SSB TURİZM İNŞAAT İÇ VE DIŞ TİCARET LTD. ŞTİ.

PERSONAL DATA PROCESSING STORAGE AND DESTRUCTION POLICY

Phone	**: +90 (212) 939 4500**
Fax	**: +90 (212) 939 45 15**
Email	**: info.ottomare.istanbul@radissonblu.com**
Address	**: Kazlıçeşme Mah. Abay Cad. No: 223 A Zeytinburnu İstanbul**
Central Registration System Number	**: 07810472554000014**
Tax Office	**: Zeytinburnu**
Tax Number	**: 7810472554**
Trade Register Number	**: 791977**

Table of Contents

1. INTRODUCTION

As SSB TURİZM İNŞAAT İÇ VE DIŞ TİCARET LTD. ŞTİ. ("Company - Radisson Blu Ottomare"), We attach great importance to its processing and protection all kinds of personal data belonging to all persons, including persons, Guests, potential guests, agents, intermediary institutions, suppliers, sub-employers, service providers and managers and employees, business partners, company partners, employees, employee candidates, visitors, interns, employees of public institutions and organizations and private legal entities and related third parties whom we have a legal relationship with in accordance with the Law on Protection of Personal Data numbered 6698 ("LPPD") to be limited to the company's field of activity. For this purpose, our company takes the necessary administrative and technical measures in accordance with the legal regulations and decisions taken.

Numbered 108 The Convention on the Protection of Individuals Against Automatic Processing of Personal Data of Council of Europe which was opened for signature in Strasbourg on January 28, 1981 and entered into force on October 1, 1985 was signed by our country on January 28, 1981. This contract has been included in our domestic law by being published in the Official Gazette dated 17 March 2016 and numbered 29656. Accordingly, the Law on Protection of Personal Data ("LPPD") entered into force after being published in the Official Gazette dated 07.04.2016. It is regulated by the General Data Protection Regulation/Regulation (GDPR) within the scope of the European Union (EU) legislation on the protection of personal data.

Personal Data Protection and Processing and Storage and Destruction Policy and its annexes prepared within the scope of the Personal Data Protection Law No. 6698 and the relevant legislation have been prepared by the data controller ("Company - Radisson Blu Ottomare") within the scope of the personal data protection law numbered 6698 ("law") and the regulation on the deletion, destruction or anonymization of personal data.

2.PURPOSE

With this policy text prepared by our company, ("Company - Radisson Blu Ottomare"), in terms of completing the harmonization process with the PPD Law, in line with the basic principles written below personal data belonging to guests, potential guests, agents, intermediary institutions, suppliers, sub-employers, service providers and managers and employees, business partners, company partners, employees, employee candidates, interns, visitors, employees of public institutions and organizations and private legal entities and related third parties are aimed to be processed in accordance with The decisions published and the principles decided by the PPD Institution, T.R. Constitution, International Conventions, Law No.6698 on the Protection of Personal Data and relevant legislation and the persons concerned are aimed to use their rights effectively. Business and operations related to the storage and destruction of personal data are carried out in accordance with this policy.

3. SCOPE

Personal data belonging to guests, potential guests, agents, intermediary institutions, suppliers, sub-employers, service providers, managers and employees, business partners, company partners, employees, employee candidates, interns, visitors, employees of public institutions and organizations and private law legal entities and related third parties are within the scope of this policy prepared, provided that they are fully or partially automatic in our company or are parts of any data recording system, this policy is applied in the company's activities for the processing of all kinds of personal data, which are processed by non-automatic means, including personal data.

4. ABBREVIATIONS AND DEFINITIONS

ABBREVIATIONS	DEFINITIONS
Explicit Consent	Consent regarding a specific subject, based on information and expressed with free will
Buyer Group	The category of real or legal persons to whom personal data is transferred by the data controller
Anonymization	Making personal data unrelated to an identified or identifiable real person under any circumstances, even by matching other data.
Employee	includes employees of SSB TURİZM İNŞAAT İÇ VE DIŞ TİCARET LTD. ŞTİ.
Employee Candidate	Those who fill out the job application form and apply for a job by using the website or coming to the workplace in person
Electronic Environment	Media where personal data can be created, read, changed and written with electronic devices
Non-Electronic Environment	Other than electronic media, all written, printed, visual, etc. other environments
Provider	Real or legal person providing services under a specific contract with the company
Related User	The 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 the person or unit responsible for the storage, protection and backup of the data technically.
Related Person	Real person whose personal data is processed.
Recording Medium	Any environment in which personal data are processed, which are fully

