



PERSONAL DATA PROTECTION POLICY

OUR IDENTITY AS DATA CONTROLLER

Fer Hotel is a hotel affiliated to Nuruosmaniye Turizm ve Otelcilik Sanayi ve Ticaret Anonim Şirketi, providing luxury boutique hotel services at Molla Fenari Mah. Türbedar Sk. No: 12 İç Kapı No: 1 Fatih / İSTANBUL since March 2016. You can find more information about us by visiting our website www.ferhotel.com.

PURPOSE AND SCOPE OF THE POLICY

This policy aims to describe the principles of processing your personal data by Fer Hotel in the capacity of data controller, as well as the legal basis and purposes of processing, data collection methods and the measures taken to disclose, store, anonymize, delete, destroy and ensure the security of personal data, and your rights and the methods for exercising these rights.

Customers, employees, employee candidates, interns, authorized officers of suppliers, employees of suppliers and visitors whose personal data is processed by Fer Hotel and their parents, guardians or representatives covered by this policy.

OUR DATA PROCESSING PRINCIPLES

Legality, honesty and transparency: We process your personal data lawfully, honestly and clearly.

Proportionality and Limitation: We collect your personal data for specific, explicit and legitimate purposes and do not process it in a way that does not comply with these purposes.

Minimum relevant data: Personal data is relevant, sufficient and limited to the extent required by the purposes of processing. We do not process any irrelevant personal data.

Accuracy: We process personal data accurately and update it as necessary. We ensure that inaccurate personal data is deleted in accordance with the purposes of processing or is corrected without delay.

Retention to the extent necessary: We retain your personal data to the extent necessary for the purposes of processing. At the end of this period, your personal data is deleted, destroyed or anonymized.

Data integrity and confidentiality: We process your personal data by taking technical and administrative measures that will prevent unauthorized or unlawful processing as well as loss, deletion or damage of the personal data.

Being available for inspection: We fulfill our responsibilities to demonstrate our compliance with all of the above-mentioned principles.

OUR PERSONAL DATA PROCESSING CONDITIONS AND PERSONAL DATA PROCESSING PURPOSES

We process your personal data without your explicit consent in case of fulfillment of one of the conditions prescribed in the legal regulations. Based on these conditions, our data processing purposes are described below.

- Your personal data may be processed if it is expressly prescribed in the laws. Fer Hotel processes personal data as follows:
 - Customer data as it is explicitly prescribed in the Identity Notification Law No 1774,
 - as it is explicitly prescribed in the Foreigners and International Protection Law No 6458,
 - Labor Law No 4857,
 - personal data of its employees as it is explicitly prescribed in the Social Insurances and Health Insurance Law No 5510,
 - It processes the personal data of its customers, visitors and employees that include their internet logs in accordance with the Law No 5651, if they use the internet of the Hotel.

- Personal data may be processed if it is required for the protection of life or bodily integrity of the person or someone else, who is unable to express his or her consent due to actual impossibility or whose consent is not legally recognized. Fer Hotel processes your personal data by obtaining your explicit consent for the following purposes:
 - Sharing your personal data with the emergency services, when your or someone else's life is in danger,
 - Avoiding any situations that might endanger your life due to dietary, allergic or disability reasons.

- Personal data may be processed if it is required to process the personal data of the parties due to the conclusion or implementation of a contract. As a hotel service provider, Fer Hotel processes personal data of its customers for:
 - Making room reservations,
 - Providing the requested products and services,
 - Processing payments,
 - Ensuring communication,

