Holiday Inn Istanbul City
Turgut Özal Cad. 189 (Millet Cad.) Topkapı
34280 İstanbul – Turkey
T: +90 (212) 530 99 00 | F: +90 (212) 530 99 24
E: info@hiistanbulcity.com.tr
www.hiistanbulcity.com.tr

HOLIDAY INN ISTANBUL CİTY OLCAY TURİZM SANAYİ VE TİCARET A.Ş.
POLICY OF PROTECTION AND PROCESS OF PERSONAL DATA

1. INTRODUCTION

The Law on Protection of Personal Data no 6698 as issued for the purpose of protecting fundamental rights and freedoms primarily the secrecy of private life and to regulate the rules and procedures that the real persons/legal entities that process personal data are obligated to comply with, has entered into force with being published on the official gazette dated 07.04.2016.

The activities that Holiday İnn İstanbul City, Olcay Turizm ve Ticaret A.Ş. executes in processing and protecting Personal Data are regulated under 'Holiday İnn İstanbul City, Olcay Turizm ve Ticaret A.Ş. Personal Data Protection Policy' and the Policy is provided to your access by publishing over www.address of our Company.

2.PURPOSE

The purpose of this Policy is to determine the procedures and rules that our company is subject to in processing personal data, to ensure efficient and orderly execution of the technical and administrative activities performed in protecting data through managing thereof under a Policy, to inform people (employee candidate, employee, intern, hotel guest/guest of the hotel guest, payer of the hotel guest, member, visitor, potential customer, supplier/customer and subemployer officers and employees, member).

2. SCOPE

Policy is related to the personal data located at the systems where data is processed through fully or partially automated or not automated provided that it is a part of any data storage system. The explanations made for 'Personal Data' in the Policy shall also cover 'Special Data'.

3. DEFINITIONS

Company	OLCAY TURİZM SANAYİ VE TİCARET A.Ş.
Explicit consent:	Consent about a specific subject based on information and expressed in free will
Personal Data	Any information related to the identitied or identifiable real person
Personal Data of Special Nature	Data on criminal convictions and security measures, biometric data, nationality, health data etc.
Data Supervisor	Real or legal person who determines the purposes and means of personal data processing and in charge of establishing and managing the data recording system
Data Processor	Real and legal person who processes personal data on behalf of the data supervisor with the authorization invested by the data supervisor
Relevant person	Real person whose personal data are processed

Holiday Inn Istanbul City
Turgut Özal Cad. 189 (Millet Cad.) Topkapı
34280 İstanbul – Turkey
T: +90 (212) 530 99 00 | F: +90 (212) 530 99 24
E: info@hiistanbulcity.com.tr
www.hiistanbulcity.com.tr

Employee	Employees within the framework of the agreement signed with the company
Employee Candidate	Natural persons who applied for a job or submitted their CV / information to the company
Intern	People that are interns in the Company
Intern Candidate	Persons who have applied to the company for an internship and have opened their resume and other relevant information for review.
Hotel Guest and Gues of the Hotel Guest	People staying at Holıday Inn İstanbul City and benefiting from the products and services of the company
Member	Members of IHG Rewards Club Card created for providing advantages to the hotel guests such as general/special campaigns, promotions, discounts, gifts that the InterContinental Hotels Group ("IHG") to which Holiday Inn Istanbul City is included and the members of SPA Center within Holiday Inn Istanbul City
Visitor	Natural persons visiting the physical premises where the Company operates or website thereof
Supplier	Third parties with whom the company is in contractual relationship and providing products / services to the company
Potential Customer	Prospective customers who want to buy products or services from the company
Customer	Third party / legal entities to which the Company provides products and services within the contractual relationship
Third Person	Real persons whose personal data is processed (Employees Family (Spouse and Child Information, Person Paying on behalf of Hotel Guest)
Data Supervisor Representative	means the Data Supervisor Representative appointed for the Company as per article 11/3 of 'Regulation on Data Supervisor Registry' which was published on the Official Gazette dated 30.12.2017 and numbered 30286 and which entered into force on 01.01.2018
Contact Representative	means the Contact Representative appointed for the Company as per article 11/4 of 'Regulation on Data Supervisor Registry' which was published on the Official Gazette dated 30.12.2017 and numbered 30286 and which entered into force on 01.01.2018
LAW ON THE PROTECTION OF PERSONAL DATA (LPPD)	Law on Protection of Personal Data no 6698 as published on the Official Gazette dated 07.04.2016 and numbered 29677 and entered into force on 24.03.2016
Protection of Personal Data Board	Protection of Personal Data Board
PDP Institution	Personal Data Protection Authority

Policy	Personal Data Protection and Processing Policy
Application Form	Application Form to be used by the Person (Data Owner) as Data Supervisor Company in accordance with the Law on the Protection of Personal Data No. 6698.
The processing of personal data	All kinds of processes performed on data including acquisition, recording, storing, retaining, modifying, re-arranging, disclosing, transmission, taking over, making available, classifying or prevention of use through fully or partially automated ways or through non-automated ways, provided that these are part of any data recording system
Erasing of Personal Data	Making personal data inaccessible and reusable by the relevant users.
Destruction of Personal Data	Process of making personal data inaccessible, recoverable and unusable by anyone, in any manner.
Anonymization of Personal Data	Making personal data unlikely to be associated with any identified or identifiable real person in any way, even when paired with other data
Data Recording system	Recording system in which personal data is structured and processed according to certain criteria

