PERSONAL DATA RETENTION AND DESTRUCTION PROCEDURE

(Personal Data Retention and Destruction Policy)

This document is the English version of İZ.KVK.PR04. In the event of any discrepancy between the two texts, the Turkish original prevails. This document is the instrument referred to as the "personal data retention and destruction policy" in the Regulation on the Deletion, Destruction or Anonymisation of Personal Data. This copy is the publicly disclosed version; details concerning technical infrastructure and security measures have been removed for information-security reasons.

1. INTRODUCTION

By means of this Personal Data Retention and Destruction Procedure (the **"Procedure"**), the procedures and principles governing retention and destruction activities are established for Türkiye Kooperatif Ticaret Eğitim ve Büro İşçileri Sendikası İktisadi İşletmesi İstanbul Şubesi (the **"Enterprise"**) and **İZZ Hotel Koşuyolu** operating within it, in its capacity as data controller under Law No. 6698 on the Protection of Personal Data (the **"Law"**). All operations relating to the retention and destruction of personal data are carried out in accordance with this Procedure.

The Enterprise acts in accordance with this Procedure and the principles set out in it in respect of the retention and destruction of the personal data it holds, in compliance with the Law and with the Regulation on the Deletion, Destruction or Anonymisation of Personal Data (the **"Regulation"**).

2. PURPOSE OF THE PROCEDURE

The principal purpose of this Procedure is to establish the procedures and principles governing the methods and processes for the retention and destruction of personal data processed under the Law and the Regulation, and thereby to inform the data subjects whose personal data is processed.

3. SCOPE OF THE PROCEDURE

This Procedure has been prepared for natural persons whose personal data is processed within the Enterprise by wholly or partly automated means, or by non-automated means provided that it forms part of a data recording system. This Procedure does not apply to data that does not constitute personal data, and may be amended only by written decision where required by the Law or by other regulations on the protection of personal data.

4. DEFINITIONS

"Explicit Consent" Consent relating to a specific matter, based on information and expressed by free will.
"Recipient Group" The category of natural or legal persons to whom personal data is transferred by the data controller.
"Anonymisation" Rendering personal data incapable of being associated with an identified or identifiable natural person in any way, even by matching it with other data.
"Electronic Medium" Media in which personal data can be created, read, altered and written by electronic devices.
"Non-Electronic Medium" All other written, printed, visual and similar media falling outside electronic media.
"Data Subject" The natural person whose personal data is processed.
"Relevant User" Persons who process personal data within the data controller's organisation 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 back-up of the data.
"Destruction" The deletion, destruction or anonymisation of personal data.
"Contact Person" The natural person notified by the data controller at the time of registration with the Registry, for communication with the Authority in respect of obligations arising under the Law and secondary legislation issued thereunder.
"Personal Data" Any information relating to an identified or identifiable natural person.
"Personal Data Processing Inventory" The inventory in which data controllers detail the personal data processing activities they carry out in connection with their business processes, by associating them with the purposes and legal grounds of processing, the data category, the recipient group and the data subject group, and by setting out the maximum retention period necessary for the purposes of processing, the personal data envisaged to be transferred to foreign countries, and the measures taken in respect of data security.
"Personal Data Retention and Destruction Procedure" The instrument on which data controllers rely for determining the maximum period necessary for the purpose of processing and for deletion, destruction and anonymisation operations.
"Processing of Personal Data" Any operation performed on data such as obtaining, recording, storing, retaining, altering, reorganising, disclosing, transferring, taking over, making retrievable, classifying or preventing the use of personal data by wholly or partly automated means, or by non-automated means provided that it forms part of a data