- Sending notifications by post, phone etc. or informing them about unplanned situations;
 - It also processes personal data of its employees, employee candidates and interns for the purpose of fulfilling its obligations arising from the employment contract,
 - It also processes personal data of the authorized officers and employees of suppliers through the contracts signed with the suppliers for the purpose of ensuring supply chain.
- Personal data may be processed to fulfill legal obligations. Accordingly, your personal data is processed to fulfill our legal obligations arising from the situations that are clearly prescribed in the laws.
 - Although personal data that is made public by the relevant person may be processed, Fer Hotel does not process any personal data for any purpose based on this condition.
 - Personal data may be processed if the processing of data is required for the conclusion, use or protection of a right.
 - Your personal data may be processed for our legitimate interests, provided that it does not harm your fundamental rights and freedoms. Accordingly, your personal data is processed for the following purposes:
 - ensuring customer satisfaction,
 - maintaining our commercial reputation,
 - resolving disputes,
 - fraud protection (monitoring and checking our systems, verification of the validity of your card and prevention of fraud in the payments made by credit card,
 - business performance and increasing business performance,
 - monitoring the safety and security of our employees and guests, food safety and cleanliness, monitoring any accidents and undesired situations, prevention and identification of crimes (use of security cameras and call recording system)
 - marketing our products and services;
 - conducting our business in accordance with legal regulations.
 - Your personal data may not be processed without obtaining your explicit consent. Upon obtaining your explicit consent, we process your personal data for:
 - Sending e-mails to promote our hotel and inform you about promotions,
 - When you visit our website, making it easier for you to use our website through using cookies and similar technologies and also offering you advertisements and promotions for marketing purposes.

PROCESSING OF SPECIAL PERSONAL DATA

According to legal regulations, the data regarding race, ethnicity, political thought, philosophical belief, religion, sect or other beliefs, appearance and dress, membership to associations, foundations or unions, health, sexual life, criminal convictions and security measures as well as biometrical and genetic data is defined as special personal data.

Personal data other than health and sexual life may be processed without obtaining the explicit consent of the data owner in the cases prescribed in the laws. Personal data related to health and sexual life may be processed by the persons or authorized institutions and organizations that are under the obligation of confidentiality, without obtaining the explicit consent of the data owner, only for the purpose of protecting public health, performing preventive medicine, medical diagnosis, treatment and care services, planning and managing health services and financing. Except for these cases, special personal data is not processed without obtaining the explicit consent of the data owner.

The data regarding the disability, diet or allergic condition that is notified by the guests or through their parents/guardians or representatives is processed only for the purpose of providing the services requested by guests, and is never disclosed to third parties except for these purposes.

Fer Hotel processes the data of its employees, employee candidates and interns related to criminal convictions and security measures as well as their health reports for the purpose of being placed in the personnel file or appointing employees in line with their health condition at the time of appointment, in accordance with the relevant legislation and legal obligations.

Fingerprint data of the employees is processed in accordance with the contract signed with the employees for the purposes of determining their attendance at the workplace and ensuring information security. Fingerprint data is deleted within one week after the employee leaves the workplace, but their log records are kept.

The blood group data of the employees is processed so that it can be used in case of an emergency as part of occupational health and safety.

DATA INVENTORY AND DATA CATEGORIES

Fer Hotel collects the personal data of customers, employees, employee candidates, interns, authorized officers and employees of suppliers and visitors and their parents, guardians or representatives in a data inventory. The inventory is arranged according to the principles published by the data protection authorities. The data owner categories are provided in the following table.

Data Owner Category	DEFINITION
Guest/Customer	It refers to the people who benefit from the accommodation or other services provided by Fer Hotel.
Employee	It refers to the employees of Fer Hotel.

Employee Candidate	It refers to the people who have applied for a job at Fer Hotel but have not started working yet.
Intern	It refers to the people who are doing their internship at Fer Hotel.
Visitor	It refers to the people who come to Fer Hotel to visit the employees or customers.
Supplier's Employee/Authorized Officer	It refers to the employees and authorized officers of the organizations that sell services or products to Fer Hotel.
Parent/Guardian	It refers to the people who are the Parents or Guardians of the people who receive services from Fer Hotel or who provide services to Fer Hotel.
Representative	It refers to the individuals who receive services from Fer Hotel or who are the representatives of the people who provide services to Fer Hotel.