4. EXECUTION OF POLICY AND RESPONSIBILITIES

5.1 'Olcay Turizm ve Ticaret A.Ş is responsible for the implementation of this policy as 'Data Supervisor'.
5.2 The Board of Directors of 'Olcay Turizm ve Ticaret A.Ş.' shall be authorized and responsible for the preparation, implementation and updating of the policy.
5.3 I Contact persons (employee, employee candidate, inter, intern candidate, hotel guest / guest of the hotel guest, host, member, visitor, potential customer / customer // supplier / subcontractor officials and employees, third parties (employee relatives (spouse and child)) (the person making the payment on behalf of the hotel guest) are obliged to act in accordance with the policy provisions, to ensure that these provisions are complied with and to notify the Company Data Supervisor Representative in case of any violation.
5.4 The policy has been published on the 'www.hiistanbulcity.com.tr' website and is also made accessible by uploading to common data processing systems.
5.5 Updates to the policy will be made accessible by the Board of Directors either on the Company's web address or on the common data processing system.
5.6 In the event of a conflict between the policy and the existing provisions of the law, the provisions of the law shall prevail and the Board of Directors of the Company shall make the necessary update available to bring the policy in line with the provisions of the law.
5.7 The authority to decide the repeal of the policy; belongs to the board of directors.

6. PRINCIPLES OF PERSONAL DATA PROCESSING

6.1. The General Principles in Processing of Personal Data

Personal data are processed in accordance with LPPD Law No. 6698 and secondary regulations in accordance with the procedures and principles stipulated in this Policy.

The Company follows the following principles in the processing of personal data:

6.1.1 Processing compliance with the Rule of Law and Good Faith

Personal Data is processed in accordance with applicable legal regulations and rule o good faith. The Company considers the proportionality requirements in the processing of personal data and does not use the personal data for purposes other than purposes of processing.

6.1.2 Accuracy and up to date

The necessary measures are taken in the collection and processing of personal data and their accuracy is ensured and an opportunity is given to the relevant persons to update their personal data.

6.1.3 Processing for Specific, Clear and Legitimate Purposes

The purpose of the personal data processing is determined by the Company in a clear and precise manner and the data is processed in connection with the services provided by the group and as required for them.

6.1.4 Being Connected, Limited and Proportionate to the Purpose of Processing

Personal data and processing purposes are categorized by the Company 'Data Inventory' and the processing of data that is not related to the achievement of the objectives is avoided.

6.1.5. Maintaining for the time required for the purpose foreseen in the relevant legislation or for the purposes for which it is being processed

The Company maintains personal data only for the period required by the relevant legislation and for the purpose for which it was processed. In determining the storage periods, firstly, it is determined whether a period for the storage of personal data is stipulated in the related legislation and if a period is determined, this period is complied with, and if a period is not determined, legal and criminal statute of limitations shall be taken into consideration and the personal data shall be kept for the time required for the purpose for which it was processed. Personal data is deleted or destroyed if the period is expired or the reasons for the processing of the personal data disappear. In case of changes in the data processing periods, new determined periods are taken as basis.

7. TERMS OF PROCESSING OF PERSONAL DATA

In the processing of personal data, the Company complies with the personal data processing terms stated in Article 5 of the LPPD no. 6698.

7.1. Presence of Explicit Consent of the Person Concerned

According to LPPD no. 6698, the basic reason for compliance with the law regarding the processing of personal data is 'Explicit Consent'. Explicit Consent refers to the consent of the person on a particular subject, which is based on information and is disclosed at will.

In processing of personal data by the Company, it is primarily determined whether the 'data processing terms' stated in paragraph 2 of article 5 and paragraph 3 of article 6 in LPPD no 6698 are present and if any of these terms are absent, the personal data processing shall be performed based on 'explicit consent' received from the relevant person with regards to data processing activity.

7.2. Clear Prediction of Processing in Laws

If clearly stipulated in the legislation, the personal data of the person concerned may be processed in accordance with the law without 'explicit consent'.

7.3. Failure to Obtain the Explicit Consent of the Related Person Due to Actual Impossibility

Personal data may be processed without explicit consent if it is necessary to process personal data in order to protect the life and body integrity of the person who is unable to disclose his consent due to actual impossibility or whose consent is not granted legal validity.

7.4. Obligation to Process Personal Data of the Parties to the Agreement, provided that it is directly related to the establishment and execution of an Agreement

In transactions that are directly related to the establishment of the agreement or the performance of the contractual debt, personal data may be processed without explicit consent.

7.5. Obligation of Personal Data Processing by Data Supervisor to fulfill his Legal Obligation

Where data processing is stipulated as obligatory in the legislation, personal data may be processed to fulfill the legal obligation of the Company.