“Explicit Consent” Consent relating to a specific matter, based on information and expressed by free will.
recording system.
“Deletion of Personal Data” Rendering personal data in no way accessible or reusable by relevant users.
“Destruction of Personal Data” Rendering data in no way accessible, retrievable or reusable by anyone.
“Board” The Personal Data Protection Board.
“Authority” The Personal Data Protection Authority.
“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 an association, foundation or trade union, health, sexual life, criminal convictions and security measures, as well as biometric and genetic data.
“Periodic Destruction” The deletion, destruction or anonymisation operation carried out ex officio at recurring intervals as set out in this Procedure, where all of the conditions for processing personal data under the Law have ceased to exist.
“VERBİS (Data Controllers Registry Information System)” The information system created and managed by the Presidency, accessible over the internet, which data controllers use for registration with the Registry and for other related operations.
“Data Processor” The natural or legal person who processes personal data on behalf of the data controller, on the basis of the authority granted by the data controller.
“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.

5. RESPONSIBILITY AND ALLOCATION OF DUTIES

Under the Law and the applicable legislation, a Contact Person has been designated and notified in the VERBİS registration in order to ensure internal coordination within the Enterprise, its maintenance and continuity, and communication with the Authority. The Contact Person is responsible for the follow-up, notification and monitoring of applications and data breaches within the scope of the Law.

In the conduct of retention and destruction processes, the information technology officer is responsible for technical destruction operations, unit managers are responsible for identifying the physical and electronic records within their own units and preparing them

for destruction, and the Contact Person is responsible for coordinating the process and preserving the records.

6. MEDIA IN WHICH PERSONAL DATA IS RETAINED

Personal data processed by the Enterprise is retained in electronic and non-electronic media.

6.1. Electronic Media

This includes the property management system and reservation systems, e-mail and guest communication platforms, office and productivity software and the associated cloud storage areas, server and back-up infrastructure, end-user devices allocated to employees, and the closed-circuit television and audio recording systems.

Information on transfers abroad, including the hosting of reservation engine records outside Türkiye, is available in İZ.KVK.FR07 Hotel Guest Privacy Notice.

6.2. Non-Electronic Media

- Accommodation registration forms, contracts and undertakings kept in paper form,
- Invoices, receipts and other printed accounting documents,
- Personnel files,
- Guest complaint and satisfaction forms, visitor registers,
- Manual data recording systems, unit cabinets and archive cabinets.

7. RETENTION AND DESTRUCTION OF PERSONAL DATA

The Law provides that personal data must be processed in a manner connected with, limited to and proportionate to the purpose, and retained for the period prescribed by the applicable legislation or necessary for the purpose for which it is processed, thereby indicating the requirement to retain personal data for defined periods. Accordingly, personal data processed by the Enterprise is retained for the periods prescribed by the applicable legislation and/or required in accordance with the purposes of processing. Where the reasons requiring processing cease to exist, notwithstanding that the personal data has been processed in accordance with the applicable legislation, the Law and the Enterprise's own rules, such personal data is deleted, destroyed or anonymised by the data controller ex officio or upon the request of the data subject.

7.1. Explanations Concerning Retention

Article 4 of the Law provides that personal data processed must be connected with, limited to and proportionate to the purposes for which it is processed, and retained for the period

prescribed by the applicable legislation or necessary for those purposes; Articles 5 and 6 set out the conditions for processing personal data.

7.1.1. Legal Grounds Requiring Retention

Personal data processed within the Enterprise is retained within the limits set out in the Law and other applicable legislation. Where no such period is prescribed by law, it is first assessed whether the personal data falls within the classification of special categories of personal data. Where special categories of personal data have not been processed and retained in accordance with Article 6 of the Law, they are destroyed immediately by the methods set out in Article 9. Following this process, it is determined whether there is a legitimate purpose for retaining the personal data. Where a decision is taken to retain it, the data is retained for the reasonable periods required under the relevant statutory provisions, established practice and the Enterprise's own rules, and is destroyed at the end of that period.