In the personal data processing inventory, all data is categorized as identity, communication, location, personal file, legal procedure, customer transaction, physical space security, transaction security, risk management, finance, professional experience, marketing, audio-visual records, health information, criminal conviction and security measures.

Data Type	DEFINITION
Identity	Identity data is the name, surname, Turkish Identity Number, Passport Number, Registration Number, Place of Birth, Date of Birth and similar identification details.
Communication	Communication data is the information used for communication such as the relevant person's address, phone number, e-mail address, KEP address.
Location	The data indicating the location of the person is the location data. It may be GPS positioning as well as vehicle recognition data, meeting attendance minutes and the vouchers issued by the restaurants or cafes where the person receives services may also contain location data.
Personal File	It is the information available in the personal file of the person. Information such as payroll information, disciplinary investigation, employment-termination document records, assets declaration information, resume information, performance assessment reports fall into this type of category.
Legal Procedure	Information contained in the correspondence made with judicial authorities and the information available in the case file
Customer Transaction	Invoices issued for the services provided as well as bills, bond and check information, order and request information etc. are customer transaction data.
Physical Space Security	Visitor records, employee and visitor entry and exit records, etc. are personal data related to physical space security.
Transaction Security	IP data, website login and logout information, system logs, password and code information are accepted as Transaction Security data.

Finance	Bank Information, IBAN Number, account information, credit and risk information and personal assets information of individuals are financial data.
Professional Experience	Diploma Information, Training Certificates, Participation Certificates, courses attended, certificates of expertise on a particular subject, information on previous jobs and work experiences, projects realized etc.
Marketing	Shopping history information, data obtained through surveys and campaign studies, digital marketing information, website cookies etc. are marketing data.
Audio-visual records	Video recordings, photographs, audio recordings and camera footage constitute audio-visual records.
Health Data	Health reports of individuals, information on disability condition, information on personal health status, blood type, information on the devices and prosthesis, prescriptions, information on diagnosis and treatment, drugs used etc. are health data.
Criminal Conviction and Security Measures	Data such as criminal conviction of the person or the decisions related to security measures fall into this type of categorization.
Biometrical Data	Biometrical data is the information such as fingerprint information, face recognition information, palm information, retina data and voice recognition information etc. that allows the person to be distinguished from other people depending upon their biological characteristics.

According to the organizational structure of Fer Hotel and depending upon the categories of data processed; legal reasons, purposes of processing, retention periods, parties to whom such data is transferred inland and abroad and the administrative and technical measures taken for the protection of data are described in details. The accuracy and currency of the inventory are checked at regular intervals, and modifications are made if necessary.

RETENTION AND ANONYMIZATION & DELETION OF PERSONAL DATA

Although the personal data is processed in accordance with the provisions of the Article 138 of the Turkish Penal Code and the Article 7 of the Personal Data Protection Law No 6698; in case the reasons that require processing of data disappear, the data is irretrievably deleted, disposed of or anonymized upon a decision being made by Fer Hotel or upon the request of the personal data owner. The retention periods of the data are determined according to the relevant legislation and the needs of Fer Hotel.

For the deletion, disposal or anonymization processes, the decisions and suggestions of the Personal Data Protection Authority regarding these matters are taken into consideration. The most suitable solution allowed by the technology is applied by considering the needs and means of Fer Hotel.

DATA RETENTION PERIODS

Fer Hotel records the personal data that it processes as long as it is required to do so in accordance with the relevant legislation in terms of the purpose of collecting this data, and then it disposes of or anonymizes such personal data. The retention periods of personal data are provided in the following table.