	or partially in automated ways or non-automated ways provided that being part of any data recording system.
Personal Data	Any information related to the identified or identifiable real person
Personal Data Processing Inventory:	It means the inventory created and elaborated by data controllers by associating personal data processing activities carried out by data controllers depending on the business processes and personal data processing purposes and the legal reason with the data category, the transferred recipient group and the data subject group, and where they explain the maximum retention period required for the purposes for which the personal data is processed, the personal data foreseen to be transferred to foreign countries and the measures taken regarding data security.
The processing of personal data	All kinds of processes performed on personal data including obtaining, recording, storing, keeping, changing, re-arranging, disclosure, transmission, acquisition, making available, classification or prevention of use in whole or in part, automatically or in non-automatic ways, being part of any data recording system
Law	Law No. 6698 on Protection of Personal Data
Board	Personal Data Protection Board
Institution	Personal Data Protection Institution
Personal Data Contact Person	Real person notified during registration to the registry for real and legal persons resident in Turkey by the data controller, for real and legal persons who are not resident in Turkey by the representative of the data controller in order to communicate with the institution regarding their liabilities within the scope of the Law and the secondary regulations to be issued based on this Law,
Anonymization of Personal Data	Making personal data not to be associated with any identified or identifiable real person in any way, even when paired with other data.
Destruction of Personal Data	It refers to the deletion, destruction or anonymization of personal data.
Deleting of Personal Data	The process of making personal data inaccessible and unavailable in any way for relevant users.
Destruction of Personal Data	The process of rendering personal data inaccessible, unrecoverable and unusable by anyone in no way
Sensitive Personal Data	Information about security measures with biometric and genetic data of people with respect to race, ethnicity, political thought, philosophical

	belief, religion, sect or other beliefs, appearance and clothing, membership to an association, foundation or trade union, medical condition, sexual life, criminal conviction
Periodic Destruction	In the event that all the processing conditions of personal data in the Law disappear, the process of erasure, destruction, or anonymization of the personal data that will be carried out at regular intervals specified in the storage and destruction policy.
Policy	Personal Data Processing, Storage and Destruction General Policy
Company	SSB TURİZM İNŞAAT İÇ VE DIŞ TİCARET LTD. ŞTİ.
Data Processor	A real or legal person who processes personal data on his behalf on the basis of the authority conferred by the data officer
Recording system	A recording system in which personal data are structured and processed according to certain criteria.
Data Controller	Real or legal person responsible for identifying the purposes and means of personal data processing, and installing and managing data recording system.
Data Controllers Registry Information System	The information system that data controllers will use in the application to the Registry and in other relevant transactions related to the Registry, accessible on the internet, created and managed by the Directorate
VERBIS	Data Controllers Registry Information System
Board of Directors	Company Board of Directors
Regulations	Regulation on Deletion, Destruction or Anonymization of Personal Data published in the Official Gazette dated October 28, 2017

5. RESPONSIBILITY AND TASK DISTRIBUTION

In accordance with the Law on PPD numbered 6698 and the relevant legislation, the Company Data Contact Person was determined in order to ensure the necessary coordination within the company within the scope of ensuring, preserving and maintaining compliance with the legislation on protection of personal data, its duties and responsibilities were defined and the necessary decisions were taken and communicated to the relevant parties. The technical and administrative measures taken within the scope of this policy, to increase the training and awareness of the employees of the relevant unit, to prevent the illegal processing and access of personal data and to ensure the legal storage of personal data, to ensure data security in all environments where personal data is processed. and administrative measures are carried out by the data contact person and responsible units.

6. MEDIA WHERE PERSONAL DATA ARE STORED

Personal data kept by our company, servers-server, software used, personal computers, mobile devices such as phones, tablets, mobile applications, optical discs, removable memory, personal data kept in electronic media and on paper, forms containing accommodation and service information, personal files, job application forms, contracts between the company and third parties, manual data recording systems (questionnaire forms, visitor forms, personal data kept in written, printed and visual media, unit cabinets, archive rooms are recorded in non-electronic physical media such as.

Your personal data are securely stored in accordance with the Law on PPD No.6698 and related legislation, and international data security principles. Your personal data are obtained, recorded, stored, changed, reorganized by our company, as the subject of all kinds of processing performed on your personal data, by obtaining, recording, storing, changing, rearranging, completely or partially, automatically or by non-automatic means provided that it is a part of any data recording system.

7. PROCESSING OF PERSONAL DATA AND GENERAL PRINCIPLES

7.1.Privacy Policy

As explained in this policy, the data of both employees and all relevant persons who have personal data in contact with our company are confidential. Within the scope of this policy and the measures taken, except for the cases specified in the law, no one may use, reproduce, copy, transfer or transfer the data of individuals for any other purpose for any other purpose, and cannot be used for purposes other than those determined by the policies.

7.2 Basic Principles

Personal Data being processed by our company is processed in accordance with the principles specified in Article 4 of the Law on PPD numbered 6698. The Company, in the processing, protection, deletion and destruction processes of Personal Data, according to the principles written below, It is processed in accordance with the prescribed procedures and principles.

