CROWNE PLAZA İSTANBUL ASIA HOTEL-VIA OTELCİLİK YÖNETİMLERİ A.Ş.

PERSONAL DATA STORAGE AND DISPOSAL POLICY

1. INTRODUCTION AND THE PURPOSE AND SCOPE OF THE POLICY

Law No. 6698 on the Protection of Personal Data, which entered into force in 2016 after the protection of personal data became a constitutional right in 2010, is a legal protection device developed in order to protect the principle of privacy during the processing of personal data and to prevent damage to fundamental rights and freedoms.
Pursuant to Article 16 of Law No. 6698 ("KVKK" or "Law"), data controllers who are obliged to register with the Data Controllers Registry are obliged to prepare a personal data retention and destruction policy in accordance with the personal data processing inventory. This Personal Data Storage and Destruction Policy has been prepared in order to determine the procedures and principles to be applied by Crowne Plaza Istanbul Asia Hotel - Via Otelcilik Yönetimleri A.Ş. regarding the deletion, destruction or anonymization of personal data in accordance with the Law No. 6698 and other legislation.
Pursuant to the Law on the Protection of Personal Data and the Regulation on the Deletion, Destruction or Anonymization of Personal Data dated October 28, 2017 ("Regulation"), which is a secondary regulation of the Law, the personal data storage and destruction policy that we have prepared in order to fulfill our obligations as Crowne Plaza Istanbul Asia Hotel is as a minimum;

a) The purpose of preparing the personal data retention and destruction policy,
b) Definitions of legal and technical terms in the personal data storage and destruction policy,
c) The recording media regulated by the personal data retention and destruction policy,
ç) Explanation of the legal, technical or other reasons requiring the storage and destruction of personal data,
d) Technical and administrative measures taken for the secure storage of personal data and the prevention of unlawful processing and access,
e) Technical and administrative measures taken for the destruction of personal data in accordance with the law,
f) Titles, units and job descriptions of those involved in personal data storage and destruction processes,
g) Table showing storage and destruction periods, ğ) Periodic destruction periods,
h) If an update has been made to the existing personal data storage and destruction policy, it includes information regarding the change in question.

2. DEFINITIONS

Law / KVKK is one of the definitions in the Personal Data Protection Law No. 6698, which entered into force on 07/04/2016 with its publication in the Official Gazette;

Board; Personal Data Protection Board,

Data Controllers Registry Information System (VERBIS); the information system created and managed by the Presidency, accessible via the internet, which data controllers will use in the application to the Registry and other transactions related to the Registry,

Explicit Consent; consent on a specific subject, based on information and expressed with free will,

Personal Data; any information relating to an identified or identifiable natural person,
Sensitive Personal Data; biometric and genetic data related to 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,
Processing of Personal Data; all kinds of operations performed on personal data such as obtaining, recording, storing, storing, preserving, modifying, reorganizing, disclosing, transferring, taking over, making available, classifying or preventing the use of personal data in whole or in part automatically or by non-automatic means provided that it is part of any data recording system,
Disposal is the deletion, destruction or anonymization of personal data.

- The process of deleting personal data, making the data unusable,
- Destruction of personal data is the process of making the data inaccessible, unrecoverable and unusable by anyone in any way,
- Anonymization, making the data impossible to be associated with an identified or identifiable natural person, even by matching the data with other data.

Recording Medium; any medium in which personal data processed by fully or partially automated or non-automated means, provided that it is part of any data recording system,
Electronic Recording Environment; environments where personal data can be created, read, changed and written with electronic devices**,**
Non-Electronic Recording Media; all written, printed, visual, etc. media other than electronic media,
Personal data processing inventory; the inventory that data controllers create by associating the personal data processing activities they carry out depending on their business processes with the personal data processing purposes and legal reason, data category, transferred recipient group and data subject group, and detailing the maximum retention period required for the purposes for which personal data are processed, personal data foreseen to be transferred to foreign countries and the measures taken regarding data security,
Personal data retention and destruction policy; the policy on which data controllers rely for the process of determining the maximum period of time required for the purpose for which personal data are processed and the process of deletion, destruction and anonymization,
Periodic destruction; the process of deletion, destruction or anonymization to be carried out ex officio at recurring intervals specified in the personal data storage and destruction policy in case all the conditions for processing personal data specified in the law disappear,
Data recording system refers to the recording system in which personal data are structured
and processed according to certain criteria.