DATA	LEGAL REASON	RETENTION PERIOD
Human Resources Data - Job Application	Such data is kept for assessing applications. It is kept for 2 years as a reasonable period.	2 Years
Human Resources Data - Personal File	The data kept in the personal files of the employees are retained in accordance with the provisions of the Labor Law No 4857 and the Code of Obligations No 6098, depending upon the statute of limitations.	10 years
Accounting Data	The data on accounting records is kept in accordance with the provisions of the Code of Obligations No 6098, depending upon the statute of limitations.	10 years
Data of the Employee/Authorized Officer of Supplier	Contact and identity data contained in the necessary invoices/receipts and contracts regarding the goods/services received in relation with the employee and authorized officer of the supplier is kept for 10 years within the scope of the Code of Obligations No 6098.	10 years
Guest Use Data	The data of the guests regarding the services that they receive at the hotel is kept in accordance with the provisions of the Code of Obligations No 6098, depending upon the statute of limitations.	10 years
Visual Recordings	The data regarding advertising, training and events organized by Fer Hotel is kept either under the contract or upon obtaining explicit consent. The data obtained with explicit consent is collected within the scope of the explicit consent. The records regarding advertising and training are kept indefinitely.	Indefinitely/during the term of explicit consent
Identity and Contact Information of Guests	Identity and contact information of the guests is kept for 10 years in accordance with the Code of Obligations No 6098. Such data may be only used for advertising purposes upon obtaining the explicit consent of the guest.	10 years
Visitor Records	Visitor records are kept for the security of the hotel. They are kept for 2 years in accordance	2 years

	with the statute of limitations prescribed in the Turkish Penal Code.	
Security Camera	Security camera recordings	1 month
Website Logs	Within the scope of the Law no 5651, the log records of the IP addresses connected to Fer Hotel's own website www.ferhotel.com are kept for 2 years.	2 years
Internet Use Data	Internet use log records of guests, employees and visitors are recorded for 2 years in accordance with Law No 5651 and relevant legislation.	2 years
Employee Fingerprint Data	Within the scope of the employee's contract, fingerprint access system is used to follow up the attendance of employees, ensure hotel security, quality management and information security. Such data is recorded during the term of employment. It is deleted within 1 week after the person leaves the company.	1 Week

ANONYMIZATION

Anonymization of personal data refers to the process of making it impossible to associate personal data with an identified or identifiable natural person under any circumstances, even if it is matched with other data. For the anonymization of personal data; it must be impossible to associate personal data with an identified or identifiable natural person, even by using suitable techniques in terms of the recording media and the relevant field of activity, such as retrieval of the personal data by the data controller or recipient groups and/or matching the data with other data.

Fer Hotel takes all necessary technical and administrative measures in the process of anonymizing personal data. Anonymization of personal data is executed in accordance with the principles described in the Regulation on the Deletion, Disposal or Anonymization of Personal Data and the methods in the relevant guide published by the Personal Data Protection Authority.

DELETION OF PERSONAL DATA

Deletion of personal data is the process of making personal data inaccessible and non-reusable for the relevant users.

Fer Hotel takes all necessary technical and administrative measures to make the deleted personal data inaccessible and non-reusable for the relevant users. The following methods are used for the deletion of data.

Application Type Cloud Solutions as Service

In the cloud system, data is deleted by sending a deletion command. During the execution of this process, it should be noted that the relevant user does not have the authorization to restore the deleted data in the cloud system.

Personal Data on Papers

Personal data on papers is deleted by using the blackening method. Blackening process is executing by cutting the personal data on the relevant document, if possible and if it is not possible, by making it invisible to the relevant users by using fixed ink, which cannot be read through using any technological solutions.

Office Files on the Central Server

It is ensured that the file is deleted through the deletion command in the operating system or the access rights of the relevant user on the file or the directory, where the file is located, are removed. During the execution of such operation, it should be noted that the relevant user cannot be the system administrator.

Personal Data in Portable Media

No confidential data is carried on portable media. Personal data in portable media is deleted with the software suitable for the relevant hardware.

Databases

The relevant lines that contain personal data are deleted with database commands (DELETE etc.). During the execution of such operation, it should be noted that the relevant user cannot be the database administrator.

DESTRUCTION OF PERSONAL DATA

Destruction of personal data is the process of making personal data inaccessible, unrecoverable and unusable by anyone in any way whatsoever. Fer Hotel takes all necessary technical and administrative measures regarding the destruction of personal data.