- To comply with the law and good faith.
- To be accurate and up to date when necessary.
- Processing for specific, explicit and legitimate purposes.
- Being Limited, Proportional and Expedient to Purpose of Data Processing
- Retaining Personal Data for the Period Required for the Purpose stipulated in the Legislation or for the Purpose for Which They are

8. CONDITIONS OF PROCESSING PERSONAL DATA

Personal data processed by our company are processed in accordance with Article 5 of Law No. 6698. Personal data cannot be processed without the express consent of the data subject. However, in the presence of one of the principles we have stated below, it is possible to process personal data without the explicit consent of the person concerned.

- In the event that it is clearly prescribed by the laws. Legality principle
- In the event that the person who cannot explain his/her consent due to the actual impossibility, or is not legally valid at his/her discretion, or is obliged to protect the life or physical integrity of the person himself/herself or someone else. The actual impossibility.
- Provided that it is directly related to drawing up or performing a contract, it is required to process personal data of the parties of the contract. Performance of Agreement.
- In case it is obligatory for the data controller to fulfill his/her legal obligations. legal liability
- In the event that it is publicized by the person concerned himself/herself. publicity
- In the event that data processing is obligatory for the establishment, use or protection of a right, Contingency
- Provided that it does not harm the fundamental rights and freedoms of the person concerned, it is an obligation to process data for legitimate interests of the data officer. legitimate interest

9.CONDITIONS OF PROCESSING SPECIAL QUALIFIED PERSONAL DATA

Special Qualified Personal Data processed by our company are processed in accordance with Article 6 of Law No. 6698. Personal data relating to the race, ethnic origin, political opinion, philosophical belief, religion, religious sect or other belief, appearance, membership to associations, foundations or trade-unions, data concerning health, sexual life, criminal convictions and security measures, and the biometric and genetic data are special categories of personal data

It is regulated by the law article that the processing of sensitive personal data without the express consent of the person concerned is prohibited. Accordingly, Special Qualified Personal Data cannot be processed without the express consent of the person concerned. However, as written in the law article; However, as written in the law article; in the 6.1 paragraph of Law, other than health and sexual life, Personal data can be processed without the explicit consent of the person concerned in cases stipulated by the laws.

However Personal data on health and sexual life can be processed without the express consent of the person concerned for purposes;

- Protection of public health
- Preventive medicine
- Conducting medical diagnosis, treatment and care services,
- Planning and management of health care financing
- By persons or authorized institutions and organizations under the obligation of secrecy

Our company acts in accordance with the law numbered 6698 and the relevant legal legislation in the processing of special qualified personal data, and such data is also processed by taking adequate measures determined by the Board.

10. PROCESSING AND COLLECTION OF PERSONAL DATA AND LEGAL REASONS:

Your personal data being limited to the stated purpose, are processed and collected for the purpose filling application forms, contracts, arranging printed forms, creating membership through technological software programs used in electronic environment, e-mail, filling application forms, creating personal files, preparing contracts, execution, accounting, processing financial information for the establishment and maintenance of financial and social rights, realizing sales transactions and ensuring corporate development within the scope of company activities. Your personal data are processed and collected by fully or partially automated or non-automatic means provided that it is part of any data recording system by using the video camera recording system in order to ensure indoor and outdoor security in company buildings and extensions, using the fingerprint system, which is a personnel attendance control system, for the purpose of evaluating the performances of the company employees for the reasons of your express consent, by using the company's buildings and extensions, website, mobile applications, calling our call services, complaint management systems, market research companies and reference methods. In addition, your personal data are processed and collected through audio recordings recorded by corporate call center services performed on behalf of Radisson Blu Ottomare (Company), tourism agencies providing intermediary services, information recorded, obtained through third party websites, e-mail, letter or other communication tools.

In accordance with the legal regulations that our company is subject to, in order to provide products and services by our company and to fulfill our company’s obligations arising from contracts and legal legislation, As a rule, your personal data and special quality personal data are processed based on the explicit consent of the person concerned. In addition, within the scope of your contact with our company, your personal data are processed without seeking explicit consent in the following cases.

- It is necessary to process personal data belonging to the parties of the contract, provided that it is directly related to the establishment or execution of contracts between our company and third real and legal persons,
- It is mandatory for the company to fulfill its legal obligation,
- In the event that personal data is revealed to the public by the person concerned himself/herself.
- In the event that data processing is mandatory 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 process data for legitimate interests of the data officer.
- In the event that it is clearly stipulated by the laws,

In accordance with the article 5/1-h of the Communiqué on the Procedures and Principles for Fulfilling the Obligation of Disclosure to Articles 5 and 6 of the Law on the Protection of Personal Data No. 6698 your personal data are processed, collected and transferred to the specified purposes.