7.6. Publication of Personal Data by the Person concerned

If the person (Data owner) has publicized his personal data, such data may be processed by the Company Group.

7.7 Obligation of Data Processing to Establish, Use or Protect a Right

Where personal data processing is compulsory for the establishment, use or protection of a right, the data may be processed without the explicit consent of the person concerned.

7.8 Obligation to process data for the legitimate interests of the data supervisor

Personal data may be processed for the legitimate interests of the Data Supervisor Company in cases where personal data processing is obligatory, provided that no harm is caused to the fundamental rights and freedoms of the relevant people.

8. PURPOSE OF PROCESSING PERSONAL DATA

Within the scope of LPPD no 6698 and relevant legislation, the Company may process personal data limited to the purposes stated below and in compliance with the "General Principles" in article 4 of LPPD, "Personal Data Processing Terms" in article 5 and "Terms for Processing Personal Data with Special Nature"in article 6.

The Company shall process the personal data as determined below;

• For our relevant business units to perform the works necessary for you to enjoy the products and services of Holiday Inn Istanbul City, to offer you with various room options in line with the preferences that you notify us, to manage your hotel reservations and accommodation processes, to monitor your use of services

• Performing the payment transactions related to the services and products we offer, execution of the obligations necessary as per E-Archive legislation, management of the objection processes related to your payments, performance of the obligation to inform the authorized institutions and organizations in line with your objections

Holiday Inn Istanbul City
Turgut Özal Cad. 189 (Millet Cad.) Topkapı
34280 İstanbul – Turkey
T: +90 (212) 530 99 00 | F: +90 (212) 530 99 24
E: info@hiistanbulcity.com.tr
www.hiistanbulcity.com.tr

• In case there is an Explicit Consent, to perform the IHG Rewards Club card membership that the InterContinental Hotels Group ("IHG") offers, within the scope of your membership, to manage your reservations in the hotels within the IHG Group, to ensure you enjoy the campaigns, discounts, promotions and gifts in your accommodations/in the extras you benefit, to send commercial electronic messages for the InterContinental Hotels Group ("IHG") to contact you for advertisement, sales, marketing, promotion, discount, membership terms, introduction and informing

• In case there is an Explicit Consent, to inform, direct you abour all products and services offered in our hotel and its units, to offer you advantages/benefits such as advertisements, sales, marketing, campaign, promotion, discount, membership terms and to send you commercial electronic messages for these purposes

• Within the scope of organization and event management, to establish Corporate Communication for the Events and Organizations Planned to be Held at the Units in the Hotel, to provide Offers, to Record Potential Customers, to Monitor and Execute the Agreement Processes with the Customers With Regards to the Agreed Event and Organizations,

• Measuring and increasing customer / visitor satisfaction, demand / complaint management, developing and diversifying our services in line with your requests and needs, and conducting necessary quality and standard audits

• In case there is an Explicit Consent, to send satisfaction survey to you within the scope of measuring customer satisfaction by our Hotel and InterContinental Hotels Group ("IHG"), for our company to contact you to ask whether the satisfaction survey is sent, to perform listing, reporting, statistics and analysis works for increasing the personal preference options with regards to the methods of use of the product and services presented by our hotel and affiliated units and to develop our products and services in connection with this

• Ensuring the security of life and property and legal, commercial and occupational health of real and / or legal third party institutions and organizations (employees, guests, visitors, customers, suppliers, etc.) in our hotel and its affiliated units

• Establishment, Management and Communication of Relations with Customer / Potential Customer / Suppliers (Authorized and Employee), Follow-up of Agreement Processes and Obtain Financial Consensus, Execution of Legal, Commercial and Administrative Obligations Arising from Agreements

• Planning and Execution of the Company's Commercial and / or Business Strategies

• Execution of Management Activities

• Execution of finance and accounting transactions

• Execution of Human Resources Process and Policies

• Fulfillment of Obligations Arising from Labour Law, Social Security Law, Occupational Health and Safety Law and Other Legislation for Employees

• Monitoring Employee Assignment Processes, Workplace Entry and Exit, Employee Rights and Benefits Processes

• Conducting Internal Audit / Investigation / Intelligence Activities

• Planning and execution of emergency management processes,

• Management of Legal Operations

•Planning, control and execution of information security processes

• Recording of In-Hotel Internet Access Logs in accordance with Law No. 5651

• Performance of Information Securing, Reporting Obligations foreseen by the Official Institutions and the Information and Document Requests made by Official Institutions, Judicial Organs and/or Administrative Authorities

• Giving information to the authorized institutions and organizations due to legal obligation and / or performing
the activities and obligations related to the audit

• Taking necessary technical, legal and administrative measures within the scope of data security
and may be processes within the personal data process terms and purposes stated in article 5 and 6 of Law no 6698.