Local Systems

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

De-magnetization: It is the process of exposing the magnetic media to a very high magnetic field by passing it through a special device and corrupting the data available on it in an unreadable way.

Physical Destruction: It refers to the physical destruction of optical media and magnetic media such as melting, burning or pulverization. Data is rendered inaccessible by implementing the processes such as melting, burning, pulverization of the optical or

magnetic media or passing it through a metal shredder. In terms of solid state disks, if the overwriting or de-magnetization is not successful, this media is physically destroyed.

Overwriting: It is the process of preventing the recovery of old data through writing random data consisting of 0s and 1s on magnetic media and rewritable optical media for at least seven times. This process is executed by using special software.

Environmental Systems

The destruction methods that could be used depending upon the type of media are as follows:

Network devices (switches, routers etc.): The storage media in these devices are fixed. The products often have a delete command, but they do not have destruction feature. They are destroyed by using one or more of the suitable methods mentioned above in the section 'Local Systems'.

Flash-based medias: Flash-based hard disks that have ATA (SATA, PATA etc.), SCSI (SCSI Express etc.) interfaces are destroyed by using the command, if supported, and by using the destruction method recommended by the manufacturer, if not supported, or by using one or more of the suitable methods mentioned above in the section 'Local Systems'.

Magnetic tape: It is the media that stores data through micro magnet parts on flexible tape. It is destroyed by de-magnetizing it through exposing it to very strong magnetic media or by using physical destruction methods such as burning and melting.

Magnetic disk-line units: They are media that store data through micro magnet parts on flexible (plate) or fixed media. They are destroyed by de-magnetizing it through exposing it to very strong magnetic media or by using physical destruction methods such as burning and melting.

Mobile phones (Sim cards and fixed memory areas): There is a delete command in fixed memory areas in portable smartphones, but most of them do not have a destruction command. They are destroyed by using one or more of the suitable methods mentioned above in the section 'Local Systems'.

Optical discs: These are data storage media such as CDs and DVDs. They are destroyed by using physical destruction methods such as burning, breaking into small pieces and melting.

Peripherals such as printers and fingerprint door access systems that have removable data recording media: After verifying that all data recording media have been removed, they are destroyed by using one or more of the suitable methods mentioned above in the section 'Local Systems' depending upon their characteristics.

Peripherals such as printers and fingerprint door access systems that have fixed data recording media: Most of these systems have a delete command, but they do not have

destruction command. They are destroyed by using one or more of the suitable methods mentioned above in the section 'Local Systems'.

Paper and Microfiche Media

As the personal data available in such media is permanently and physically written on the media, the main media is destroyed. During this process, the media is broken into small pieces of incomprehensible size and horizontally and vertically, if possible, by using paper shredders or clippers in a way that cannot be reassembled. Personal data transferred from the original paper format to the electronic media by scanner is ensured to be destroyed by using one or more of the above-mentioned suitable methods, depending upon the electronic media where it is located.

Cloud Systems

During the storage and use of personal data in the above-mentioned systems, it is required to do encryption by using the cryptographic methods and, where possible, separate encryption keys should be used for personal data, particularly for each cloud solution that provides service. When the cloud computing service relationship expires, all copies of the encryption keys required to make personal data usable are destroyed.

DOMESTIC TRANSFER OF YOUR PERSONAL DATA

For the domestic transfer of personal data, minimum one of the following conditions must be fulfilled in accordance with the Article 8 of the Law No 6698:

- Obtaining the explicit consent of the data owner,
- It is clearly prescribed in the laws,
- It is mandatory for the protection of life or bodily integrity of the person or someone else, who is unable to express his or her consent due to actual impossibility or whose consent is not legally recognized,
- It is required to process the personal data of the parties directly in relation with the conclusion or implementation of a contract,
- It is mandatory for the data controller to fulfill its legal obligation,
- The personal data has been made public by the data owner by himself/herself,
- Processing of data is mandatory for the conclusion, use or protection of a right,
- Processing of data is mandatory for the legitimate interests of the data controller, provided that it does not harm the fundamental rights and freedoms of the data owner.

