, criminal convictions and security measures, as well as biometric and genetic data
Periodic Destruction: The deletion, destruction, or anonymization process to be carried out ex officio at recurring intervals specified in the personal data retention and destruction regulation when all of the conditions for processing Personal Data stipulated in the Law cease to exist
Deletion: Rendering Personal Data inaccessible, irretrievable, and unusable in any way for the Relevant Users
Regulation: Regulation on the Deletion, Destruction or Anonymization of Personal Data
Data Processor: A natural or legal person who processes Personal Data on behalf of the Data Controller based on the authority granted by the Data Controller
Data Recording System: A recording system in which Personal Data are processed by structuring them according to specific criteria
Data Controller: The natural or legal person who determines the purposes and means of processing Personal Data and is responsible for the establishment and management of the data recording system
VERBIS: Data Controllers Registry Information System
Destruction: Rendering Personal Data inaccessible, irretrievable, and unusable by anyone in any way

5. IMPLEMENTATION PRINCIPLES

5.1. Distribution of Duties and Responsibilities

Pursuant to subparagraph (f) of Article 6 of the Regulation, it is stipulated that the titles, duties, and units of the persons involved in the retention and destruction processes of Personal Data must be specified. Within this scope, in order to prevent the unlawful processing and access of Personal Data and to ensure the lawful retention of Personal Data, the titles, duties, and units of the persons within the Company

responsible for the management of data security, retention and destruction processes, and the implementation of technical and administrative measures have been specified.

Company Management: Responsible for ensuring that employees act in accordance with the Policy.

Personal Data Management Committee: Responsible for directing all planning, analysis, research, and risk identification activities in projects carried out within the scope of compliance with the Law; managing the processes that must be carried out in accordance with the Law, the Policy, and other issued policies and procedures; conducting correspondence with the relevant units in order to determine the locations of Personal Data and making decisions in order to evaluate requests received from Data Subjects.

Legal Department and Information Technology Department: Responsible for reviewing requests from Data Subjects and reporting them to the Personal Data Management Committee for evaluation; carrying out the actions related to Data Subject requests that are evaluated and decided upon by the Committee in accordance with the Committee's decision; supervising retention and destruction processes and reporting these audits to the Committee; and executing the retention and destruction processes.

Human Resources and IMS Department: Responsible for the implementation of policies in accordance with their job descriptions and for conducting audits regarding the protection, retention, and destruction of Personal Data.

Employees: Obliged to act in accordance with the Regulation.

5.2. Recording Environments

5.2.1. Digital Environments

- Servers (e-mail, database, web, file sharing, backup, etc.)
- Software (office software, IFS, VERBIS)
- Information security devices (firewall, intrusion detection and prevention systems, antivirus, etc.)
- Personal computers (desktop, laptop)
- Mobile devices (phone, tablet, etc.)
- Optical discs (CD, DVD, etc.)
- Removable storage devices (USB, Memory Card, etc.)
- Printer, scanner, photocopy machine, fax
- Social media accounts
    - Facebook - https://www.facebook.com/quadplusotomasyon
    - Instagram - https://www.instagram.com/quadplusotomasyon
    - LinkedIn - https://www.linkedin.com/company/quadplusotomasyon
    - YouTube - https://www.youtube.com/channel/UCQO2xN7FM7fSmhP2NGAcVCw

5.2.2. Non-Digital Environments

- Paper
- Manual data recording systems (survey forms, visitor undertaking forms)
- Written, printed, visual environments

The table below shows the environments in which the Personal Data and Special Categories of Personal Data retained by the Company are recorded. Personal Data retained by our Company are stored in the most appropriate recording environment according to their nature and legal status.

Recording Environment	Description

Electronic Environments	▪ Servers (backup, e-mail, web, etc.) ▪ Information Security Devices (firewall, intrusion detection and prevention, antivirus, etc.) ▪ Company Computers (Desktop, etc.) ▪ Company Mobile Devices (Phone, etc.)
Non-Electronic Environments	▪ Paper ▪ Written, printed, visual environments

5.3. Explanations Regarding Retention and Destruction

Personal Data belonging to employees, employee candidates, visitors, suppliers, and customers, as well as Personal Data belonging to employees of third parties, institutions, or organizations with whom the Company has relations, are retained and destroyed by the Company in accordance with the Law.