The following legislative provisions apply to the retention of personal data:

- *Law No. 6698 on the Protection of Personal Data*
- *Law No. 1774 on the Notification of Identity and its Implementing Regulation*
- *Labour Law No. 4857 and related legislation*
- *Law No. 5510 on Social Insurance and Universal Health Insurance and related legislation*
- *Turkish Code of Obligations No. 6098*
- *Law No. 5651 on the Regulation of Publications on the Internet and Combating Crimes Committed by Means of Such Publications*
- *Turkish Commercial Code No. 6102*
- *Law No. 6502 on Consumer Protection*
- *Law No. 6563 on the Regulation of Electronic Commerce and the Regulation on Commercial Communication and Commercial Electronic Messages*
- *Tax Procedure Law No. 213*
- *Law No. 6331 on Occupational Health and Safety and the Regulation on Occupational Health and Safety Services*
- *Law No. 3071 on the Exercise of the Right to Petition*
- *Regulation on the Relations of Tourism Establishments with the Ministry, with One Another and with Their Customers*

- *Regulation on the Qualifications of Tourism Facilities and other secondary legislation in force under the laws listed above*

7.1.2. Processing Purposes Requiring Retention

Data relating to guests, employees and suppliers that is necessary for the fulfilment of legal obligations where required or mandated by legislation, for the continuity of business and commercial activities, for the conclusion and performance of contracts, and for the planning and provision of employee rights and fringe benefits, is retained by the Enterprise within the limits set out in the Law and other applicable legislation.

The Enterprise also retains the personal data it processes in the course of its activities for the following purposes:

Conduct of emergency management processes
Conduct of information security processes
Conduct of job candidate application processes
Fulfilment of obligations arising from employment contracts and legislation in respect of employees
Conduct of processes relating to employee fringe benefits and entitlements
Conduct of audit and ethics activities
Conduct of training activities
Administration of access rights
Conduct of activities in compliance with legislation
Conduct of finance and accounting affairs
Ensuring the security of physical premises
Conduct of assignment processes
Follow-up and conduct of legal affairs
Conduct of communication activities
Planning of human resources processes
Conduct and audit of business activities
Conduct of occupational health and safety activities

Conduct of emergency management processes
Receipt and evaluation of suggestions for the improvement of business processes
Conduct of business continuity activities
Conduct of accommodation and reservation processes
Conduct of procurement processes for goods and services
Conduct of after-sales support services for goods and services
Conduct of goods and services sales processes
Fulfilment of notification obligations arising from legislation (including the Identity Notification System)
Conduct of activities directed at customer satisfaction
Conduct of performance evaluation processes
Conduct of advertising, campaign and promotion processes
Conduct of retention and archiving activities
Conduct of contract processes
Follow-up of requests and complaints
Ensuring the security of movable property and resources
Administration of remuneration policy
Ensuring the security of the data controller's operations
Provision of information to authorised persons, institutions and organisations
Conduct of management activities
Creation and follow-up of visitor records

7.2. Legal Grounds Requiring Destruction

Personal data processed within the Enterprise is deleted, destroyed or anonymised for the reasons set out below, in accordance with this Procedure and the Personal Data Processing and Protection Procedure, and in compliance with the Regulation on the Deletion, Destruction or Anonymisation of Personal Data. Those reasons are:

- Amendment or repeal of the legislative provisions forming the basis for the processing of the personal data,
- Disappearance of the purpose requiring the processing or retention of the personal data,
- Withdrawal of the data subject's explicit consent, where the processing of personal data is based solely on the condition of explicit consent,
- Acceptance by the Enterprise of an application made by the data subject, within the framework of the rights under Article 11 of the Law, for the deletion or destruction of their personal data,
- Where the Enterprise rejects an application made to it by the data subject for the deletion, destruction or anonymisation of their personal data, where the response given is found inadequate, or where no response is given within the period prescribed by the Law, and the data subject lodges a complaint with the Board and that request is upheld by the Board,
- Expiry of the maximum period requiring the retention of the personal data, in the absence of any condition justifying its retention for a longer period.

Where these reasons arise, the personal data concerned is deleted, destroyed or anonymised upon the request of the data subject or ex officio. Where considered necessary, the Enterprise management, the Board and the data subjects are informed in respect of this process.