Holiday Inn Istanbul City
Turgut Özal Cad. 189 (Millet Cad.) Topkapı
34280 İstanbul – Turkey
T: +90 (212) 530 99 00 | F: +90 (212) 530 99 24
E: info@hiistanbulcity.com.tr
www.hiistanbulcity.com.tr

9. PROCESSING PURPOSES OF PERSONAL DATA WITH SPECIAL NATURE AND METHODS OF PROTECTION

9.1. Purposes of Processing Data with Special Nature

As per article 6/1 of LPPD no 6698; 'data of the people related to race, ethnicity, political opinion, philosophical belief, religion, sect or other beliefs, clothing, membership to foundations, association or union, health, sexual life, criminal conviction and data related to judicial measures and the biometric and genetic data' are personal data with special nature.

Data with special nature are processed under the terms below within the scope of 'Terms for Processing Personal Data with Special Nature' determined in article 6 of LPPD no 6698, with taking the measures determined by Personal Data Protection Board with regards to protection of these data:

•If the Personal Data Owner's Explicit Consent is present,

• If the Personal Data Owner's Explicit Consent is absent, the personal data other than Health and sexual life shall be processed under the terms foreseen in the law, the personal data related to Health and sexual life can only be processed under the legislation in cases where there is an obligation to protect public health, preventive medicine, medical diagnosis, treatment and caretaking services, planning and managing healthcare services and financing and also in cases where there is a confidentiality obligation.

9.2. Protection Methods for Data with Special Nature

Pursuant to the Resolution of the Personal Data Protection Board dated 31/01/2018 and numbered 2018/10;

A separate systematic, manageable and sustainable policy and procedure for the security of private personal data has been determined.

For employees involved in the processing of Personal Data with Special Nature,

• Regular training is provided in topics such as Laws and related regulations and Security of Personal Data with Special Nature,

• Confidentiality agreements are made,

• A clear definition of the scope and duration of authorization of users who have the authorization to access to data,

• Authorization checks are performed periodically,

• The authority of the employees who have changed their jobs or leave their jobs in this field is immediately removed and the inventory assigned to them is returned,

If the medium where personal data with special nature are processes, maintained and / or accessed are electronic medium;

• Data is kept using cryptographic methods,

• Cryptographic keys are kept in secure and different environments,

• All transaction logs performed on the data are logged securely,

• The security updates of the data environments are continuously monitored, the necessary security tests are regularly conducted / performed, the test results are recorded,

• If the data is accessed through a software, user authorizations for this software are performed, security tests of these software are performed regularly and test results are recorded,

• If remote access to data is required, at least two-level authentication system is provided,

If the medium where personal data with special nature are processes, maintained and / or accessed are physical medium;

Sufficient security measures are taken according to the nature of the medium in which the Personal Data with Special Nature are stored (against electricity leaks, fire, flood, theft etc.)

• By ensuring the physical security of these environments, unauthorized entry and exit is prevented,

If Personal Data with Special Nature is going to be transferred;

• If the data is needed to be transferred via e-mail, it is ensured that they are transferred by using encrypted corporate e-mail address or Registered Electronic Email (REM) account,

• If it is needed to be transferred via media such as portable memory, CD, DVD, it shall be realized by cryptographic encoding and the cryptographic key shall be kept in a different environment,

•If it is transferred between servers in different physical environments, the performance of transferring data by establishing a VPN between servers or by using sFTP method,

• If data needs to be transferred via paper, necessary measures are taken against risks such as theft, loss or sighting of unauthorized persons and the documents are sent in "confidential documents" format.

In addition to the above-mentioned measures, technical and administrative measures to ensure the appropriate level of security specified in the Personal Data Security Guidelines published on the website of the Personal Data Protection Institution are also taken into consideration.

10. Transfer of Personal Data
10.1. Domestic Data Transfer

The Company may transfer the personal data to third parties in line with the legitimate and lawful personal data processing purposes stated in paragraph 8 of the policy and based on one of more personal data processing terms stated in article 5 of LPPD and within the scope of the regulation foreseen in article 8 of LPPD:

• If the Personal Data Owner's Explicit Consent is present,

• If there is a special regulation in the law that personal data will be transferred,

• If the personal data holder is obliged to protect the life or body integrity of the owner or someone else and the personal data holder is unable to disclose his consent due to the actual impossibility,

• In case the processing of personal data belonging to the parties of an agreement is necessary, provided that it shall be directly related to the conclusion or fulfillment of such agreement,

• Should personal data transfer is mandatory for our Company to fulfill its legal obligation,

• In case the Personal data is made available to the public by the personal data owner,

• In case the personal data transfer is mandatory for the establishment, exercise or protection of any right,

• Personal data may be transferred if data transfer is mandatory for the legitimate interests of the Company, provided that it does not harm the fundamental rights and freedoms of the personal data holder.

10.2. Transferring Personal Data Abroad
10.2.1 Obtaining the explicit consent of the person concerned for the transfer of personal data abroad

Pursuant to Article 9 of LPPD No. 6698, 'Personal data cannot be transferred abroad without the explicit consent of the person concerned.' When the personal data needs to be transferred abroad by the Company, firstly, it is determined whether one of the conditions listed in article 5 of the law are present, if any of these conditions are absent, the personal data may be transferred abroad with taking the explicit consent.