Subjects Defined by the Personal Data Protection Law and Regulation

Data Controller is 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.
Relevant User; persons who process personal data within the organization of the data controller or in accordance with the authorization and instruction received from the data controller, except for the person or unit responsible for the technical storage, protection and backup of the data.
Recipient Group is the category of natural or legal person to whom personal data is transferred by the data controller.
Data subject is the natural person whose personal data is processed.
Direct identifiers are identifiers that, on their own, directly reveal, disclose and distinguish the person with whom they are in a relationship**.**
Indirect identifiers are identifiers that, in combination with other identifiers, reveal, disclose and make distinguishable the person to whom they relate.

3. GENERAL INFORMATION AND BASIC PRINCIPLES

- In the event that all of the conditions for processing personal data specified in Articles 5 and 6 of the Law disappear, personal data are deleted or destroyed by Crowne Plaza Istanbul Asia Hotel as the data controller ex officio or upon the request of the data subject.
- The requests submitted to us by the data subject in order to exercise any right written in Article 11 of the Law are finalized within 30 (thirty) days at the latest and the data subject is informed.
- Crowne Plaza Istanbul Asia Hotel acts in accordance with the general principles in Article 4 of the Law and the technical and administrative measures to be taken within the scope of Article 12, the provisions of the relevant legislation, board decisions and the personal data storage and destruction policy in the deletion, destruction or anonymization of personal data.
- All transactions regarding the deletion, destruction, anonymization of personal data are recorded by Crowne Plaza Istanbul Asia Hotel.
- Unless otherwise decided by the Board, it chooses the appropriate method of ex officio deletion, destruction or anonymization of personal data as the data controller. However, upon the request of the data subject, the appropriate method may be selected by explaining the reason.

4. RECORDING MEDIUMS

Personal data belonging to the data subjects are securely stored by Crowne Plaza Istanbul Asia Hotel in the environments listed below in accordance with the relevant legislation, especially the provisions of KVKK, and within the framework of international data security principles:

ELECTRONIC MEDIA

- **Servers** (Backup server and storage unit, electronic mail server, database server, web server, file server, application server, etc.)
- **Software (**Office software, accounting software and other related ERP software Information security systems (firewall device, firewall software, antivirus)
  - **Personal computers** (Desktop, laptop)
  - **Mobile devices** (phones, tablets, etc.)
  - **Optical disks** (CD, DVD etc.)

    Removable memory
  - **Printer, scanner, photocopier**
  - **Camera Recording Systems**
  - **Personal computers (Desktop, laptop)**
  - **Mobile devices (phones, tablets, etc.)**
  - **Optical disks (CD, DVD etc.)**
  - **Removable memories**
  - **Printer, scanner, photocopier**
  - **Camera Recording Systems**

A. NON-ELECTRONIC MEDIA

- **Paper**
- **Manual data recording systems (such as questionnaires, forms, consents, releases, cards)**
- **Written, printed and visual media**

B. NON-ELECTRONIC MEDI

- **Paper**
- **Manual data recording systems (such as questionnaires, forms, consents, releases, cards)**
- **Written, printed and visual media**

C.

NON-ELECTRONIC MEDI

- **Paper**
- **Manual data recording systems (such as questionnaires, forms, consents, releases, cards)**
- **Written, printed and visual media**

5. REASONS FOR STORAGE AND DESTRUCTION OF PERSONAL DATA

5.1. Storage of Personal Data

The personal data processed may vary according to the type and nature of Crowne Plaza Istanbul Asia Hotel services.

Personal data belonging to the relevant persons; Crowne Plaza Istanbul Asia Hotel, as the data controller, stores the data of

employees and customers, which are necessary for the performance of mutual acts/actions such as explicitly stipulated in the laws, determination of commercial and business strategies, employment contracts, sales and service contracts, in physical or electronic media in a secure manner within the limits specified in the KVKK and other relevant legislation.

More precisely, the legal purposes and reasons requiring storage are as follows:

A. Purposes;

- ❖ Sustaining commercial activities,
- ❖ Fulfillment of legal obligations,
- ❖ Planning and execution of employee rights and benefits,
- ❖ Conducting employee satisfaction and loyalty processes,
- ❖ Ability to manage customer relations,
- ❖ The establishment, exercise or protection of a right,
- ❖ Data processing is mandatory for the legitimate interest of the data controller, provided that it does not harm the fundamental rights and freedoms of the data subject,
- ❖ Legislation clearly stipulates the storage of personal data,
- ❖ In cases where one of the conditions listed in Article 5/2 of the KVKK cannot be mentioned, the explicit consent of the data subjects in terms of storage activities,
- ❖ Ensuring physical space security,
- ❖ Personal data are stored within the framework of the limits set by the law and regulation for the reasons of the execution of the remuneration policy.