10.1. Processing of Personal Data

- Your identity information (TR/Foreigner Identity Number, name and surname, place and date of birth, mother and father name, marital status, gender, passport information, information on your driver's license, your identity card or other population on the identity sharing system ID information)
- Your contact information (your phone numbers, contact address, e-mail address)
- Your location information (license plate information, address, location information of your location)

- Guest Transaction/Accommodation Information (Reservation information, arrival at the hotel, date of departure from the hotel, room information, number of days to stay, identity, contact, proximity information about the guests staying at the hotel, bank, credit card, mail order, invoice, payment information, forms and records of guests exhibiting inappropriate behavior, signature circular, power of attorney, contract information)
- Request and Complaint Information, Information and records collected from electronic and physical media regarding the requests and complaints of people benefiting from products and services, complaint information received via internet and social media, online channels)
- Personal Information (Employment contract, education, diploma information, certificate information, SSI employment entry, exit declaration, GSS login information, identity information written on the family status declaration, dependents, spouse, child proximity information, registration information of family members, debit document, employment certificate, resignation, termination, severance and notice pay payroll, salary payroll information, disciplinary investigation information, SGK registration number, service statement, background information, leave information, personnel performance evaluation reports, occupational accident information, information in the job application form, reference, information, Bank account information, IBAN number information)

- Legal Transaction Information (Personal information in correspondence with judicial authorities, information in lawsuits and enforcement files)
- Lost Property Information (Information on the property found in the found property report, name, surname, date, time, signature information of the person found)

- Information shared on Social Media and Internet Sales Sites (The information shared by the people who benefit from our products and services using our social media accounts, the identity, communication, location, bank, payment that the people who receive the services and products consent to share via the websites abroad and domestic agencies, financial information)
- Physical Space Security Information (Entry-exit registration information of guests, potential guests, employees, interns, suppliers, service providers and visitors who benefit from our products and services, our hotel and its add-ons, your camera recording images if you visit our offices, your vehicle license plate information if you use our parking lot, information on the forms)
- Professional experience information (education information, diploma information, working life, reference information, courses attended, in-service training information, certificates, driving license, other information on the notified forms)
- Visual Records (Photo information on the completed, printed forms, documents and official identity documents, photographs taken as part of job application and company activities, advertising, marketing, web page in company campaigns, social media accounts or third-party social media channels, shared your photos, your images in camera recordings)
- Health Information (Health reports, blood group information, personal health and physical disability information, information about health tests)
- Information on Criminal Convictions and Security Measures (Criminal record, conviction, legal status information)
- Within the scope of lease agreements made with our company, identity, contact, location, bank, financial information, signature circular, power of attorney, contract information on the lease agreements,
- Voice recordings recorded through corporate call center services performed on behalf of Radisson Blu Ottomare (Company), information processed, recorded, obtained through tourism agencies providing intermediary services, third party websites, your personal information obtained by e-mail, letter or other communication means.

Your personal data are processed and protected by our data controller company in accordance with Article 20 of the Constitution and Article 4 of the Law on PPD for the purposes and legal reasons written above.

10.2. Personal Data Processing Inventory

Personal data are processed based on Personal Data Processing Inventory which is stated that it is mandatory to include the matters and information listed in the relevant legislation and is stated in 5/1. article of Regulation and must be regulated. Personal Data Processing Inventory has been created separately by our company and it is updated periodically.

11. PRINCIPLES ON PERSONAL DATA STORAGE AND DESTRUCTION

With this policy created by our company, personal data belonging to guests, potential guests, agents, intermediary institutions, suppliers, sub-employers, service providers, managers and

employees, business partners, company partners, employees, employee candidates, interns, visitors, public institutions and organizations and private law employees of legal entities and third parties are stored and destroyed in accordance with the relevant legislation, procedure and law. Detailed explanations regarding storage and destruction are set out below.

11.1. Storage of Personal Data

The processing of personal data is defined in Article 3 of Law No. 6698, the personal data processed in 4. article have been regulated that they must be related, limited and measured for the purpose of processing, and must be kept for the period stipulated in the relevant legislation or for the purpose for which they are processed, and the processing conditions of personal data are listed in Articles 5 and 6 of Law No. 6698. Detailed explanations regarding this are written above in the text of this policy, and within the scope of company activities, personal data are stored by taking administrative and technical measures for a period of time stipulated in the relevant legislation or in accordance with our processing purposes.

11.2. Legal Reasons Requiring the Storage of Personal Data

With this policy, personal data processed within the scope of our company's activities they are kept and stored for the period written in the relevant legislation. Personal data are stored for the periods stipulated in the laws to which individuals are subject within the scope of the activities of the company and the written retention periods within the framework of secondary regulations and the statute of limitations to which the crimes stipulated in the laws are subject. The increase stipulated in the legal legislation to which our company is subject to its activities considering the termination periods and any disputes with third parties that the company has legal contact with or that may arise, the corporate memory of the company and its commercial business and activities, except for the periods stipulated in the law, the legitimate interest of the company and the establishment and execution processes of contracts made or to be made with the relevant data owners. The storage and destruction periods of personal data are determined by this policy as an institutional decision.