10.2.2 Transfer of Personal Data Provided that the Conditions for the Processing of Personal Data are met, even if the Person concerned does not provide explicit consent

The personal data may be transferred abroad without explicit consent if if any of the following conditions stated in paragraph two of article 5 of LPPD no 6698 and that are written below are present;

• In case it is clearly stated in law,

• The fact that the person who cannot explain his consent due to the actual impossibility or who is not legally valid at his/her discretion is obliged to protect the life or body integrity of the person himself or someone else,
• The requirement of transfer of personal data belonging to the parties of an agreement is necessary, provided that it is directly related to the conclusion or fulfillment of that agreement,
• Mandatory for the company to fulfill its legal obligations,
• Publicity of the personal data with special quality by the relevant person,
• In the event that data processing is obligatory for the establishment, use or protection of a right,
• Provided that it does not harm the fundamental rights and freedoms of the person concerned, it is an obligation to transfer data for legitimate interests of the data supervisor
and if

the following are present in the foreign country to which the personal data is going to be transferred;

a) Adequate protection,

b) In the absence of adequate protection is not an adequate protection of the consent of the Board of Protection of Personal Data, and to commit themselves in writing to the responsible data in Turkey and in the relevant foreign country

.

10.3. Transfer of Data of Special Nature

10.3.1. Transferring Data with Special Nature into the Country

In accordance with the regulation provided for in Article 8 of the LPPD,

A) In cases where explicit consent is required, by obtaining explicit consent in accordance with Article 8, paragraph 1,

B) In case of the existence of one of the conditions mentioned in the second paragraph of Article 5, without explicit consent,

C) With taking sufficient measures, the Company may domestically transfer without explicit consent under the terms stated in paragraph 3 of article 6 as below;

• Personal data other than health and sexual life (race, ethnicity, political thought, philosophical belief, religion, sect or other beliefs, clothing, association, foundation or union membership, criminal convictions and security measures and biometric and genetic data) in conditions foreseen by law,

• The data relating to health and sexual life, only within the scope of processing by the authorized institutions and organizations and the persons under the obligation of keeping secret for planning and managing the financing planning and healthcare services and executing protective medicine, medical diagnosis, treatment and care services and protecting public health.

10.3.2. Transferring Personal Data to Abroad

The personal data may be transferred abroad by the Company Pursuant to Article 9 of the LPPD no. 6698

• By obtaining explicit consent in cases requiring explicit consent,

• In the event of the existence of any of the conditions stated in the second paragraph of Article 5 of the Law, without explicit consent,

• Without explicit consent in the presence of any of the conditions specified in paragraph 3 of Article 6, provided that adequate measures are taken, and the following are present in the foreign country to which the personal data is going to be transferred;

a) Adequate protection,

b) In the absence of adequate protection is not an adequate protection of the consent of the Board of Protection of Personal Data, and to commit themselves in writing to the responsible data in Turkey and in the relevant foreign country,

.

10.4. Categorization of Personal Data

In accordance with enlightenment obligation Article 10 of the LPPD, the Company has disclosed below the personal data owner in order to inform the personal data holder which groups of personal data holders are under the obligation of disclosure:

CATEGORIZATION OF PERSONAL DATA

Identity Information	Information such as Name-Surname, TR ID No, Nationality, Mother's name, Father's name, Place of Birth, Date of Birth, Marital Status, Sex, Place of Registry, Volume No, Family Row No, Row No, SSI Registration No, Religion, Tax No, ID No, passport no which are explicitly understood to belong to a real person with determined or determinable identity, which are processed with partial or full automated systems or as non-automated as a part of data recording system, which are related to the identity of the person
Contact information	Information such as telephone number, address, e-mail address, which is clearly owned by an identifiable or identifiable natural person
Family members and emergency contact information	Information about family members (spouses and children) relatives and other persons that can be reached in case of emergency (Name-Surname, Mobile phone) in order to protect the legal and other interests of the personal data holder of the Company, which are explicitly belonging to a identified or identifiable real person
Financial Information	The bank account number, IBAN number, invoice, check, promissory note data taken in relation to the legal relationship established by the Company's personal data owner, which is clearly owned by an identified or identifiable real person
Personal Information	Any personally identifiable or personally identifiable personal data processed to obtain information that would be the basis for the creation of personal rights of natural persons in a service relationship with the Company
Professional Experience	Diploma information, courses attended, vocational training information, certificates that clearly belong to an identified or identifiable real person
Biometric Data	Fingerprint Information, face recognition information etc.
Personal Data of Special Nature	Data stated in Article 6 of the LPPD (Health data, Blood type, Data on Criminal Conviction and Security measures, National data), which clearly belong to an identified or identifiable real person.
Audio/Visual Information	Photo and camera record data that clearly belong to an identified or identifiable real person

Holiday Inn Istanbul City
Turgut Özal Cad. 189 (Millet Cad.) Topkapı
34280 İstanbul – Turkey
T: +90 (212) 530 99 00 | F: +90 (212) 530 99 24
E: info@hiistanbulcity.com.tr
www.hiistanbulcity.com.tr