Within the Company, Personal Data belonging to the persons to whom services are provided and to our Company personnel are processed in accordance with the provisions set forth in the Law and are retained in the recording environments specified in this Policy and the Data Security Procedure, and are destroyed in the specified manners.

Personal Data are retained in accordance with Articles 5 and 6 of the Law and based on the personal data processing conditions stated in the information notices. Within this scope, Personal Data are retained for the duration of the validity of the conditions specified for the processing of Personal Data, and when the relevant processing conditions cease to exist or upon the application of the Data Subject to our Company (after verifying the other legal obligations that our Company must comply with), the retained Personal Data are deleted, destroyed, or anonymized upon request.

5.3.1. Legal Grounds Requiring Retention

Personal Data processed within the scope of the Company's activities are retained for the period stipulated in the relevant legislation. Within this scope, Personal Data are retained in accordance with the following:

- Turkish Personal Data Protection Law No. 6698
- Labor Law No. 4857
- Turkish Code of Obligations No. 6098
- Social Insurance and General Health Insurance Law No. 5510
- Law No. 5651 on the Regulation of Publications on the Internet and Combating Crimes Committed Through Such Publications
- Occupational Health and Safety Law No. 6331
- Right to Information Law No. 4982
- Law No. 3071 on the Exercise of the Right to Petition

Personal Data are retained for the retention periods stipulated under these laws and other secondary regulations in force pursuant to these laws.

5.3.2. Processing Purposes Requiring Retention

The Company retains the Personal Data it processes within the scope of its activities for the following purposes:

- Execution of Emergency Management Processes
- Execution of Information Security Processes
- Execution of Employee Candidate / Intern / Student Selection and Placement Processes
- Execution of Employee Satisfaction and Engagement Processes
- Fulfillment of Obligations Arising from Employment Contracts and Legislation for Employees
- Execution of Fringe Benefits and Benefits Processes for Employees
- Execution of Audit / Ethics Activities
- Execution of Training Activities
- Execution of Access Authorization Processes
- Conducting Activities in Compliance with Legislation
- Execution of Finance and Accounting Operations
- Ensuring Physical Space Security
- Execution of Assignment Processes
- Follow-up and Execution of Legal Affairs
- Execution of Internal Audit / Investigation / Intelligence Activities
- Execution of Communication Activities
- Planning of Human Resources Processes
- Execution / Supervision of Business Activities
- Execution of Occupational Health / Safety Activities
- Receiving and Evaluating Suggestions for the Improvement of Business Processes
- Execution of Business Continuity Activities
- Execution of Logistics Activities
- Execution of Goods / Services Procurement Processes
- Execution of Goods / Services Sales Processes
- Execution of Goods / Services Production and Operational Processes
- Execution of Customer Relationship Management Processes
- Organization and Event Management
- Execution of Performance Evaluation Processes
- Execution of Risk Management Processes
- Execution of Retention and Archiving Activities
- Execution of Social Responsibility and Civil Society Activities
- Execution of Contract Processes
- Execution of Sponsorship Activities
- Execution of Strategic Planning Activities
- Monitoring of Requests / Complaints
- Execution of Supply Chain Management Processes
- Execution of Wage Policy Processes
- Ensuring the Security of Data Controller Operations
- Work and Residence Permit Procedures for Foreign Personnel
- Execution of Investment Processes
- Execution of Talent / Career Development Activities
- Providing Information to Authorized Persons, Institutions and Organizations
- Execution of Management Activities
- Creation and Monitoring of Visitor Records

5.3.3. Reasons Requiring Destruction

Personal Data are destroyed in the following cases:

- Expiration of the retention periods specified in the relevant legislation,
- Amendment or repeal of the provisions of the relevant legislation that constitute the basis for processing,
- Elimination of the purpose requiring the processing or retention of the Personal Data,
- In cases where the processing of Personal Data is based solely on Explicit Consent, withdrawal of Explicit Consent by the Data Subject,
- Acceptance by the Company of the application made by the Data Subject within the scope of the rights set forth in Article 11 of the Law regarding the deletion or destruction of their Personal Data,
- Expiration of the maximum period requiring the retention of Personal Data and the absence of any condition justifying the retention of Personal Data for a longer period; in such cases, Personal Data shall be deleted, destroyed, or anonymized by the Company upon the request of the Data Subject or ex officio.
- In cases where the Company rejects the request made by the Data Subject for the deletion, destruction, or anonymization of their Personal Data, finds the response insufficient, or fails to respond within the period stipulated in the Law; if the Data Subject files a complaint with the Personal Data Protection Authority and this request is deemed appropriate by the Authority, the Personal Data shall be deleted, destroyed, or anonymized by the Company upon the request of the Data Subject or ex officio.

In addition, the necessary protocols and procedures regarding the reasons requiring destruction have completed the internal approval process within the Company and are implemented.

5.4. Teknik ve İdari Tedbirler

Technical and administrative measures are taken to ensure the secure retention of Personal Data, to prevent unlawful processing and access, and to ensure the lawful destruction of Personal Data.

The Company takes all necessary technical and administrative measures appropriate to the nature of the relevant Personal Data and the environment in which they are stored in order to ensure the secure retention of Personal Data and to prevent unlawful processing and access. In addition, our Company also takes technical and administrative measures within the framework of the adequate measures determined and announced by the Personal Data Protection Authority for Special Categories of Personal Data pursuant to Article 12 of the Law and the fourth paragraph of Article 6 of the Law.

5.4.1. Technical Measures

The technical measures taken by the Company regarding the Personal Data it processes are listed below.

- Access to information systems and user authorization are carried out through security policies via the access and authorization matrix and the corporate active directory.
- Necessary measures are taken to ensure the physical security of the Company’s information systems equipment, software, and data.
- In order to ensure the security of information systems against environmental threats, hardware-based (access control system allowing only authorized personnel to enter the system room, 24/7 monitoring system, ensuring the physical security of edge switches forming the local area network, fire suppression system, climate control system, etc.) and software-based (firewalls, attack prevention systems, network access control, systems preventing malicious software, etc.) measures are implemented.
- Access procedures are established within the Company, and reporting and analysis activities regarding access to Personal Data are carried out.

- Security vulnerabilities are monitored, appropriate security patches are applied, and information systems are kept up to date.
- Strong passwords are used in electronic environments where Personal Data are processed.
- Data backup programs that ensure the secure storage of Personal Data are used.
- Employees involved in the processing of Special Categories of Personal Data are provided with training on the security of Special Categories of Personal Data, confidentiality agreements are executed, and the authorizations of users who have access to the data are defined.
- Adequate security measures are taken for the physical environments where Special Categories of Personal Data are processed, stored, and/or accessed; physical security is ensured and unauthorized entry and exit are prevented.

5.4.2. Administrative Measures

The administrative measures taken by the Company regarding the Personal Data it processes are listed below.

- A Personal Data Processing Inventory has been prepared.
- Employees sign confidentiality agreements, undertakings, and consent forms regarding the activities carried out by the Institution.
- Before commencing the processing of Personal Data, the Institution fulfills its obligation to inform the Data Subjects.
- Periodic and random internal audits are conducted.
- A risk analysis regarding the Regulation is conducted.
- Information security training is provided to employees.

5.5. Personal Data Destruction Techniques

At the end of the retention period stipulated in the relevant legislation or the retention period required for the purpose for which they are processed, Personal Data are destroyed by the Company ex officio or upon the request of the Data Subject in accordance with the provisions of the relevant legislation using the techniques specified below.

In accordance with the Law, other relevant legislation, and the Policy, the Company deletes, destroys, or anonymizes the Personal Data it retains when the reasons requiring the processing of the data cease to exist, either upon the request of the Data Subject or ex officio within the periods specified in the Policy.

The deletion, destruction, and anonymization techniques used by the Company are listed below:

5.5.1. Deletion & Destruction of Personal Data

Personal Data Stored on Servers: For Personal Data stored on servers whose retention period has expired, deletion is carried out by the Information Technology Officer by removing the access authorization of the relevant users.

Personal Data in Digital Environments: Personal Data stored in electronic environments whose retention period has expired are rendered completely inaccessible and unusable for all employees except the Information Technology Officer.