Except for the cases described here, Fer Hotel does not share your personal data with third parties in any way whatsoever. In accordance with the personal data processing conditions and our data processing purposes described above, your personal data is disclosed to:

Authorized public institutions and law enforcement authorities to fulfill our legal obligations prescribed in the laws,

Our suppliers and other natural persons and private law legal entities for the purpose of maintaining our commercial activities, fulfilling the requirements of our contracts and protecting our legitimate interests. The main parties include reservation service providers, payment service providers, IT service providers, security cameras service providers, switchboard service providers, transfer service providers and legal service providers.

OVERSEAS TRANSFER OF YOUR PERSONAL DATA

Fer Hotel discloses personal data in the following cases by obtaining a letter of undertaking that sufficient protection will be provided and the following conditions are fulfilled.

- For the reasons arising from the law or an international treaty,
- If it is mandatory for the implementation of a contract,
- In case of existence of actual impossibility,
- Due to a legal responsibility of Fer Hotel,
- Due to the establishment, protection and use of a right,
- As part of an essential legitimate interest of Fer Hotel

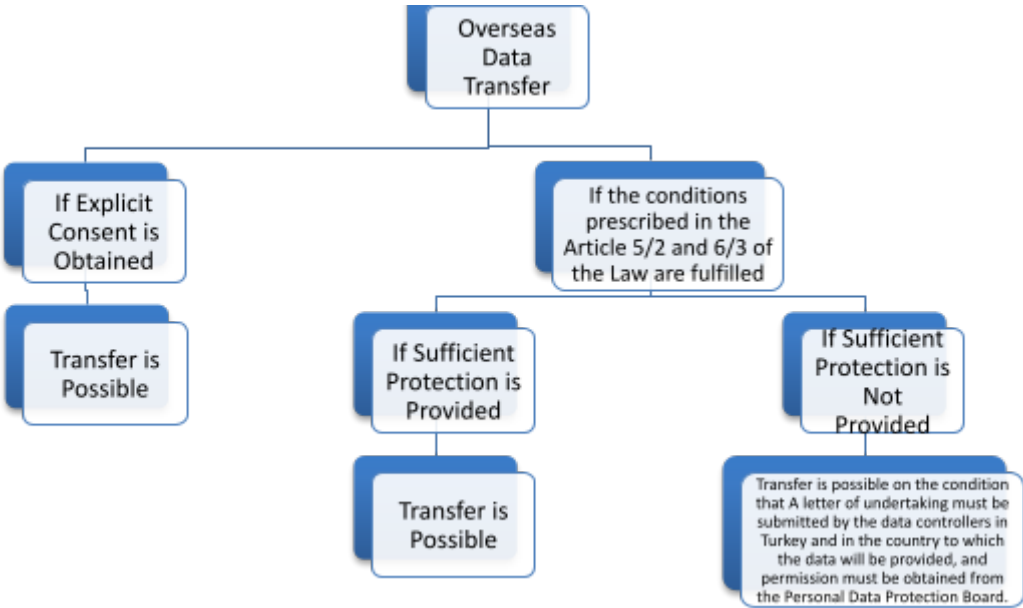
According to the Article 9 of the Law, overseas data transfer is possible in case of:

- Obtaining explicit consent of the data owner,
- Fulfillment of the conditions prescribed in the Law for the data transfer to the countries that provide sufficient protection (the countries which are recognized as safe by the Board) (the conditions prescribed in the paragraph 2 of the Article 5 and the paragraph 3 of the Article 6 of the Law),
- Fulfillment of the conditions prescribed in the Law for the data transfer to the countries that do not provide sufficient protection (the conditions prescribed in the paragraph 2 of the Article 5 and the paragraph 3 of the Article 6 of the Law), on the condition that it is undertaken in writing that sufficient protection will be provided, and permission is obtained from the Board. Data may not be transferred to third parties abroad without obtaining permission from the Board.