Nationality	Nationality
Transaction security	IP Address Information, Website Login and Exit Information, password and password information
Legal transaction	Correspondence with the judicial authorities, information in the case file, etc.
Criminal Conviction and Security Measures	Data on criminal convictions and security measures received from persons working in the company
Customer Transaction	Invoice, check, demand information for customers who purchase products or services from the company
Marketing Information	Information about the products and services offered by the company, personal data processed for marketing and promotion by determining the usage habits, preferences, satisfaction and needs of the personal data owners and the reports prepared about this data
Claim / Complaint Management Information	Data for receiving and evaluating any complaints / requests addressed to the Company, which are clearly owned by an identified or identifiable real person, processed in part or completely automatically or non-automatically as part of the data recording system.
Physical Area Security Information	Information about camera records, security records and documents taken during the entrance and stay in the hotel owned by the company

CATEGORIZATION RELATED TO THE OWNERS OF THE PERSONAL DATA PROCESSED BY TIMS GROUP

Personal Data Owner Category Explanation

Employee	Company employees
Employee Candidate	Natural persons who applied for a job or submitted their CV / information to the company
Intern	Interns at the company
Intern Candidate	Persons who have applied to the company for an internship and have opened their resume and other relevant information for review.
Hotel Guest and Guests of the Hotel Guest	Persons staying at the hotel owned by the Company and benefiting from the products and services offered by the hotel

Potential Customer	Prospective customers who want to receive services from the company
Customer Company Officer (s)	Authorities and employees / subcontractors and employees of third party legal entities to whom the Company provides products or services within the contractual relationship
Customer	Third parties to whom the Company provides products or services in a contractual relationship
Supplier Company Officer / Employees	Real persons, including officials / employees of the supplier company and its subcontractors providing goods or services to the company
Supplier	In carrying out the activities of the Company, it defines the person who provides services to the Company on an agreement basis in accordance with the orders and instructions of the Company.
3rd person	Real persons whose personal data is processed (Employees Family (Spouse and Child Information, Person Paying on behalf of Hotel Guest)
Visitor	Natural persons visiting the physical premises where the Company operates or website thereof

10.6 PEOPLE TO WHO THE COMPANY TRANSFERS PERSONAL DATA

In accordance with Article 10 of the LPPD, Company informs the personal data owner of the groups of persons to whom personal data are transferred.

The Company may transfer the personal data of the personal data holders managed under the policy in accordance with Articles 8 and 9 of the LPPD to the following categories of persons:

- Company customers / subcontractors,
- Company suppliers / subcontractors,
- In case of explicit consent, to the foreign InterContinental Hotels Group to which the Holiday Inn hotels are affiliated with
- to legally authorized public institutions and organizations, administrative authorities

11. METHOD OF COLLECTING PERSONAL DATA AND LEGAL REASON

Your personal data can be collected orally, in writing or electronically through our hotel and its affiliates, company website, call center and suppliers for the purposes of personal data processing specified in this enlightenment text.

12. OBLIGATIONS OF THE COMPANY WITH DATA SUPERVISOR STATUS

The company shall inform the relevant people through the authorized people during acquiring personal data about the information below;

- Identification of data supervisor or its representative, if any,
- For what purpose the personal data is to be processed,

- To whom and what purpose the processed personal data shall be transferred,
- Method and legal reason of collecting personal data,
- Other rights listed in Article 11

13. RIGHTS OF THE RELEVANT PERSON
13.1 Enlightening the Personal Data Owner

The Company informs the persons concerned about the method of collection of personal data and the legal reasons, the purpose of processing the personal data, to whom and for what purpose the personal data can be processed and the rights of the personal data holder listed in Article 11 of the LPPD.

13.2 Rights of the Personal Data Holder under LPPD

Without prejudice to the conditions provided for in Article 28 titled 'Exceptions' of the LPPD, in accordance with Article 11 of the Law, the persons concerned are entitle to apply to the Company and request the following related to the personal data;

- Learn whether your personal data is processed,
- If processed, request information to be provided,
- To learn the purpose of processing and whether it is used in accordance with this purpose,
- Knowing the third parties to whom your personal data has been transferred inside or outside the country,
- To request correction if it is incomplete or incorrectly processed,
- To request the deletion or destruction of personal data in accordance with the provisions of Article 7 of the Law,
- To request notification of the operations carried out in compliance with subparagraphs (d) and (e) to third parties to whom his personal data has been transferred,
- Object to a detrimental result due to analysis with exclusive automated systems,
- To claim damages if you incur losses due to unlawful processing of your personal data.

13.3. Exercise of Rights by Personal Data Owner

The Company shows how the relevant people will use their rights and the applications may be done in writing or in electronic medium with the methods stated below after filling out the 'Data Owner Application Form' located over the address www.hiistanbulcity.com.tr.

In case of a written request;

A signed original copy of the Data Owner Application Form shall be submitted to 'Turgut özal Millet cad. No:189 Topkapı/Fatih/İSTANBUL address personally with a document showing your identity or as a representative with a power of attorney showing that you have the power to apply with regards to rights listed in article 11 and that is approved by the notary public or through notary or return receipt mail to the address of the company at Turgut özal Millet cad. No:189 Topkapı/Fatih/İSTANBUL address.