Personal Data Not in Digital Environments: Personal Data stored in physical environments whose retention period has expired are rendered completely inaccessible and unusable for all employees except the employees of the Human Resources Department. In addition, a redaction process is applied by crossing out/painting over/erasing the data so that they become unreadable.

5.5.2. Destruction of Personal Data

Personal Data Not in Digital Environments: Personal Data stored in paper environments whose retention period has expired are destroyed in paper shredding machines in an irreversible manner.

5.5.3. Anonymization of Personal Data

Anonymization of Personal Data refers to rendering Personal Data incapable of being associated with an identified or identifiable natural person in any way, even when matched with other data.

For Personal Data to be considered anonymized, it must be rendered incapable of being associated with an identified or identifiable natural person, even through the use of appropriate techniques in terms of the recording environment and the relevant field of activity, such as reversing the data by the Data Controller or third parties and/or matching the data with other data.

5.5.4. Deletion Methods

Personal Data are deleted using the methods provided in the table below.

Deletion Methods for Personal Data Stored in Physical Environments	
Redaction	Personal Data in physical environments are deleted using the redaction method. The redaction process is carried out by cutting out the Personal Data on the relevant document where possible; where this is not possible, by rendering them invisible using permanent ink in a manner that is irreversible and cannot be read through technological solutions.
Deletion Methods for Personal Data Stored in Cloud and Local Digital Environments	
Secure Deletion via Software	Personal Data stored in cloud environments or local digital environments are deleted through a digital command in such a way that they cannot be accessed by any relevant employees other than the database administrator once the retention period has expired, and they are rendered unusable.
Personal Data Stored on Servers	
Deletion by Removing Access Authorization	For Personal Data stored on servers whose retention period has expired, the system administrator removes the access authorization of the relevant users and performs the deletion process.

5.5.5. Destruction Methods

Personal Data are destroyed using the methods provided in the table below.

Destruction Methods for Personal Data Stored in Physical/Printed Environments	
Physical Destruction	Documents stored in printed environments are destroyed using document destruction machines in a manner that they cannot be reassembled.
Destruction Methods for Personal Data Stored in Local Digital Environments and on Servers	
Physical Destruction	This is the physical destruction of optical and magnetic media containing Personal Data, such as melting, burning, or pulverizing them. Data are rendered inaccessible

	through processes such as melting, burning, pulverizing optical or magnetic media, or passing them through a metal grinder.
Demagnetization (Degauss)	This is the process of exposing magnetic media to a high magnetic field so that the data on it are irreversibly corrupted and become unreadable.
Overwriting	The reading and recovery of old data are prevented by writing random data consisting of 0s and 1s at least seven times onto magnetic media and rewritable optical media.
Destruction by Removing Access Authorization	For Personal Data stored on servers whose retention period has expired, the system administrator removes the access authorization of the relevant users and performs the destruction process in a manner that the data cannot be accessed again.
Destruction Methods for Personal Data Stored in Cloud Environments	
Secure Deletion via Software	Personal Data stored in cloud environments are deleted via digital command in a manner that they cannot be recovered again, and when the cloud computing service relationship ends, all copies of the encryption keys required to render the Personal Data usable are destroyed. Data deleted in this way cannot be accessed again.

5.5.6. Anonymization Methods

Methods for Anonymizing Personal Data Stored in Physical/Printed Environments	
Removing Variables	This involves removing one or more direct identifiers within the Personal Data belonging to the Data Subject that may enable the identification of the Data Subject in any way. This method may be used to anonymize Personal Data, as well as to delete information within the Personal Data that does not correspond to the purpose of data processing.
Regional Masking	This is the process of deleting information that may have distinguishing characteristics related to data that constitutes an exceptional case within a data table where Personal Data are collectively stored in anonymized form.
Generalization	This is the process of combining Personal Data belonging to many individuals and converting them into statistical data by removing distinguishing information.
Lower and Upper Bound Coding / Global Coding	Ranges are defined for a particular variable and categorized accordingly. If the variable does not contain a numerical value, data within the variable that are close to each other are categorized. Values within the same category are combined.
Micro Aggregation	With this method, all records in the dataset are first arranged according to a meaningful order and then the entire set is divided into a certain number of subsets. Afterwards, the average value of the designated variable for each subset is calculated and the value of that variable in the subset is replaced with the average value. As a result, indirect identifiers within the data are distorted, making it more difficult to associate the data with the Data Subject.
Data Shuffling and Distortion	Direct or indirect identifiers within the Personal Data are mixed with other values or distorted so that the relationship with the Data Subject is broken and their identifying characteristics are removed.
Methods for Anonymizing Personal Data Stored in Digital Environments / Servers / Cloud	