8. TECHNICAL AND ADMINISTRATIVE MEASURES CONCERNING RETENTION AND DESTRUCTION

Under Article 12 of the Law, the Enterprise has taken the administrative and technical measures necessary to ensure an appropriate level of security in order to prevent the unlawful processing of personal data and unlawful access to it, and to ensure its safekeeping.

As regards administrative measures, internal rules on personal data security have been prepared, confidentiality undertakings have been signed with employees, regular training and awareness activities are carried out, data processing agreements are concluded with data processor service providers, and the personal data processing inventory is kept up to date.

As regards technical measures, access rights are defined in accordance with the need-to-know and least-privilege principles, access records are kept, network and application security is maintained, data is backed up, and encryption and data loss prevention measures are applied.

The details of the measures taken are kept in the Enterprise's internal rules and are not disclosed publicly, since their disclosure could give rise to a security vulnerability. Such information is shared upon the request of authorised public institutions and organisations.

9. TECHNIQUES FOR THE DESTRUCTION OF PERSONAL DATA

Personal data is destroyed by the Enterprise, ex officio or upon the request of the data subject, using the methods and techniques set out below.

9.1. Deletion of Personal Data

The deletion of personal data is the operation of rendering personal data in no way accessible or reusable by relevant users. The Enterprise discharges its obligation to take all necessary technical and administrative measures to ensure that deleted personal data is inaccessible and non-reusable by relevant users.

Personal data held on servers: For data whose retention period has expired, the access rights of relevant users are removed by the system administrator and the data is deleted.
Personal data stored in electronic media: Deletion is carried out by the system administrator by removing the access rights of relevant users; the relevant rows in database records are deleted by means of database commands.
Personal data stored in cloud environments and on systems hosted abroad: Data is deleted using the deletion function available at the service provider; in addition, it is rendered inaccessible by destroying the encryption keys relating to the data, and confirmation of the deletion is obtained from the provider.
Personal data held on portable media: Such data, which is stored in encrypted form in secure environments by the system administrator, is rendered inaccessible and non-reusable at the end of the retention period by means of overwriting or destruction of the encryption key.
Personal data stored in non-electronic media: Personal data held in physical media is deleted using the redaction method. Redaction is carried out by cutting out the personal data on the document where possible and, where not possible, by rendering it invisible using permanent ink in a manner that is irreversible and unreadable by technological means.

9.2. Destruction of Personal Data

Personal data stored in electronic media: Upon expiry of the retention period or upon the request of the data subject, the appropriate method among degaussing, physical destruction (melting, incineration, pulverisation) or overwriting is applied according to the characteristics of the medium in which the data is held.

Personal data stored in electronic media: Upon expiry of the retention period or upon the request of the data subject, the appropriate method among degaussing, physical destruction (melting, incineration, pulverisation) or overwriting is applied according to the characteristics of the medium in which the data is held.
Personal data stored in non-electronic media: Personal data held in physical media is destroyed irreversibly by shredding or incineration.

9.3. Anonymisation of Personal Data

The anonymisation of personal data means rendering personal data incapable of being associated with an identified or identifiable natural person in any way, even where it is matched with other data.

Where anonymisation is chosen as the method of destruction, techniques appropriate to the recording medium and the relevant field of activity — such as variable removal, masking, aggregation, data derivation and data shuffling — are used. These techniques are applied so as to ensure that the data cannot be associated with an identified or identifiable natural person, even by reversal by the data controller or third parties and/or by matching with other data.

10. RETENTION PERIODS

In respect of the personal data processed by the Enterprise in the course of its activities:

- Retention periods on a personal-data basis for all personal data within the activities carried out in connection with processes are set out in the Personal Data Processing Inventory,
- Retention periods on a process basis are set out in this Procedure.