In case of electronic request;

You may sign the Personal Data Holder Application Form with an electronic or mobile signature with a "secure electronic signature" certificate defined in the Electronic Signature Law No. 5070, and send it to our company's Registered Electronic Mail address (REM) olcayturizm@hs04.kep.tr or info@hiistanbulcity.com.tr' mail address.

13.4 Company Application Response Time

The requests you submit to the Company are responded to in writing or electronically as soon as possible and within thirty days at the latest according to the nature of your request, in return for the transaction fee specified in Article 7 of the Communiqué on the Principles and Procedures of Application to the Data Supervisor.

14. ENSURING SECURITY OF PERSONAL DATA

14.1 Technical Measures to Ensure the Legal Processing of Personal Data

• The Company undertakes all necessary technical measures to ensure the proper level of security in order to prevent unlawful processing of personal data, to prevent unlawful access to personal data, and to carry out the necessary audits or to perform the necessary audits.

• As per article 11/3 of 'Regulation on the Data Supervisor Registry' which was published on the Official Gazette dated 30.12.2017 and numbered 30286 and entered into force on 01.01.2018, a 'Data Supervisor Representative' was appointed within the company in order to determine the purpose and methods of Personal Data processing, monitoring and auditing Data Processing Procedures, efficiently performing the obligations under LPPD and secondary regulations, following the developments and administrative activities for ensuring security level in line with the protection of Personal Data in accordance with LPPD procedures, taking technical and administrative measures for this, and for the purpose of ensuring execution and audit of the Policy.

• Technical personnel are employed in addition to our existing personnel.

• Personal data processing activities are audited by technical systems, and the relevant audit report is reviewed by the Data Supervisor Representative and the Board of Directors and additional technical measures to be taken are determined and implemented immediately.

• Within the scope of the technical measures necessary to be taken under LPPD, agreements in the matter of technical support shall be executed with third persons/institutions for the purpose of analysis of the relevant current infrastructure data security and determining the missing/enhancement points if there is a missing, remedying the relevant missings in line with the roadmap established for the purpose of developing the incompliant areas emerged during the status determination of current data security, establishing the necessary software and equipment for preventing unauthorized outer access of the data and performing the relevant tests.

• The necessary internal procedures regarding the obligations to arise within the scope of Personal Data Protection Board Decisions and secondary regulations are established immediately and related technical measures are prepared and notified to the employees.

14.2 Administrative Measures to Ensure the Legal Processing of Personal Data

The Company's main administrative measures to ensure the legal processing of personal data are as follows:

• Information works to the company employees are held under the Law on Protection of Personal Data no 6698 and the relevant regulations and periodical trainings are provided in this matter.

• Commitments are taken from the employees that, in processing the personal data and personal data of special nature that they became aware of during their service agreements, they will act in accordance with the provisions foreseen in LPPD, that they will not process these other than any purpose within the scope of the legislation and secondary regulations that the Company is subject to and other than the purpose to which the data owner has given explicit consent in matters requiring explicit consent, not to transfer the personal data, without the 'explicit consent' of the personal data owner given to the Company, to domestic and foreign third persons outside the institutions which are obligated to be disclosed with under the law, that these obligations shall continue after the termination of the service contract, in case that personal data are unlawfully processed by any personnel, to forward this incident immediately to the Data Supervisor Representative, and the penalties to be applied in case of such violations are stated in these agreements.

• In the on-going contracts with the data processing person / organizations in the contractual relationship with the Company and in the agreements in progress, the commitments of the data processor in the matters that the personal data transferred to him are not processed outside the purpose and scope of data processing, that they will take all the technical and administrative measures for ensuring the appropriate level of security for allowing the safekeeping of personal data, that they will not disclose the personal data to third persons in violation with the agreement.

• In line with the 'Data Inventory' created by examining the personal data processing activities carried out by the departments of the company, the access of the employees to the personal and special data is regulated by the authority limitation decisions on the basis of the department. The relevant audits are performed by the Data Supervisor Representative.

• Necessary administrative measures are taken according to the implementation costs in order to prevent the safe storage of Personal Data, the unlawful processing, destruction, alteration or deletion of such data.

14.3 Technical Measures to Prevent Unlawful Access to Personal Data

• In order to prevent unlawful unauthorized access to personal data, to prevent unintentional or unauthorized disclosure of such data, technical measures are taken, updated and renewed periodically according to application costs.

• The necessary internal procedures regarding the obligations to arise within the scope of Personal Data Protection Board Decisions and secondary regulations are established immediately and related technical measures are prepared and notified to the employees.

• Software and hardware including virus protection systems and firewalls are installed.

• The access to and the use of the information within the scope of the power given to the employees with the administrative and technical decisions taken for limiting authority.

14.4 Administrative Measures to Prevent Unlawful Access to Personal Data

The main administrative measures taken by the Company to prevent unlawful access to personal data are as follows:

• Administrative decisions regarding the access to and authorization of personal data are taken and implemented, the employees are informed about the relevant decisions and the implementation of the decisions are also audited by the Data Responsible Representative of each company in the group.