Environments	
Masking (Encryption, Tokenization, Blurring, Shuffling, Invalidation)	Data masking refers to rendering Personal Data unintelligible in order to prevent unauthorized persons from accessing them. This method is used to prevent confidential and sensitive information within the institution from leaking internally or externally and from being obtained by malicious persons. In data masking, the data format is not changed; only the values are altered. However, this alteration is performed in a manner that cannot be detected or reversed in any way. In addition, by determining who can access which data, only authorized persons are able to view the information they are permitted to see, while other information is masked.

5.6. Retention and Destruction Periods

With respect to the Personal Data processed by the Company within the scope of its activities, the retention periods determined on a Personal Data basis for all Personal Data within the scope of activities carried out depending on the relevant processes are included in the Personal Data Inventory.

Process	Retention Period	Destruction Period
Data retained under the Labor Law (performance records, etc.)	10 years following the termination of the employment relationship	Within 180 days following the end of the retention period
Health reports	15 years following the termination of the employment relationship	Within 180 days following the end of the retention period
Data retained under Social Security Institution (SSI) legislation	10 years following the termination of the employment relationship	Within 180 days following the end of the retention period
Documents that may be used in claims/lawsuits regarding occupational accidents/occupational diseases	10 years following the termination of the employment relationship	Within 180 days following the end of the retention period
Data collected pursuant to other relevant legislation	For the period stipulated in the relevant legislation	Within 180 days following the end of the retention period
In cases where the relevant Personal Data are subject to a crime under the Turkish Penal Code or other legislation imposing criminal sanctions	For the duration of the statute of limitations for the case	Within 180 days following the end of the retention period
Data of persons receiving products/services	10 years following the recording of the data	Within 180 days following the end of the retention period

5.6.1. Data Destruction Periods

In accordance with the Law, relevant legislation, and the KVKK Personal Data Retention and Destruction Policy, the Company deletes, destroys, or anonymizes the Personal Data for which it is responsible during the first periodic destruction process following the date on which the obligation to delete, destroy, or anonymize Personal Data arises.

When the Data Subject applies to the Company pursuant to Article 13 of the Law and requests the deletion or destruction of their Personal Data;

- If all conditions for processing Personal Data have ceased to exist; the Company deletes, destroys, or anonymizes the Personal Data subject to the request using an appropriate destruction method within 30 (thirty) days from the date of receipt of the request, explaining the reason. For the Company to be deemed to have received the request, the Data Subject must submit the request in accordance with the procedures specified in the Law and secondary legislation.
- In any case, the Company informs the Data Subject regarding the action taken.
- If all conditions for processing Personal Data have not ceased to exist, the request may be rejected by the Company pursuant to paragraph 3 of Article 13 of the Law by explaining the reason, and the rejection response is notified to the Data Subject in writing or electronically within 30 (thirty) days at the latest.

5.7. Periodic Destruction Period

Pursuant to Article 11 of the Regulation, the Company has determined the periodic destruction period as 6 months. Accordingly, periodic destruction is carried out within the Institution every year in June and December (at 6-month intervals).

5.8. Publication and Storage of the Policy

The Policy is published in two different formats: with a wet signature (printed paper) and in electronic format. After being signed by the employees, it is stored both digitally and in printed form in their personnel files.

5.9. Update Period

The Policy is reviewed as needed and the necessary sections are updated.

5.10. Entry into Force and Abrogation of the Policy

The Policy shall be deemed to have entered into force following its publication through the Company's email group and its posting on the announcement boards.

6. FILING

It is maintained in the digital folders of the Integrated Management Systems Department and in the printed folders of the Human Resources Department.

7. RELATED DOCUMENTS

Turkish Personal Data Protection Law No. 6698