PERSONAL DATA RETENTION AND DESTRUCTION POLICY

1. Purpose

This Policy sets out the principles to be followed by the data controller TT HOTELS TURKEY OTEL HİZ. TUR. VE TİC. A.Ş. ("TT HOTELS") for the retention and destruction of personal data in accordance with the Personal Data Protection Law No. 6698 ("KVKK") and the relevant legislation. Its purpose is to protect the rights of data subjects, fulfil our obligations through a transparent approach, and regulate data processing activities.

2. Scope

This Policy applies to the personal data of our Company's guests, employees, employee candidates, supplier employees and visitors. It covers all electronic and non-electronic media.

3. Definitions

Recipient Group: The category of natural or legal person to whom personal data is transferred by the data controller.
Explicit Consent: Consent regarding a specific issue, based on information and expressed with free will.
Anonymization: Making personal data impossible to associate with an identified or identifiable natural person in any way, even by matching it with other data.
Employee: TT HOTELS Staff
Employee Candidate: Real person who applies to work in our company.
EBYS: Electronic Document Management System
Electronic Environment: Environments where personal data can be created, read, changed and written with electronic devices.
Non-Electronic Media: All written, printed, visual, etc. other than electronic media. other environments.
Service Provider: Natural or legal person who provides services within the framework of a specific contract between TT HOTELS and KVKK.
Relevant Person: Natural person whose personal data is processed.
Relevant User: Persons who process personal data within the data controller organization or in line with the authorization and instructions received from the data controller, excluding the person or unit responsible for the technical storage, protection and backup of the data.
Destruction: Deletion, destruction or anonymization of personal data.
Law: Personal Data Protection Law No. 6698.
Recording Environment: Any environment where personal data is processed by fully or partially automatic or non-automatic means, provided that it is part of any data recording system.
Personal Data: Any information regarding an identified or identifiable natural person.
Personal Data Processing Inventory: Personal data processing activities carried out by data controllers depending on their business processes; The inventory they create by associating the personal data with the purposes and legal reason for processing personal data, the data category, the transferred recipient group and the data subject person group, and detailing the maximum retention period required for the purposes for which personal data are processed, the personal data envisaged to be transferred to foreign countries and the measures taken regarding data security.
Processing of Personal Data: All kinds of operations performed on data such as obtaining, recording, storing, preserving, changing, rearranging, disclosing, transferring, taking over, making available, classifying or preventing the use of personal data by fully or partially automatic or non-automatic means provided that it is part of any data recording system.
Board: Personal Data Protection Board
KVKK: Personal data protection authority
Guest: Real person staying in our hotel
Special Personal Data: Data regarding people's race, ethnic origin, political opinion, philosophical belief, religion, sect or other beliefs, appearance and dress, association, foundation or union membership, health, sexual life, criminal conviction and security measures, as well as biometric and genetic data.
Periodic Destruction: The process of deleting, destroying or anonymizing personal data, which is specified in the personal data storage and destruction policy and will be carried out ex officio at recurring intervals, in case all the conditions for processing personal data specified in the law are eliminated.
Policy: Personal Data Storage and Destruction Policy
Supplier Employee: Company official/employee within the scope of a certain product or service contract.
Data Processor: Real or legal person who processes personal data on behalf of the data controller, based on the authority given by the data controller.
Data Recording System: A recording system in which personal data is structured and processed according to certain criteria.
Data Controller: The natural or legal person who determines the purposes and means of processing personal data and is responsible for establishing and managing the data recording system.

Data Controllers Registry Information System: The information system created and managed by the Presidency, accessible over the internet, that data controllers will use in applying to the Registry and other related transactions related to the Registry.
VERBİS: Data Controllers Registry Information System
Regulation: Regulation on Deletion, Destruction or Anonymization of Personal Data published in the Official Gazette dated 28 October 2017.