B. Legal Basis;

- Law No. 6698 on the Protection of Personal Data,
- Turkish Commercial Code No. 6102,
- Turkish Code of Obligations No. 6098,
- Law No. 5510 on Social Security and General Health Insurance,
- Law No. 2634 on Tourism Incentives
- Law No. 1774 on Identity Notification and Regulation on the Implementation of the Identity Notification Law,
- Law No. 5651 on the Regulation of Publications on the Internet and Combating Crimes Committed Through These Publications,
- Law No. 6331 on Occupational Health and Safety,
- Labor Law No. 4857, Vocational Education Law No. 3308,
- Law No. 2547 on Higher Education, Law No. 5434 on Retirement Health,
- Law No. 2828 on Social Services,
- Regulation on Health and Safety Measures to be Taken in Workplace Buildings and Annexes,
- Any other legal basis

5.2 Deletion and Destruction by Crowne Plaza Istanbul Asia Hotel upon request or ex officio within the limits set by the Regulation and the Law, in the cases listed below;

- ❖ Acceptance by the data controller of the application made by the data subject for the deletion, destruction or anonymization of his/her data by exercising his/her rights under Article 11 of the Law,
- ❖ The data subject makes a complaint to the Board due to the fact that the data controller does not respond to the application of the data subject by exercising his/her rights under Article 11 of the Law, rejects the application or the response is insufficient, and the Board finds it appropriate,
- ❖ The personal data has been processed with explicit consent and the data subject withdraws this explicit consent,
- ❖ Although the maximum period for retaining personal data has elapsed, there are no circumstances that justify retaining personal data for a longer period,
- ❖ Amendment or abolition of the provisions of the relevant legislation that constitute the basis for the processing or storage of personal data,
- ❖ Disappearance of the purpose requiring the processing or storage of personal data,
- ❖ It is deleted or destroyed in cases where the conditions requiring the processing of personal data in Articles 5 and 6 of the Law disappear.

6. TECHNICAL AND ADMINISTRATIVE MEASURES

The administrative and technical measures taken by the data controller Crowne Plaza Istanbul Asia Hotel for the secure

storage of personal data and the prevention of unlawful processing and access to it, and its **destruction** in accordance with the law are as follows.

6.1. Administrative Measures

Below are the administrative measures taken by Crowne Plaza Istanbul Asia Hotel:

- Corporate policies on access, information security, use, storage and disposal have been prepared and implemented.

1 **Rights of the person concerned**

ARTICLE 11- (1) Everyone can apply to the data controller;

a)Learn whether personal data is being processed,

b) Request information if personal data has been processed,

c) To learn the purpose of processing personal data and whether they are used in accordance with their purpose,

ç) To know the third parties to whom personal data are transferred domestically or abroad,

d)To request correction of personal data in case of incomplete or incorrect processing,

e) To request deletion or destruction of personal data within the framework of the conditions stipulated in Article 7,

f) To request notification of the transactions made pursuant to subparagraphs (d) and (e) to third parties to whom personal data are transferred,

g)To object to the emergence of a result to the detriment of the person himself/herself by analyzing the processed data exclusively through automated systems,

ğ) In case of damage due to unlawful processing of personal data, it has the right to demand the compensation of the damage.

- Confidentiality commitments are made.
- Signed contracts contain data security provisions.
- Personal data security policies and procedures have been determined.
- Personal data security issues are reported quickly.
- Awareness of data processing service providers on data security is ensured.
- Necessary security measures are taken for entry and exit to physical environments containing personal data.
- Physical environments containing personal data are secured against external risks (fire, flood, etc.).
- Personal data is minimized as much as possible.
- Internal periodic and/or random audits are carried out and conducted.