11.3. Purposes of Processing Requiring the Storage of Personal Data

The company stores the personal data which it processes in accordance with the relevant legislation, limited to company activities, for the following purposes. According to this; the processing purposes that require the storage of personal data are specified below.

- Taking advantage of the products and services offered by Radisson Blu Ottomare (the Company), the products and services offered; Providing them to be customized according to your tastes, habits and needs,
- Ensuring that you are notified of the general and special campaigns, promotions, promotions, discounts and advantages offered by Radisson Blu Ottomare (Company),
- Radisson Blu Ottomare (Company) loyalty program Radisson Rewards card membership and registering, To inform you about our new services and products to be offered by our

company, as well as any changes and innovations in personal data policies and membership conditions,

- Ensuring the legal and commercial security of the company and the persons who are in business relations with the company,
- Performing reservation, transportation, sales, accommodation, after-sales support services within the scope of company activities, and benefiting from discounts for guests,
- To improve company services, to continue corporate development activities, to continue advertising and marketing activities,
- To maintain the financial and accounting, administrative, legal, technical business processes of the company,
- Ensuring guest satisfaction, maintaining the request and complaint processes of the guests, following the complaint information received on the internet and social media, the request, suggestion and complaint notification processes collected through online channels,
- Planning and executing human resources processes, fulfilling employment application processes, creating personal files for employees, fulfilling financial obligations, determining company wage policy,
- Making and executing agreements and protocols with the company's guests, potential guests, suppliers, intermediary institutions, agencies, rental companies, employees and relevant third parties with whom it has a legal relationship,
- To carry out the work and transactions and processes before the PPD Institution within the scope of the PPD Law,
- Obligation of the company to prove as evidence in legal disputes with third parties,
- Using our web pages and mobile applications related to company activities,
- In relation to products and services, performing sales transactions to related persons and organizations, following up sales transactions, performing banking transactions and payment processes with credit cards, mail order, bank transfer and other commercial payment tools,
- Ensuring the physical security of the company's buildings and extensions, monitoring the employment processes of the personnel, controlling the company building entrances and exits,
- In the relevant legislation In order to fulfill the legal obligations stipulated and to ensure security, fulfillment of identity verification, identity notification obligation,

- Notifications to relevant public institutions and organizations such as Police Directorates, Revenue Administration, Tax Offices, Finance, SSI,

For these purposes, your personal data are processed in accordance with the conditions and purposes determined in accordance with Articles 5 and 6 of the Law. Personal data are not used for any purpose other than our company's activities.

11.4. Reasons Requiring the Destruction of Personal Data

Personal data are deleted, destroyed or anonymized by the company in accordance with the procedures and principles stipulated in the policy, law and regulation, upon the request of the person concerned for the following reasons, by filling out the application form. Accordingly;

- In the event that the purpose requiring the processing or storage of personal data by the company no longer exists.
- Changing or abolishing the relevant legislation provisions that are the basis for processing personal data
- In cases where the processing of personal data by the company is made only on the condition of express consent, the person concerned withdraws his express consent,
- In accordance with Article 11 of PPD Law No.6698, the application of the relevant person for the deletion and destruction of personal data within the scope of the application rights to the company is accepted by the PPD Institution,
- In cases where the PPD Institution rejects the application made by the person concerned with the request for deletion, destruction or anonymization of the personal data, finds the answer insufficient or does not respond within the period stipulated in Law No. 6698; If he makes a complaint to the PPD Board and this request is approved by the PPD Board.
- Pursuant to the relevant legal regulation, the maximum period required to keep personal data has passed and there is no reason to keep personal data.

12. Technical and Administrative Measures Regarding Storage and Destruction of Personal Data

Within the scope of the regulations determined by this policy, the following safe and proper storage of personal data, prevention of illegal processing and access, and prevention of data leaks and provision "In the processing of special qualified data, it is also necessary to take adequate measures determined by the Board." for the legal destruction of personal data according to 6/4. article of Special Qualified Personal Data which was regulated in 6. article of PPD Law No. 6698 and necessary adequate measures determined and announced by the PPD Board in order to ensure the security of Personal Data specified in 12. article of the same law the following technical and administrative measures are taken by the company as the data controller.

The Administrative and Technical Measures announced by the Personal Data Protection Authority at https://www.kvkk.gov.tr were determined and detailed as written below. These measures determined by the Board are listed in the table below.