4. Authority and Responsibilities

ROLE	JOB DESCRIPTION
Data Controller Contact Person	Within the scope of TT HOTELS, both within the scope of EU GDPR and KVKK, harmonizing the operation of the entire group with the legislation, preparing general policies, inspecting the processes, planning and preparation of trainings, examining and finalizing the applications and complaints to be made in accordance with the legislation, ensuring communication and coordination with the TUI Center and other companies of TUI, by TUI Center. Fulfilling the assigned duties is the main duty of this commission. It also performs the duties of registering to VERBİS, notifying and responding to correspondence with the KVK Authority on behalf of the Data Controller.
KVKK Commission	Local data protection compliance subject matter expert • To take into account the obligations of businesses and relevant employees under applicable data protection laws, including the EU General Data Protection Regulation. • Monitor, evaluate, analyze and verify compliance with applicable data protection laws, including regulatory and internal data protection policies. • Supporting the investigation and handling of data protection complaints and data security incidents. • Propose and monitor the performance of data protection impact assessments • To develop, deliver and monitor employee training and awareness. • Maintain and comply with applicable recordkeeping requirements. • Act as a point of contact and cooperate with the local supervisory authority. • Cooperating with the TUI Group Data Protection and Privacy Network.
Data Security Commission	Identifying IT and Physical Infrastructure gaps and informing the management how and at what costs these gaps and deficiencies can be closed, taking the necessary actions with the approval of the management, carrying out the necessary controls and inspections both on the basis of the facility and the Head Office.
Facility DPO	As TT HOTELS, ensuring that all decisions and implementation instructions taken within the scope of KVKK/GDPR are implemented and supervised in the facility in charge, and supporting the process by participating in the training given by

	the facility KVVK/GDPR trainer, To identify the problems and needs in the facilities and to report them to both the KVKK commission and the Data Security Commission, and to fulfill other duties assigned by the KVKK/GDPR Commission.
Hotel KVKK Training Officer	To make plans for the delivery of KVKK awareness training to all personnel, to provide training and or to ensure that the training is carried out.

5. Legal Reasons and Purposes Requiring Storage

Personal data is processed for the legal reasons specified in Articles 5 and 6 of KVKK and for the following purposes:

5.1. Legal Reasons

- GENERAL HYGIENE LAW NO. 1593
- LAND TRANSPORT REGULATION NO. 30295
- LABOR LAW NO. 4857
- POPULATION SERVICES LAW NO. 5490
- SOCIAL INSURANCE AND GENERAL HEALTH INSURANCE LAW NO. 5510,
- LAW NUMBERED 5651 ON REGULATION OF PUBLICATIONS MADE ON THE INTERNET AND FIGHTING CRIMES COMMITTED THROUGH THESE PUBLICATIONS,
- TURKISH CODE OF OBLIGATIONS NO. 6098,
- OCCUPATIONAL HEALTH AND SAFETY LAW NO. 6361,
- PERSONAL DATA PROTECTION LAW NO. 6698,

5.2. Purposes

Data Category	**Purpose of Personal Data Processing**
1-ID	-Execution of Emergency Management Processes -Conducting Employee Candidate / Intern / Student Selection and Placement Processes -Execution of Employee Satisfaction and Loyalty Processes - Fulfillment of Employment Contract and Legislation Obligations for Employees -Conducting Educational Activities -Conducting Activities in Compliance with Legislation -Execution of Commitment Processes to the Company / Product / Services -Ensuring Physical Space Security -Following and Execution of Legal Affairs -Performing Communication Activities -Execution/Audit of Business Activities -Performing Occupational Health / Safety Activities -Execution of Logistics Activities -Execution of Goods / Service Purchasing Processes -Execution of Goods / Service Sales Processes -Conducting Performance Evaluation Processes -Execution of Contract Processes -Following of Requests / Complaints -Foreign Personnel Work and Residence Permit Procedures -Conducting Talent / Career Development Activities -Providing Information to Authorized Persons, Institutions and Organizations -Creation and Tracking of Visitor Records
2-Contact	-Execution of Emergency Management Processes -Conducting Employee Candidate / Intern / Student Selection and Placement Processes - Fulfillment of Employment Contract and Legislation Obligations for Employees