6.2 Technical Measures

- Network security and application security are ensured.
- Closed system network is used for personal data transfers through the network.
- Security measures are taken within the scope of procurement, development and maintenance of information technology systems.
- Training and awareness raising activities on data security are carried out for employees at regular intervals.
- Access logs are regularly time-stamped.
- The authorizations of employees who change their duties or leave their jobs in this area are removed.
- Up-to-date anti-virus systems are used.
- Firewall devices and software are used.
- Personal data security is monitored.
- Personal data is backed up and the security of backed up personal data is also ensured.
- User account management and authorization control are periodically performed and monitored.
- In-house periodic and/or random audits are carried out and conducted.
- Log records are kept without user intervention.
- If sensitive personal data is to be sent via electronic mail, it is sent using KEP or corporate mail account.

7. STORAGE AND DISPOSAL PERIODS

The following criteria are utilized by the data controller Crowne Plaza Istanbul Asia Hotel in determining the storage and destruction periods of your personal data obtained in accordance with the provisions of the Law and the relevant legislation:

7.1. The period stipulated in the law or regulations regarding the storage and destruction of personal data is complied with. Following the expiration of the aforementioned period, the data is processed in accordance with Article 7.2 below.

7.2. In the event that the period stipulated in the law or regulations for the storage of the personal data in question expires or no period is stipulated for the storage of the relevant personal data, respectively;

- According to Article 6 of the Law, all personal data determined to be of special nature shall be destroyed. The method to be applied in the destruction of such data is determined according to the nature of the data and the importance of its storage for Crowne Plaza Istanbul Asia Hotel.
- The compliance of the storage of the data with the principles specified in Article 4 of the Law is questioned. Data that is found to be in violation of the principles set out in Article 4 of the Law are deleted, destroyed or anonymized.
- It is determined which of the exceptions stipulated in Articles 5 and 6 of the Law can be considered within the scope of data retention. Within the framework of the determined exceptions, reasonable periods of time for which the data should be retained are determined. Upon expiration of such periods, the data shall be deleted or destroyed.

8. PERSONAL DATA DISPOSAL PROCEDURES

8.1. Erasure of Personal Data

Deletion of personal data is the process of making personal data inaccessible and non-reusable in any way for the relevant users. Data controller Crowne Plaza Istanbul Asia Hotel has fulfilled its obligation to take all necessary technical and administrative measures to ensure that deleted personal data is inaccessible and non-reusable for the relevant users.

Since personal data can be stored in various recording media, they must be deleted by methods appropriate to the recording media. Examples of this are given below:

8.1.1. Application-as-a-Service Type Cloud Solutions (such as Office 365, Salesforce, Dropbox)

In the cloud system, data is deleted by issuing a delete command. During the aforementioned process, the relevant user is not authorized to restore the deleted data on the cloud system.

8.1.2. Personal Data on Paper Media

Blackout is done by cutting out the personal data on the relevant document, where possible, and making it invisible to the relevant users by using fixed ink in a way that cannot be reversed and cannot be read by technological solutions.

8.1.3. 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 are removed on the file or the directory where the file is located. While performing the aforementioned operation, it is ensured that the user concerned is not also the system administrator.

8.1.4. Personal Data on Portable Media

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

8.1.5. Databases

The relevant rows containing personal data are deleted with database commands (delete, alter, etc.). While performing the aforementioned operation, it is ensured that the relevant user is not also the database administrator.

8.1.6. Methods Used by Our Company

8.1.6.1. For Personal Data on Paper Media Blackout is performed by cutting out the personal data on the relevant document, where possible, and making it invisible to the relevant users by using fixed ink in a way that cannot be reversed and cannot be read with technological solutions.

8.1.6.2. For 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 are removed on the file or the directory where the file is located. While performing the aforementioned operation, it is ensured that the relevant user is not also the system administrator.

8.1.6.3. For Personal Data on Portable Media, personal data on Flash-based storage media are deleted using software suitable for these media.

8.1.6.5. For Personal Data in Databases, the relevant rows containing personal data are deleted with database commands (delete, alter, drop, etc.). While performing the aforementioned operation, it is ensured that the relevant user is not also the database administrator.

8.2. Destruction of Personal Data

Destruction of personal data is the process of making personal data inaccessible, unrecoverable and non-reusable by anyone in any way. Data controller Crowne Plaza Istanbul Asia Hotel has fulfilled its obligation to take all necessary technical and administrative measures regarding the destruction of personal data.

For the destruction of personal data, all copies containing the data are identified and the process is carried out one by one by using one or more of the following methods depending on the type of systems where the data is located

8.2.1. Local Systems

One or more of the following methods are used to destroy the data on these systems.