TECHNICAL AND ADMINISTRATIVE MEASURES

Technical Measures	Administrative Measures
Authority Matrix	Preparation of Personal Data Processing Inventory
Authority Control	Corporate Policies (Access, Information Security, Use, Storage and Destruction etc.)
Access Logs	Contracts (Between Data Controller - Data Controller, Data Controller - Data Processor)
User account management	Confidentiality Commitments

Network Security	Internal Periodic and/or Random Audits
Application security	Risk analysis
Encryption	Employment Contracts, Internal Discipline Directive
Penetration Test	Corporate Communication (Crisis Management, Informing Processes of the Board and Related Person, Reputation Management etc.)
Intrusion detection and prevention systems	Education and Awareness Activities
Log Records	Notification to Data Controllers Registry Information System (VERBİS)
Data Masking	
Data Loss Prevention Software (DLP)	
Replacement	
Firewalls	
Up-to-date anti-virus systems	
Deletion, Destruction or Anonymization	
Key Management	

12.1 Technical Measures

Regarding the technical measures stated in the table above and announced by the PPD Authority, the following necessary measures have been taken by the company as the data controller.

Taken Technical Measures:

- As a result of on-site and real-time analyzes on information security, risks and threats that will affect the continuity of information systems have been identified and are constantly monitored.
- Regarding the technical measures and the measures to be taken, the Data Processing Unit LPPD Technical Measures Analysis Report has been prepared and the necessary technical measures are taken.
- Necessary measures are taken for the physical security of the company's information systems equipment, software and data.

- Risks to prevent unlawful processing of personal data are identified, technical measures are taken in accordance with these risks, and routine and non-routine technical controls are carried out for the measures taken.
- By creating access procedures within the company, reporting and analysis studies are carried out regarding access to personal data.
- In case personal data is illegally obtained by others, necessary policies have been established by the company in order to notify the relevant person and the Board.
- Strong passwords are used in electronic environments where personal data are processed. Information systems are kept up-to-date by following security gaps.
- Access to personal data stored in electronic or non-electronic media is restricted according to access principles.
- Special quality personal data security trainings have been provided for employees involved in special quality personal data processing processes, confidentiality agreements have been made, and the authorizations of users with access to data have been defined.
- Adequate security measures are taken in the physical environments where personal data of special nature are processed, stored and/or accessed, and unauthorized entry and exit are prevented by ensuring physical security.
- Risks related to technical measures have been identified and necessary precautions and necessary actions have been taken.

12.2 Administrative Measures

Regarding the administrative measures stated in the articles above and announced by the PPD Authority, the following necessary measures have been taken by the company as the data controller.

Taken Administrative Measures

- Necessary trainings are provided in order to prevent unlawful processing of personal data, to prevent unlawful access to personal data, to ensure the preservation of personal data and to increase awareness in order to improve the quality of employees.

- Confidentiality agreements are made to the employees regarding the activities carried out by the company.
- Before starting to process personal data, the company has fulfilled the obligation to inform the relevant persons. Separate policies have been created for this.
- A personal data processing inventory has been prepared and the necessary updates are made by the company as a data controller.
- The Disclosure and Information Text has been prepared, the application form has been arranged and published on the website.
- Privacy and Cookie Policy has been established.
- Personal data protection, processing, storage and destruction policy has been determined, published on the website and implemented by the data contact person within the company.
- PPD Data Contact Person has been appointed, authorities and responsibilities have been determined.
- Explicit consent texts have been created separately according to the relevant person groups, and clarification texts were created for separate groups of people.

- Studies have been initiated to fulfill the storage and destruction requirements for personal data.
- Necessary actions have been taken to ensure compliance with the PPD Law, company contracts and texts containing personal data are scanned and made compatible with LPPD.
- A General Risk Analysis Report regarding administrative measures have been prepared.

13. EXPLANATIONS ON DESTRUCTION TECHNIQUES OF PERSONAL DATA

As written in the policy and personal data inventory created by our company, at the end of the period stipulated in the relevant legal legislation regarding the processed personal data or the required retention period for the purpose for which they are processed, personal data are destroyed by the authorized units of the company spontaneously or upon the application of the relevant personal data owner to our company, in accordance with the PPD Law No. 6698 and the provisions of the relevant legislation, using the methods and techniques specified below.

13.1 Deletion of Personal Data

- **Personal Data on the Server with Data Recording Media:** For the personal data on the servers, for those whose storage period has expired, the system administrator deletes the users by removing their access authorization.
- **Personal Data in Electronic Environment:** Those who have expired from personal data in electronic environment are inaccessible and unusable in any way for other employees (relevant users), except for the database administrator.
- **Personal Data in Physical Environment:** Those who have expired personal data kept in physical environment are inaccessible and unavailable in any way for other employees except for the department manager responsible for the document archive. In addition, the process of darkening is also applied by scratching / painting / wiping it in an illegible way.
- **Personal Data on Portable Media:** Those who have expired the personal data kept in flash-based storage media are encrypted by the system administrator and the access authorization is given only to the system administrator, and they are stored in secure environments with encryption keys.

13.2. Destruction of Personal Data

- **Personal Data in Physical Environment:** Those who have expired from the personal data in the paper environment, are irreversibly destroyed in the paper trimming machines.
- **Personal Data on Optical-Magnetic Media:** Physical destruction, such as melting, burning or pulverizing the personal data in optical media and magnetic media, are applied. In addition, magnetic media is passed through a special device and exposed to high magnetic field, making the data on it unreadable.