Retention and destruction periods on a process basis are as follows:

Process	Retention Periods (Maximum)	Destruction Periods
Legal proceedings with attorneys	Up to 5 years	In the first periodic destruction following expiry of the retention period, within 6 months at the latest
BA / BS notifications	Up to 10 years	In the first periodic destruction following expiry of the retention period, within 6 months at the latest
Tax return process	Up to 10 years	In the first periodic destruction following expiry of the retention

Process	Retention Periods (Maximum)	Destruction Periods
		period, within 6 months at the latest
Retention of employee and visitor IP addresses	Up to 2 years	In the first periodic destruction following expiry of the retention period, within 6 months at the latest
Account management process	For the duration of employment	In the first periodic destruction following expiry of the retention period, within 6 months at the latest
Data subject application records	Up to 5 years	In the first periodic destruction following expiry of the retention period, within 6 months at the latest
Destruction records	At least 3 years	In the first periodic destruction following expiry of the retention period, within 6 months at the latest
Retention of internet access logs	Up to 2 years	In the first periodic destruction following expiry of the retention period, within 6 months at the latest
Occupational health and safety activities	Up to 15 years	In the first periodic destruction following expiry of the retention period, within 6 months at the latest
Management of recruitment processes	10 years after termination of employment	In the first periodic destruction following expiry of the retention period, within 6 months at the latest
Management of exit processes	10 years after termination of employment	In the first periodic destruction following expiry of the retention period, within 6 months at the latest
CCTV image recordings	Up to 30 days	In the first periodic destruction following expiry of the retention period, within 6 months at the latest
Reception audio recordings	Up to 15 days	In the first periodic destruction following expiry of the retention period, within 6 months at the latest
Campaign / advertising process	Up to 2 years	In the first periodic destruction following expiry of the retention

Process	Retention Periods (Maximum)	Destruction Periods
		period, within 6 months at the latest
Parcel acceptance process	Up to 5 years	In the first periodic destruction following expiry of the retention period, within 6 months at the latest
Identity Notification System (notification to law enforcement) process	Period prescribed by legislation	In the first periodic destruction following expiry of the retention period, within 6 months at the latest
Guest complaint and request records	Up to 2 years	In the first periodic destruction following expiry of the retention period, within 6 months at the latest
Accounting records process	Up to 10 years	In the first periodic destruction following expiry of the retention period, within 6 months at the latest
Customer satisfaction survey	Up to 1 year	In the first periodic destruction following expiry of the retention period, within 6 months at the latest
Hotel stays	Up to 10 years	In the first periodic destruction following expiry of the retention period, within 6 months at the latest
Invoices for hotel room payments	Up to 10 years	In the first periodic destruction following expiry of the retention period, within 6 months at the latest
Follow-up of personnel file processes	10 years after termination of employment	In the first periodic destruction following expiry of the retention period, within 6 months at the latest
Personnel job application process	Up to 6 months	In the first periodic destruction following expiry of the retention period, within 6 months at the latest
Personnel salary operations	10 years after termination of employment	In the first periodic destruction following expiry of the retention period, within 6 months at the latest
Reporting processes	Up to 1 year	In the first periodic destruction following expiry of the retention

Process	Retention Periods (Maximum)	Destruction Periods
		period, within 6 months at the latest
Notifications to public authorities	Up to 10 years	In the first periodic destruction following expiry of the retention period, within 6 months at the latest
Reservation processes (reservation engine and agency channels)	Up to 10 years	In the first periodic destruction following expiry of the retention period, within 6 months at the latest
Procurement processes	Up to 10 years	In the first periodic destruction following expiry of the retention period, within 6 months at the latest
Commercial electronic message process	3 years from withdrawal of consent	In the first periodic destruction following expiry of the retention period, within 6 months at the latest
Remuneration and fringe benefits process	10 years after termination of employment	In the first periodic destruction following expiry of the retention period, within 6 months at the latest
Data breach records	Up to 5 years	In the first periodic destruction following expiry of the retention period, within 6 months at the latest
Visitor records	Up to 1 year	In the first periodic destruction following expiry of the retention period, within 6 months at the latest
Asset assignment process	For the duration of employment	In the first periodic destruction following expiry of the retention period, within 6 months at the latest

(Table 1: Retention and destruction periods on a process basis)

11. PERIODIC DESTRUCTION PERIOD

The periodic destruction period for personal data has been set at six months, as provided in the Regulation. Accordingly, the Enterprise deletes, destroys or anonymises personal data in the first periodic destruction operation following the date on which the obligation to delete, destroy or anonymise arises. Periodic destruction is carried out in January and July of each year.