- **Physical Disposal**

  The process of physically destroying optical media and magnetic media, such as melting, burning or

pulverizing. By melting, burning, pulverizing or passing optical or magnetic media through a metal grinder, the data is rendered inaccessible.

In the case of solid state disks, if overwriting or de-magnetizing 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 is done using specialized software.

8.2.2. Environmental Systems

Depending on the type of media, the destruction methods used are listed below;

- **Network devices (switch, router, etc.)**

  The storage media inside these devices are fixed. The products often have a delete command but not a destroy feature. They are destroyed using one or more of the appropriate methods specified in local systems.

- **Flash-based environments**

  Flash-based hard disks with ATA (SATA, PATA, etc.), SCSI (SCSI Express, etc.) interfaces are destroyed by using the 'block erase' command if supported, or the manufacturer's recommended destruction method if not supported, or one or more of the appropriate methods specified in local systems.

- **Mobile phones (Sim card and fixed memory space)**

  Hard memory spaces in portable smartphones have a delete command, but most do not have a destroy command. They are destroyed using one or more of the appropriate local methods. Sim cards are physically rendered unusable.

- **Optical disks**

  Data storage media such as CDs and DVDs. They are destroyed by physical destruction methods such as incineration, fragmentation, melting.

- **Peripherals such as printers with removable data recording media, fingerprint door access system**

  All data recording media are verified to be removed and destroyed using one or more of the appropriate methods specified in the local systems according to their characteristics.

- **Peripherals such as printer, fingerprint door access system with fixed data recording media**

  Most of these systems have a delete command, but not a destroy command. They are destroyed using one or more of the appropriate methods specified locally.

8.2.3. Paper and Microfiche Media

As the personal data on such media is permanently and physically written on the media, the main media is destroyed. During this process, it is necessary to shred the media with paper shredding or shredding machines into small pieces of incomprehensible size that cannot be reassembled.

Personal data transferred from the original paper format to electronic media through scanning are destroyed using one or more of the methods specified in local systems depending on the electronic media in which they are located.

8.2.4. Methods Used by Our Company

- **Optical disks**

  It is destroyed by physical destruction methods such as incineration, fragmentation and melting.

- **Paper and Microfiche Media**

  Since the personal data on such media is permanently and physically written on the media, the main media is destroyed. While this process is being carried out, the media is divided into incomprehensibly small pieces that cannot be reassembled by paper shredding or shredding procedures.

8.3. Anonymization of Personal Data

Anonymization of personal data means making personal data impossible to be associated with an identified or identifiable natural person under any circumstances, even if the personal data is matched with other data. In order for personal data to be anonymized; personal data must be rendered unassociable with an identified or identifiable natural person even through the use of appropriate techniques for the recording environment and the relevant field of activity, such as the return of personal data by the data controller or third parties and / or matching the data with other data. As the Data Controller, we do not currently use the method of anonymization of personal data. In case such destruction method is used, necessary updates will be made by us in our Storage and Destruction Policy.

9. EMPLOYEE (INCLUDED IN THE PERSONAL DATA RETENTION AND DESTRUCTION POLICY) TITLE, DEPARTMENT AND DUTY LIST

All units and employees of the Data Controller actively support the responsible units in taking technical and

administrative measures to ensure data security in all environments where personal data is processed in order to prevent unlawful processing of personal data, to prevent unlawful access to personal data and to ensure that personal data is stored in accordance with the law, by properly implementing the technical and administrative measures taken by the responsible units within the scope of the Policy, training and raising awareness of the unit employees, monitoring and continuous supervision.

The distribution of the titles, units and job descriptions of those involved in the storage and destruction of personal data is given in the table below.