If Fer Hotel transfers data to the third parties abroad, who act in the capacity of **data controller**, it submits to the Personal Data Protection Authority a letter of undertaking signed by the both parties, with the minimum conditions determined by the Personal Data Protection Authority, in relation with the fact that the both parties are data controllers. Upon the approval of the Personal Data Protection Authority, such data is transferred. Without this approval, Fer Hotel does not transfer any data to such third parties.

If Fer Hotel transfers data to the third parties abroad, who act in the capacity of **data processor**, it submits to the Personal Data Protection Authority a letter of undertaking executed and signed by the data controller and data processor, with the minimum conditions determined by the Personal Data Protection Authority, in relation with the fact that the both

parties are data controllers. Upon the approval of the Personal Data Protection Authority, such data is transferred. Without this approval, Fer Hotel does not transfer any data to such third parties.



HOW IS YOUR PERSONAL DATA COLLECTED?

The personal data of our customers is collected when they apply to our hotel for a reservation. This application may be made when they come to our hotel, or when they use our website or mobile applications, or when you contact us by phone. Besides, we process your other personal data such as video recordings and wireless internet connections in the common areas during your stay at our hotel. Personal data of our visitors is processed during their visit to our hotel. Video recordings and wireless internet connections are included in the data processed.

The processing of personal data of our employees and interns starts upon their job applications, and continues until their employment contracts expire, by making a request to them in case of necessity. Video and audio recordings in the common areas are processed while they are at the premises. Personal data of the employee candidates is processed during job applications.

The collection of personal data of the representatives and employees of suppliers starts upon signing a contract with them. Their video recordings are processed during their visit to our hotel.

Fer Hotel keeps the IP information that is required to be retained under the Law no 5651. Apart from such IP information, cookies may be used to provide effective website designs and offer website designs and contents better and to enable website users to benefit from

the website in the most effective way. Necessary notifications are made while receiving such personal data.

The legal reasons for Fer Hotel to collect such data are fulfillment of the above-mentioned data processing purposes.

THE MEASURES TAKEN BY US FOR ENSURING DATA SECURITY

Fer Hotel takes all kinds of administrative and technical measures for the security of your personal data within the scope of an information security management system application. The following administrative measures are taken:

- Personal data security policies and procedures have been determined, and the security of personal data is followed up by top management,
- No personal data is processed beyond the intended purpose, and personal data is minimized as much as possible,
- Authorization matrix has been created for the employees,
- Confidentiality commitments are taken from the employees,
- The contracts signed with suppliers and other parties, to whom data is transferred, include data security provisions,
- Necessary security measures are taken in terms of entries and exits to and from the physical environments that contain personal data,
- The security of physical environments that contain personal data against external risks (fire, flood etc.) is ensured.

The following technical measures are taken:

- Cyber security is viewed as a whole, and physical infrastructures, applications and digital environments that contain information are continuously monitored,
- Intrusion detection and prevention systems are used,
- User account management and authorization control system is implemented,
- Firewalls are used,
- Up-to-date anti-virus software is used,
- Access logs to the information systems are kept in a way that prevents any user intervention,
- Personal data is retained upon being backed up, and their security is ensured.

YOUR RIGHTS REGARDING THE PROCESSING OF YOUR PERSONAL DATA

You are always entitled to withdraw the explicit consent that we have received from you regarding our data processing purposes that require your explicit consent. In accordance with the rights granted by legal regulations, you are entitled to:

- know whether your personal data has been processed or not, and if your personal data has been processed, ask for information about processing of such data,

- know the purpose of processing of personal data and know whether such data is used in accordance with the purpose,
- know the third parties inland or abroad, to whom such personal data has been disclosed,
- If your personal data has been processed incompletely or wrongly, ask for correction of it and ask for deletion or disposal of personal data according to the conditions prescribed in the Law and provision of information to third parties, to whom such personal data has been disclosed, in connection with such deletion or disposal,
- object to the occurrence of any negative results about you through analysis of the processed data exclusively by automatic systems,
- ask for the indemnification of the loss suffered by you due to the processing of personal data in violation of the Law.