Records and minutes relating to deletion, destruction and anonymisation operations are retained for at least three years in accordance with the Regulation.

12. THE ENTERPRISE'S DUTY TO INFORM

In accordance with the obligation set out in Article 10 of the Law, the Enterprise discharges its duty to inform by notifying data subjects of the identity of the data controller, the purposes for which personal data will be processed, the parties to whom the processed personal data may be transferred and for what purposes, the method and legal ground of collection of personal data, and the rights of the data subject.

In accordance with Article 11 of the Law, the Enterprise provides the necessary information where the data subject requests it.

13. RIGHTS OF THE DATA SUBJECT

The statutory rights that the data subject may exercise under Article 11 of the Law are as follows:

- To learn whether their personal data is being processed,
- To request information if their personal data has been processed,
- To learn the purpose of processing their personal data and whether it is used in accordance with that purpose,
- To know the third parties in Türkiye or abroad to whom their personal data is transferred,
- To request the rectification of their personal data where it has been processed incompletely or inaccurately, and to request that the action taken be notified to the third parties to whom the data has been transferred,
- To request the erasure or destruction of their personal data where the reasons requiring its processing cease to exist, notwithstanding that it has been processed in accordance with the Law and other applicable legislation, and to request that the action taken be notified to the third parties to whom the data has been transferred,
- To object to an adverse outcome arising against them as a result of the analysis of the processed data exclusively by automated means,
- To claim compensation for damage suffered as a result of the unlawful processing of their personal data.

14. EXERCISE OF THE DATA SUBJECT'S RIGHTS

In accordance with the Law, requests relating to the exercise of the rights set out above may be submitted through the contact addresses below by means of a wet-signed petition delivered in person, through a notary public or by registered mail with return receipt, or by using a registered electronic mail (KEP) address, secure electronic signature, mobile signature, or an e-mail address previously notified to the Enterprise and recorded in the Enterprise's systems. Please verify the current application methods against the applicable legislation before applying.

Postal Address	Acıbadem Mahallesi, Şeyh Galip Sokak No: 11, Kadıköy / İstanbul
E-mail Address	kvkk@izzhotelkosuyolu.com
Registered Electronic Mail (KEP)	turkiyekoopisiktisadiisletmesi@hs01.kep.tr

Where requests are submitted in writing, they are concluded free of charge as soon as possible and within thirty days at the latest, according to the nature of the request. Where the operation requires an additional cost, the fee set out in the tariff determined by the Personal Data Protection Board will be charged.

15. THE DATA SUBJECT'S RIGHT TO LODGE A COMPLAINT WITH THE BOARD

Where an application is rejected, where the response given is found inadequate, or where no response is given within the prescribed period, the data subject may lodge a complaint with the Board within thirty days of learning of the data controller's response and, in any event, within sixty days of the date of application. Under the Law, a complaint may not be made without first exhausting the application procedure.

16. ENTRY INTO FORCE, PUBLICATION AND UPDATING

This Procedure was approved by decision of the Enterprise management on 15.07.2026 and is published on the website of İZZ Hotel Koşuyolu (www.izzhotelkosuyolu.com) and made available to data subjects.

The Procedure may be amended by decision of the Enterprise management. Amendments are published on the same website. The current version is identified by the revision number and date shown in its footer.

İZ.KVK.PR04-EN Rev.03 (Presentation Copy) Date: 10.08.2026