13.3. Anonymization of personal data

The anonymization of personal data is to make the personal data unidentified or identifiable, making it impossible to contact a natural person in any way, even when matching personal data with data belonging to other third parties.

In order for personal data to be anonymized; it is in the form of making it unrelated/unrelated to a real person whose identity is definite or identifiable through the use of appropriate techniques in terms of the recording medium and the relevant field of activity, such as the return of the data controller or third parties and/or matching of data with other data of personal data.

14. PERSONAL DATA STORAGE AND DESTRUCTION PERIODS

The personal data processed by the company within the scope of this policy and the relevant legislation are made according to the category of the data processed, for the periods stipulated in the relevant legislation or required by the purpose of processing, in accordance with the LPPD and the procedures and principles determined by this policy. Considering the legitimate interest of the company and the establishment and execution of contracts with the relevant data owner, the lawsuits and legal transactions that may be filed, the storage and destruction periods of personal data are determined as written in the personal data processing inventory.

Our company keeps personal data within the scope of its activities for the period specified in the relevant legislation or required for the purpose of processing the personal data, depending on the nature of the processed data. Regarding the processed personal data, first of all, it is determined whether a period is stipulated for the storage of personal data in the relevant legislation, the personal data is stored in accordance with the specified period, and in the event that no period is stipulated, the processed personal data is required for the purpose of processing and is implemented by our group companies. It keeps it for the period determined in accordance with the policies.

It is based on the storage periods determined in the personal data processing inventory by our company, and at the end of the periods specified in the inventory, personal data are deleted, destroyed or anonymized according to the nature of the data and the purpose of use in accordance with the legal regulations.

15. THE DISCLOSURE OBLIGATION OF THE DATA RESPONSIBLE

Our company pays utmost attention to the processing and protection of your personal data in accordance with the Law on Protection of Personal Data numbered 6698 ("LPPD"). As a data controller, all necessary technical and administrative measures have been taken to prevent unlawful processing of personal data, to prevent unlawful access to personal data, and to ensure the preservation of personal data. Pursuant to Article 10 of the Law; we inform you with the policies and clarification text created to cover personal data belonging to guests, potential guests, agents, intermediary institutions, suppliers, sub-employers, service providers and managers and employees, business partners, company partners, employees, employee candidates, interns, visitors, employees of public institutions and organizations and private law

legal entities and related third parties. The information required to be notified to personal data owners in accordance with the said disclosure obligation are as follows:

1. Identification of data controller or its representative, if any,

2. For what purpose the personal data is to be processed,

3. To whom and what purpose the processed personal data shall be transferred,

4. Method and legal reason of collecting personal data,

5. Application and other rights enumerated in Article 11 of the Law on PPD.

In accordance with Article 10 of the Law on the Protection of Personal Data No. 6698 (“Law”) and the provisions of the Communiqué on Procedures and Principles for Fulfilling the Disclosure Obligation, you can examine the Information Text prepared by our company as a data controller on our website.

16. RIGHTS OF THE PERSONAL DATA OWNER (APPLICATION RIGHT)

An "APPLICATION FORM" has been prepared by our company as a data controller in accordance with the Communiqué on the Principles and Procedures of Application to the Data Supervisor, within the scope of Article 11 "regulating the rights of the data subject" of the Personal Data Protection Law No 6698. It is possible to use the application right by filling out the application form on our website.

16.1. Application Right of Personal Data Owner

In accordance with Article 11 of the Law; everyone has the following rights regarding themselves by applying to the data controller.

1. To learn whether personal data has been processed or not,

2. To request the relevant information if personal data has been processed,

3. To learn the purpose for the processing of personal data and whether those have been used in accordance with the purpose or not,

4. To know the third parties to whom personal data has been transferred within Turkey or abroad,

5. To request the rectification of the data in the event they are processed incompletely or inaccurately,

6. To request the erasure or destruction of his personal data under the conditions specified in Article 7 of the PDP Law,

7. Requesting that the correction, deletion or destruction of personal data be notified to third parties to which personal data is transferred,

8. To object to the appearance of a result against the person himself due to analyzing the processed data exclusively through automated systems,

9. Claiming compensation in the event that the person suffers loss due to illegal processing of the personal data.

16.2. Procedure, duration and principles in Replying of Data Officer to Applications

In accordance with the 13/1. article of LPPD No. 6698, you must submit your applications to our company in writing or by the above written methods determined by the PPD Authority in order to use your rights stated above. Our company will conclude your requests in the application free of charge as soon as possible and within thirty days at the latest, depending on the nature of the request. However, if the transaction requires an additional cost, the fee in the tariff determined by the Board will be requested. In case the application is caused by the error of the data controller, the fee collected is returned to the person concerned.