We have taken all measures to ensure that you can easily use these rights. However, in accordance with the Communiqué on the Procedures and Principles of Making Applications to the Data Controller as published by the Personal Data Protection Board, it is mandatory to specify the following information in your application:

- Name, surname and signature, if a written application is made,
- Turkish identification number for the citizens of the Republic of Turkey,
- Nationality, passport number or identification number, if any, for foreigners,
- Domicile or workplace address to be used for notifications,
- E-mail address, telephone and fax number, if any, to be used for notifications,
- Subject of the request.

You can prepare a petition that contains the foregoing information on your own, or you can use your rights by using the application form available at our website www.ferhotel.com.

Your applications that do not contain any incomplete information will be finalized within maximum 30 days in accordance with the law and honesty rules. In case of any missing information in the application, your application will be responded upon requesting additional information from you.

APPLICATION METHODS

You can submit your requests within the scope of your rights described in the Article 11 of the Personal Data Protection Law No 6698, by using one of the following methods in accordance with the Article 13 of the Law and the Article 5 of the Communiqué on the

Procedures and Principles of Making Applications to the Data Controller. Your request will be responded within 30 days in accordance with the Article 13 of Law No 6698.

The applicant will make an application together with the papers and documents that will prove his/her identity. If these documents cannot be verified, no positive response will be given. For more information, you can review our Personal Data Protection Policy available at www.ferhotel.com.

The response to the application is sent by using the method that has been used to make the application, unless otherwise indicated. If you request, response can be also sent by using any of the methods indicated above.

Applications are free of charge. However, if we have to incur expense to send response, a fee may be charged according to the tariff determined by the Personal Data Protection Board. If it is concluded that Fer Hotel has made a mistake according to the subject of request, the fee charged is refunded.

It is possible to make your application by selecting one of the 5 methods described below.

Application Method	Application Requirements	Application Address	Other Requirements
Personal Application	You can make an application to the address where our hotel operates, personally by verifying your identity or by submitting a power of attorney through a representative. The application may be also made with an application form or a petition, but it must bear original signature.	Fer Hotel Molla Fenari Mah. Türbedar Sk. No: 12 İç Kapı No: 1 Fatih/ İSTANBUL	The application will be submitted in a closed envelope. The statement "Information Request under the Personal Data Protection Law" must be written on the envelope.
Application by Post	You can make an application by sending the application form or petition that bears original signature through post. If the application is made by a representative based on a notarized signature circular, the original power of attorney must be also placed into the envelope.	Fer Hotel Molla Fenari Mah. Türbedar Sk. No: 12 İç Kapı No: 1 Fatih/ İSTANBUL	The statement "Information Request under the Personal Data Protection Law" must be written on the envelope.
Application through Notary Public	You can make an application personally or through a representative via notary public. In this application, the method of receiving the answer must be also indicated.	Fer Hotel Molla Fenari Mah. Türbedar Sk. No: 12 İç Kapı No: 1 Fatih/ İSTANBUL	

Application Through Registered Electronic Mail (KEP)	<p>You can make an application by sending your electronically-signed petition from your KEP address. Unless otherwise indicated, the answer will be sent to your KEP address.</p>	@hs01.kep.tr	<p>“Information Request under the Personal Data Protection Law” must be indicated in the Subject section.</p>
Application Through Electronic Mail	<p>If you have provided us with your e-mail address during check-in to the hotel, you can apply through this e-mail address. If you have not provided your e-mail address, you can request information via e-mail by indicating your reservation number (voucher), name, surname, date of accommodation at the hotel and room number.</p>	fom@ferhotel.com	<p>“Information Request under the Personal Data Protection Law” must be indicated in the Subject section.</p>