STAFF TITLE AND UNIT	POSITION	RESPONSIBILITY
LAWYER LEGAL DEPARTMENT	PERSONAL DATA STORAGE AND DESTRUCTION POLICY APPLICATION RESPONSIBLE	ENSURING COMPLIANCE WITH THE RETENTION PERIOD OF DATA AND MANAGING THE DESTRUCTION PROCESS WITHIN THE PERIODIC DESTRUCTION PERIOD
INFORMATION TECHNOLOGIES MANAGER INFORMATION TECHNOLOGIES	INFORMATION TECHNOLOGIES DEPERTMANI PERSONAL DATA STORAGE AND DESTRUCTION POLICY APPLICATION RESPONSIBLE	ENSURING COMPLIANCE WITH THE RETENTION PERIOD OF DATA AND MANAGING THE DESTRUCTION PROCESS WITHIN THE PERIODIC DESTRUCTION PERIOD
ACCOUNTING MANAGER ACCOUNTING	FINANCIAL AFFAIRS DEPARTMENT PERSONAL DATA STORAGE AND DESTRUCTION POLICY APPLICATION RESPONSIBLE	ENSURING COMPLIANCE WITH THE RETENTION PERIOD OF DATA AND MANAGING THE DESTRUCTION PROCESS WITHIN THE PERIODIC DESTRUCTION PERIOD
HUMAN RESOURCES MANAGER HUMAN RESOURCES	HUMAN RESOURCES DEPARTMENT PERSONAL DATA STORAGE AND DESTRUCTION POLICY APPLICATION RESPONSIBLE	ENSURING COMPLIANCE WITH THE RETENTION PERIOD OF DATA AND MANAGING THE DESTRUCTION PROCESS WITHIN THE PERIODIC DESTRUCTION PERIOD
OTHER DEPARTMENT MANAGERS	DEPARTMENTS RESPONSIBLE FOR IMPLEMENTING THE PERSONAL DATA RETENTION AND DESTRUCTION POLICY	ENSURING COMPLIANCE WITH THE RETENTION PERIOD OF DATA AND MANAGING THE DESTRUCTION PROCESS WITHIN THE PERIODIC DESTRUCTION PERIOD

10. TABLE OF STORAGE AND DISPOSAL PERIODS

Regarding the personal data processed by the Company within the scope of the activities;

- Retention periods on the basis of personal data related to all personal data within the scope of activities carried out under the departments are as in the Personal Data Processing Inventory.
- Retention periods on the basis of data categories are included in the registration to VERBIS. Below is the Retention and Destruction Table created on the basis of processes.

STORAGE AND DISPOSAL TABLE

ACTIVITY	STORAGE DURATION	DISPOSAL DURATION
CONTRACT PROCESSES	Duration of Legal Relationship + 10 Years	At the first periodic destruction following the end of the storage period

GENERAL ASSEMBLY MEETING PROCESSES	Duration of Legal Relationship + 10 Years	At the first periodic destruction following the end of the storage period
CAMERA RECORDING	1 Month	By writing on it at the end of the storage period
LOG RECORD TRACKING SYSTEMS	2 Years	At the first periodic destruction following the end of the storage period
EXECUTION OF HUMAN RESOURCES PROCESSES	10 YEARS Following the Termination of the Activity	At the first periodic destruction following the end of the storage period
OCCUPATIONAL HEALTH AND SAFETY	Duration of Legal Relationship + 15 Years	At the first periodic destruction following the end of the storage period
TAX AND SSI TRANSACTIONS	Duration of Legal Relationship + 10 Years	At the first periodic destruction following the end of the storage period
DISCIPLINARY REGULATIONS PENALTY DATA	Duration of Employment Contract + 10 Years	At the first periodic destruction following the end of the storage period
DATA PROCESSING PROCESSES FOR THE HOST	Duration of Legal Relationship + 10 Years	At the first periodic destruction following the end of the storage period
PAYSLIP	Duration of Legal Relationship + 10 Years	At the first periodic destruction following the end of the storage period
RECRUITMENT ACTIVITY	Duration of Legal Relationship + 2 YEARS	At the first periodic destruction following the end of the storage period

1. UPDATES

The changes made in this policy according to the laws and regulations and the decisions taken by Crowne Plaza Istanbul Asia Hotel, which has the title of data controller, are in the table below.

UPDATE DATE	BASIS	SCOPE OF THE AMENDMENT

2. PERIODIC DESTRUCTION PERIOD

Pursuant to Article 11 of the Regulation, the Authority has set the periodic destruction period as 6 months. Accordingly, periodic destruction is carried out by the data controller in June and December every year.

3. PUBLICATION, STORAGE AND UPDATING OF THE POLICY:

The Policy is stored in two different media, wet signed (printed paper) and electronic media, and published on the website. It is reviewed as needed and the necessary sections are updated.

4. REFERENCE DOCUMENTS

- Law No. 6698 on the Protection of Personal Data,
- Regulation on Deletion, Destruction or Anonymization of Personal Data No. 30224 dated 28.10.2018.

5. ENFORCEMENT

This policy has entered into force as of the date of its publication and is updated annually within the framework of the procedures and principles set out above.