16.3. Right of Personal Data Owner to Complain to the Board

In the event that the personal data owner's application is rejected, or the response is found to be insufficient, or the response is not given in due time, a complaint may be made to the Board within thirty days from the date of receipt of the reply from our Company or within sixty days as of the application date, in any case. In accordance with Article 13 of the Law, complaints cannot be filed without exhausting the remedy.

17. CASES IN WHICH THE PERSONAL DATA OWNER CANNOT EXTEND THEIR RIGHTS

Pursuant to the 28/1. article of PPD Law No. 6698, the following issues are excluded from the scope of application of the law (exceptions), and personal data owners cannot claim their rights enumerated in article 16 above.

- Provided that Personal data is not provided to the third parties and the obligations relating to data security are adhered to, processing the same within the scope of the operations related to the family individuals living with fully itself or living in the same housing by the real persons.
- Processing the personal data for the purposes of investigation, planning and statistics by anonymizing with official statistics.
- Processing personal data within the context of artistic, historical, literary or scientific purposes or freedom of speech provided that the personal data does not breach the natural defence, national security, public security, public order, economic security and confidentiality of private life or personal rights, and does not constitute a crime.
- Processing the personal data within the scope of preventive, protective and intelligence operations executed by state institutions and organizations so authorized by the law to ensure national defence, national security, public safety, public order or economic security.

- Processing the personal data by judicial or enforcement authorities in relation to the investigation, proceedings, litigation or execution procedures.

According to the 28/2. article of the PPD Law No. 6698. provided that it is appropriate and proportionate to the purpose and basic principles of this law, the rights specified in Article 10 regulating the data controller's obligation to inform, in Article 11, which regulates the rights of the person concerned, except the right to claim damages, and in Article 16, which regulates the obligation to register in the Data Controllers Registry are not applied in the following cases:

- To process personal data being required for prevention of committing an illegal act or criminal investigation.
- To process personal data publicized by the person concerned.
- Processing personal data being required for disciplinary investigation or prosecution and conducting supervisory or regulatory duties by the authorized public institutions and organizations and professional public organizations by the power granted by the law,
- Processing personal data being required for protecting economic and financial interest of the State with regard to the budgetary, tax related and financial issues.

18. PERIODIC DISPOSAL OF PERSONAL DATA and INSPECTION TIME

The periods for ex officio deletion, destruction or anonymization of personal data are regulated as written below in Article 11 of the Regulation. According to this; the data controller, who has prepared a personal data storage and destruction policy, deletes, destroys or anonymizes the personal data in the first periodic destruction process following the date when the obligation to delete, destroy or anonymize personal data. The time interval for periodic destruction is determined by the data controller in the personal data storage and destruction policy. This period cannot exceed six months in any case. The data controller, who is not obliged to prepare a personal data storage and destruction policy, deletes, destroys or anonymizes personal data within three months following the date when the obligation to delete, destroy or anonymize personal data. In addition, he/she will make the necessary audits by the personal data contact person and the data controller every three months for not more than six months. The data controller and the data contact person may shorten the periods specified in this article in the event of damages that are difficult or impossible to compensate and in case of obvious unlawfulness.

19. DELETION AND EXTRACTION PERIOD ON THE APPLICATION OF THE RELATED PERSON

The periods of deletion and destruction of personal data upon the application of the relevant person are regulated as stated below in 12. Article of the Regulation. According to this; if all the conditions for processing personal data have disappeared; the data controller deletes, destroys or anonymizes the personal data subject to the request. The data controller finalizes the request of the person concerned within thirty days at the latest and informs the relevant person. If all the conditions for processing personal data have disappeared and the personal data subject to the request is transferred to third parties, the data controller will notify the third party; He/she ensures that the necessary procedures are carried out within the scope of this Regulation before the third party. If all the conditions for processing personal data are not eliminated, this request may be rejected by the data controller by explaining the reason in accordance with the third paragraph of 13. Article of the Law, and the rejection response is notified to the relevant person in writing or electronically within thirty days at the latest.

20. PUBLISHING, STORING AND UPDATING THE POLICY

This policy prepared by the company is published in two different media on the company's website https://www.radissonhotels.com/en-us/hotels/radisson-blu-istanbul-ottomare, in wet signed form (printed paper) and in electronic environment. It will be deemed to have been disclosed to the public upon publication of the policy on the website. The printed paper copy is kept in the PPD file by the data contact person. This policy is reviewed by the designated data contact person within the scope of its powers and responsibilities, from the date of its publication, once a year at the end of each year, and the relevant sections will be updated as necessary.

21. ENFORCEMENT AND TERMINATION OF THE POLICY

This policy, written in articles above, will be deemed to have entered into force after its publication on the company's website. If it is decided to annul the policy with the consent of the data controller and the decision of the personal data contact person, the old copies of the policy with wet signature are canceled by the data contact person (by stamping the cancellation stamp or written cancellation) and for a period of at least 5 years, the relevant personal data contact person stored in the unit.

Policy Effective Date	Date Of Update