	-Conducting Activities in Compliance with Legislation -Execution of Commitment Processes to the Company / Product / Services -Ensuring Physical Space Security -Following and Execution of Legal Affairs -Performing Communication Activities -Execution of Logistics Activities -Execution of Goods / Service Purchasing Processes -Following of Requests / Complaints -Foreign Personnel Work and Residence Permit Procedures -Providing Information to Authorized Persons, Institutions and Organizations -Creation and Tracking of Visitor Records
4-Essentials	- Fulfillment of Employment Contract and Legislation Obligations for Employees -Conducting Educational Activities -Conducting Performance Evaluation Processes -Conducting Talent / Career Development Activities -Providing Information to Authorized Persons, Institutions and Organizations
5-Legal Action	-Following and Execution of Legal Affairs
6-Customer Transaction	-Execution of Emergency Management Processes -Conducting Activities in Compliance with Legislation -Ensuring Physical Space Security -Following and Execution of Legal Affairs -Performing Communication Activities -Execution/Audit of Business Activities -Performing Occupational Health / Safety Activities -Execution of Goods / Service Purchasing Processes -Execution of Goods / Service Sales Processes -Following of Requests / Complaints -Providing Information to Authorized Persons, Institutions and Organizations -Performing Management Activities -Creation and Tracking of Visitor Records
7-Physical Space Security	-Ensuring Physical Space Security -Providing Information to Authorized Persons, Institutions and Organizations -Creation and Tracking of Visitor Records
8-Transaction Security	-Execution of Information Security Processes -Providing Information to Authorized Persons, Institutions and Organizations
10-Finance	-Conducting Employee Candidate / Intern / Student Selection and Placement Processes - Fulfillment of Employment Contract and Legislation Obligations for Employees -Following and Execution of Legal Affairs -Foreign Personnel Work and Residence Permit Procedures -Providing Information to Authorized Persons, Institutions and Organizations
11-Professional Experience	-Execution of Emergency Management Processes -Conducting Employee Candidate / Intern / Student Selection and Placement Processes - Fulfillment of Employment Contract and Legislation Obligations for Employees -Conducting Educational Activities -Conducting Activities in Compliance with Legislation -Ensuring Physical Space Security -Performing Communication Activities -Performing Occupational Health / Safety Activities -Execution of Goods / Service Purchasing Processes -Conducting Performance Evaluation Processes -Execution of Contract Processes -Foreign Personnel Work and Residence Permit Procedures -Conducting Talent / Career Development Activities -Providing Information to Authorized Persons, Institutions and Organizations

13-Visual and Audio Records	-Conducting Employee Candidate / Intern / Student Selection and Placement Processes -Performing Communication Activities -Foreign Personnel Work and Residence Permit Procedures -Providing Information to Authorized Persons, Institutions and Organizations
16-Philosophical Beliefs, Religion, Sects and Beliefs	- Fulfillment of Employment Contract and Legislation Obligations for Employees
21-Health Information	-Execution of Emergency Management Processes -Conducting Employee Candidate / Intern / Student Selection and Placement Processes - Fulfillment of Employment Contract and Legislation Obligations for Employees -Performing Occupational Health / Safety Activities -Providing Information to Authorized Persons, Institutions and Organizations -Other (Protection of Public Health)
23-Criminal Conviction and Security Measures	-Conducting Employee Candidate / Intern / Student Selection and Placement Processes -Ensuring Physical Space Security -Conducting Performance Evaluation Processes -Providing Information to Authorized Persons, Institutions and Organizations
24-Biometric Data	-Ensuring Physical Space Security
26-Other Information - Body Information	-Other (Supply of clothing to staff)

6. Measures Implemented to Protect Personal Data

Technical and Administrative Measures
The following technical and administrative measures are taken to ensure the security of personal data:

Key management is implemented.
Network security and application security are ensured.
A closed system network is used for personal data transfer via the network.
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.
Access logs are kept regularly.
Corporate policies on access, information security, use, storage and destruction have been prepared and implemented.
Confidentiality commitments are made.
The authorities of employees who change their duties or leave their jobs in this area are removed.
Up-to-date anti-virus systems are used.
Firewalls are used.
Personal data security policies and procedures have been determined.
Personal data security issues are reported quickly.
Personal data security is monitored.
Necessary security measures are taken regarding entry and exit to physical environments containing personal data.
The security of physical environments containing personal data against external risks (fire, flood, etc.) is ensured.
The security of environments containing personal data is ensured.
Personal data is reduced as much as possible.
Personal data is backed up and the security of the backed up personal data is ensured.
User account management and authorization control system is implemented and these are also monitored.
Periodic and/or random audits are carried out within the institution.
Log records are kept without user intervention.
Current risks and threats have been identified.
Cyber security measures have been taken and their implementation is constantly monitored.
Penetration testing is applied.
Data processing service providers are periodically audited regarding data security.
Data processing service providers are made aware of data security.
There are disciplinary regulations for employees that include data security provisions.
Training and awareness activities on data security are carried out for employees at regular intervals.
An authority matrix has been created for employees.

Protocols and procedures for the security of special personal data have been determined and implemented.
If sensitive personal data is to be sent via e-mail, it must be sent encrypted using a corporate mail account.
The signed contracts contain data security provisions.
Encryption is done.

7. Measures Applied for the Storage and Destruction of Special Personal Data

Special categories of personal data are strictly protected in accordance with Article 6 of KVKK. Your data, which is processed and stored with the legal consent of the relevant person, is preserved by taking the necessary measures within the limits stipulated by the law. Our company acts with the same sensitivity in the process of processing and storing this sensitive data.

Adequate precautions must be taken for special personal data, both due to their nature and the fact that they may cause victimization or discrimination. These data; Data regarding race, ethnic origin, political thought, philosophical belief, religion, sect or other beliefs, appearance and clothing, association, foundation or union membership, health, sexual life, criminal conviction and security measures, as well as biometric and genetic data.

TT HOTELS takes the necessary measures to protect special personal data that are determined as "special nature" by the Law and processed in accordance with the law. In the technical and administrative measures taken to protect personal data, sensitivity is shown for special personal data.

8. Personal Data Inventory and Retention Periods

8.1. Recording Environments

ELECTRONIC MEDIA	NON-ELECTRONIC MEDIA
Servers (Domain, backup, email, database, web, file sharing, etc.) Software (Office Software, PMS, etc.) Information security devices (firewall, log file, antivirus, etc.) Workstations (Desktop, laptop, etc.) cloud environments Mobile devices (phone, tablet, etc.) Optical discs (CD, DVD, etc.) Removable memories (USB, Memory Card, etc.)	paper Written, printed, visual media

The retention periods of the data are determined in the Retention Periods Table of the "Personal Data Storage and Destruction Policy" document. Referring to the specified table, the general storage periods are as follows.

8.2. Storage Periods

Data Category	**Data Retention Period**
1-ID	10 Years
2-Contact	10 Years
4-Essentials	10 Years
5-Legal Action	10 Years
6-Customer Transaction	10 Years
7-Physical Space Security	1 Month
8-Transaction Security	Indefinite
10-Finance	10 Years
11-Professional Experience	10 Years

Data Category	Data Retention Period
13-Visual and Audio Records	10 Years
16-Philosophical Beliefs, Religion, Sect and Other Beliefs	10 Years
21-Health Information	15 Years
23-Criminal Conviction and Security Measures	10 Years
24-Biometric Data	While working
26-Other Information - Body Information	1 Year

* It must be regulated for a longer period of time in accordance with the legislation or there may be statute of limitations, limitation periods, retention periods, etc. If a longer period is stipulated for storage, the periods in the legislation are considered as the maximum storage period.