• Employees are informed that they will not be able to disclose the personal data they have learned to another person in contradiction to the legislation, they cannot use it for any purpose other than processing purposes, and that this obligation will continue after their resignation and necessary arrangements are made in the service agreements accordingly.

• Interns who do internship in the company are informed that personal data learned in any way during the internship will not be disclosed to the person contrary to the LPPD, that the data cannot be accessed unlawfully, and that the data cannot be used for purposes other than processing and the related commitments are taken from the interns.

• "CONFIDENTIAL" is printed on all pages of confidential documents.

• The 'confidential information' is defined in the service agreements and the commitments from the employees are taken stating that they will show all diligence necessary to keep the confidential information confidential and protect them under the law, that they will not copy and keep this information without the written permit of the Company, that they will not disclose these information in writing, verbally and/or electronically to third parties other than the institutions that the company is obligated to disclose under the legislation provisions, that, in case he becomes aware that the confidential information is disclosed by another employee against the protocol provisions, to immediately inform the officer of the unit in writig, that they will deliver the materials, tools and documents consisting of confidential information to the Company against a delivery record in case the service agreement is terminated.

14.5. Technical Measures to Keep Personal Data in Safe Environments

The main technical measures taken to protect personal data in secure environments are as follows:

- In order to ensure the safe storage of personal data, backup programs are used in a lawful manner.
- Technical personnel are employed in technical matters.
- Servers are maintained in physically secure environments. Unauthorized access is prevented by identifying technical personnel who could access these environments.
- Employees are logged in to the company systems with their user name and password, and employees are trained not to share their user name and password with third parties.
- Continuous updating of operating systems, system software and security software on the server is ensured.
- Server logs (logs) are subject to regular audits and monitoring.
- Access codes for database servers, modems, central, anti-virus program, bulk e-mail software are kept only by the IT Officer.

14.6. Measures to be Taken in Case of Unauthorized Disclosure of Personal Data

- If the personal data processed in accordance with Article 12 of the LPPD is obtained by others through unlawful means, the Company shall be required to carry out the necessary administrative measures to ensure that the data is notified to the 'Data Supervisor Representative', the relevant personal data owner and the PPD Board.

15.1 CAMERA MONITORING AT COMPANY CENTER ADDRESS BUILDING ENTRY AND INTERNAL PARTS

In compliance with the Law on Private Security Services and the relevant legislation, limited to the purposes of Life and Property Safety of the Real Persons and/or Legal Entity Third Party Institutions and Organizations in relation with our company (employees, hotel guests/guests of the hotel guests, visitors, supplier company employees and officers, customer officers and employees, members etc.) and ensuring Legal, Commercial and Occupational Safety and Security, Monitoring the Entry and Exits, the physical security and auditing of the building used by our company, visual recording of general service areas such as the entrance doors, building outer façade of our centre, facilities and businesses, restaurant, cafeteria, lobby, visitor waiting lounge, elevator, car lot, security cabin, floor corridors with security cameras are made. Pursuant to Article 10 of the LPPD, the personal data holder is illuminated by multiple methods of camera monitoring. No monitoring is carried out in areas that may result in interference to individual's privacy by exceeding the security objectives. Only a limited number of employees have access to live camera footage and recordings recorded and stored digitally. A limited number of people having access to the records declare, through the confidentiality commitment, that they will protect the confidentiality of the data they access.

15.2 PROCESSING RECORDS RELATED TO INTERNET ACCESS

For the purpose of ensuring security and the purposes stated in personal data policy, our Company records the log records related the internet access of the hotel guests/guests of the hotel guests, member etc people accommodation in the hotel and affiliated units for the time that they stay in the business as per the mandatory rule of the law no 5651 and the legislation regulated thereunder, and these records are processed in case they are requested by authorized public institutions and organizations or for performing our legal obligations related to the auditing procedures that will be performed within the Company.

16. PERIOD OF STORAGE OF PERSONAL DATA

Personal data is processed in accordance with the data processing and statute of limitations in order to fulfill the related obligations under the laws and secondary regulations, and in case of changes in the data processing periods, new periods are taken as basis.

Holiday Inn Istanbul City
Turgut Özal Cad. 189 (Millet Cad.) Topkapı
34280 İstanbul – Turkey
T: +90 (212) 530 99 00 | F: +90 (212) 530 99 24
E: info@hiistanbulcity.com.tr
www.hiistanbulcity.com.tr

17. DELETION, DESTRUCTION AND ANONYMIZATION OF PERSONAL DATA

In case the causes for processing are no longer present despite they are processed in compliance with LPPD and the other relevant legislation provisions, the necessary administrative measures are taken for deleting, destroying or anonymizing th personal data ex oficio or upon the request of the relevant person, and the works for establishing the technical infrastructure in this matter still continues.

18. UPDATE Updating this Policy shall be performed with a decision to be taken by the Company Board of Directors and shall enter into force. The Company reserves the right to review and update the Policy within the scope of changes in legislation.