9. Reasons Requiring Destruction

Personal data;

- Amendment or abolition of the relevant legislative provisions that constitute the basis for its processing,
- The purpose requiring processing or storage is eliminated,
- In cases where personal data is processed only on the basis of explicit consent, the relevant person withdraws his/her explicit consent,
- TT HOTELS accepts the application made by the relevant person regarding the deletion and destruction of his personal data within the framework of his rights in accordance with Article 11 of the Law,
- In cases where TT HOTELS rejects the application made by the relevant person requesting the deletion, destruction or anonymization of his personal data, finds the answer given insufficient, or does not respond within the period stipulated in the Law; Complaining to the Personal Data Protection Board and this request being approved by the Board,
- The maximum period requiring personal data to be stored has passed and there are no conditions that justify storing personal data for a longer period of time,

In such cases, it is deleted, destroyed or ex officio deleted, destroyed or anonymized by our organization upon the request of the relevant person.

In addition to all these, some of the laws that require the processing and storage of data are stated below:

- Turkish Code of Obligations No. 6098,
- Personal Data Protection Law No. 6698,
- Labor Law No. 4857
- Social Insurance and General Health Insurance Law No. 5510,
- Occupational Health and Safety Law No. 6331
- Turkish Commercial Code No. 6102
- Tax Procedure Law No. 213
- General Hygiene Law No. 1593
- Road Transport Regulation No. 30295

and all other mandatory legislative provisions.

10. Personal Data Destruction Techniques

At the end of the period stipulated in the relevant legislation or the storage period required for the purpose for which they are processed, personal data are destroyed by our organization ex officio or upon the application of the relevant person, using the techniques specified below, in accordance with the provisions of the relevant legislation.

10.1. Deletion Methods

Personal Data on Servers

For personal data on the servers whose retention period has expired, the system administrator removes the access authorization of the relevant users and deletes them.

Personal Data in Electronic Media

Among the personal data in the electronic environment, those whose period of storage has expired are made inaccessible and unusable in any way for other employees (relevant users) except the database administrator.

Personal Data in Physical Environment
For personal data kept in physical media, for which the period requiring its storage has expired, it is made inaccessible and unusable in any way for other employees, except for the unit manager responsible for the document archive. In addition, blackening is also applied by drawing/painting/erasing the surface so that it cannot be read.

Personal Data Contained in Portable Media
Among the personal data kept in Flash-based storage media, those that have expired are stored in secure environments with encryption keys, by being encrypted by the system administrator and access authorization is given only to the system administrator.

10.2. Destruction Methods

Personal Data in Physical Environment
Personal data stored on paper that have expired are irreversibly destroyed in paper shredding machines.

Personal Data Contained in Optical/Magnetic Media
Personal data contained in optical media and magnetic media whose storage period has expired are physically destroyed, such as melting, burning or pulverizing. In addition, the data on the magnetic media is rendered unreadable by passing it through a special device and exposing it to a high magnetic field.

10.3. Anonymization Procedures
Anonymization is the process of making personal data unable to be associated with a specific person. The following methods are used:
Masking: Hiding directly identifying information.
Generalization: Organizing data to represent a specific group.
Data Exchange: Hiding identity information by randomly changing data.
These methods are used especially in statistical analysis and reporting processes.

11. Periodic Destruction
Data is periodically destroyed when the purposes of processing no longer exist and their retention period expires:

Destruction Period	Frequency
Electronic Data	1 time in 6 months
Physical Data	1 time in 6 months

12. Publication and Storage of the Policy
The policy is published electronically and disclosed to the public on the website.

13. Policy Update and Compliance
Our company reserves the right to update it at any time within the framework of changes that may be made in the legislation and the purpose of storage/destruction of personal data within the company.

14. Enforcement of the Policy
This Policy is deemed to have entered into force upon its publication on the company's website.