

DATA PROTECTION INFORMATION

IMOLA HOTEL PLATAN

- valid from 2023.01.01.

IMOLA VENDEGHAZ KFT. (3300 Eger, 6. Street Kossuth Lajos, represents: managing director Imre Toth; e-mail: recepicio@imolaplattan.hu; tel.: 36/513-888), as the operator of the IMOLA HOTEL PLATAN accommodation (hereinafter referred to as the Service Provider/data controller), as a data controller, acknowledges the content of this legal information as binding. It undertakes to ensure that its data management in relation to its service complies with the provisions set out in this information sheet and the applicable legislation.

The scope of this information sheet covers data management on the Service Provider's website (www.imolaplattan.hu) and its subdomains. The data protection information is continuously available on the following website: <http://www.imolaplattan.hu/>

When providing services at the Data Controller's accommodation, the Service Provider acts based on the internal data protection regulations.

Amendments to the information sheet and the internal data protection policy will enter into force upon publication on the above website.

The data management principles of the service provider are in accordance with the applicable data protection legislation, with the following:

- CXII of 2011 Act - on the right to informational self-determination and freedom of information (hereinafter: Info.tv.)
- CVIII of 2001 Act - on certain issues of electronic commercial services and services related to the information society.
- XLVII of 2008 law - on the prohibition of unfair trade practices towards consumers.
- XLVIII of 2008 Act - on the basic conditions and certain limitations of economic advertising activity.

Definitions

1. *concerned/guest/User*: natural person identified or identifiable based on any information.
 - a) *identifiable natural person*: the natural person who directly or indirectly has an identifier, such as a name, identification number, location data, online identifier or a physical, physiological, genetic, mental, economic, cultural or social identity of the natural person or can be identified based on several factors.
2. *personal data*: any information about the data subject.
3. *special data*: all data belonging to special categories of personal data, i.e., personal data referring to racial or ethnic origin, political opinion, religious or worldview beliefs or trade union membership, as well as genetic data, biometric data aimed at the unique identification of natural persons, health data and personal data concerning the sex life or sexual orientation of natural persons.
4. *consent*: a voluntary, definite and clear statement of the data subject's will based on adequate information, with which the data subject indicates through a statement or other behaviour that clearly expresses his will that he gives his consent to the processing of his personal data;
5. *data controller*: the natural or legal person or organization without legal personality who - within the framework defined by law or a mandatory legal act of the European Union - independently or together with others determines the purpose of the data management, the data

management (including the device used) makes and implements relevant decisions or has them implemented by the data processor.

6. *data management*: regardless of the procedure used, any operation performed on the data or the set of operations, including in particular collection, recording, recording, organization, storage, change, use, query, transmission, disclosure, coordination or connection, locking, deletion and destruction, and preventing further use of the data, taking photographs, audio or video recordings, and recording physical characteristics suitable for identifying the person (e.g. fingerprint or palm print, DNA sample, iris image);
7. *data transfer*: making the data available to a specific third party.
8. *disclosure*: making the data available to anyone.
9. *data deletion*: rendering the data unrecognizable in such a way that its recovery is no longer possible.
10. *restriction of data processing*: blocking of the stored data by marking it for the purpose of restricting the further processing of the data.
11. *data destruction*: complete physical destruction of the data carrier containing the data.
12. *data processing*: the set of data processing operations performed by a data processor acting on behalf of or at the request of the data controller.
13. *data processor*: a natural or legal person, or an organization without legal personality, who - within the framework and conditions defined by law or a mandatory legal act of the European Union - processes personal data on behalf of or at the direction of the data controller.
14. *data controller*: the body performing a public task, which produced data of public interest that must be published electronically, or whose operation generated this data.
15. *data provider*: the body performing a public task, which - if the data controller does not publish the data himself - publishes the data provided by the data controller on the website.
16. *data file*: the totality of the data managed in one register.
17. *third party*: a natural or legal person, or an organization without legal personality, who is or is not the same as the data subject, the data controller, the data processor or the persons who carry out operations aimed at processing personal data under the direct control of the data controller or data processor.

Basic principles

1. Personal data can only be processed for specific purposes, in order to exercise rights and fulfil obligations. In all stages of data management, the purpose of data management must be met, the collection and management of data must be fair and legal.
2. Only personal data that is essential for the realization of the purpose of data management and suitable for achieving the purpose can be processed. Personal data can only be processed to the extent and for the time necessary to achieve the purpose.

Data handling

1. Legal basis for data management: Info tv. CLVI of 2016 on the state tasks for the development of tourist areas based on § 5 (1) point a). Act 9/H. § (1) of the public interest goal, and the Info tv. Consent of the data subject based on point b) of section 5 (1).
2. Scope of processed data: surname and first name, surname and surname at birth, place and time of birth, gender, citizenship, mother's surname and surname at birth, identification data of the personal identification document or travel document, address of the accommodation service, starting and expected and actual end date.

3. Duration of data management: IMOLA VENDEGHAZ Kft., as a data controller, processes the data specified in point 2 of the user of the accommodation service for the purpose specified in point 1 until December 31 of the 7th year following the given year.
4. The deletion or modification of personal data can be initiated in the following ways:
 - by post at Imola Hotel Platan (3300 Eger, 7. Street Csakany)
 - via e-mail at recepcio@imolaplattan.hu.
5. We inform our Users that the court, the prosecutor, the investigative authority, the infringement authority, the public administrative authority, the data protection commissioner, or other bodies, based on the authorization of the law, may request the transfer of data managed by the accommodation service provider, indicating the purpose of the data request, which the accommodation provider provides free of charge.
6. The accommodation provider manages the Users' personal data for the purpose of providing the service (full use of the website, e.g., request for a quote, room reservation), only to the extent and for the time necessary for this. It complies with this purpose at all stages of data management.
7. It also manages the personal data that is technically necessary for the provision of the service. If the personal data was recorded with the consent of the User, the Service Provider shall, unless otherwise provided by law,
 - a) for the purpose of fulfilling the relevant legal obligation, or
 - b) For the purpose of asserting the legitimate interests of a service provider or a third party, if the assertion of this interest is proportional to the limitation of the right to protect personal data, it can be processed without further separate consent and after the withdrawal of the User's consent.
8. In addition, the Service Provider only collects information about the Users (IP address, time of use, visited website, browser program, and one or more cookies enabling the unique identification of the browser) which is used exclusively for the development and maintenance of the Services and for statistical purposes. The Service Provider uses data processed for these statistical purposes only in a form that is not suitable for personal identification. To improve the quality of the Services, the Service Provider stores a file containing a series of characters on the User's computer, so-called places a cookie if the User consents to this. If the User does not agree to this, he/she shall notify the data controller at the contact details specified in point 4 of the "Data Management" chapter.
9. The Service Provider transfers the personal data it manages to third parties only for the purpose of developing and/or operating some of the Service Provider's services - used by the User. The Service Provider does not use the personal data it manages for the purposes of a third party and does not abuse them in any other way.
10. By using the Service, the User consents to the Service Provider collecting and managing his personal data in accordance with the provisions of this data protection information, for the purpose of fully providing the service.

Legal consequences of failure to provide data

In the absence of providing the personal data of the person concerned, the service provider will refuse the accommodation service.

Newsletter

1. XLVIII of 2008 on the basic conditions and certain limitations of economic advertising activity. pursuant to § 6 of the Act, by accepting these regulations, the User expressly consents in advance

to contact the Service Provider with its advertising offers and other mailings at the contact details provided during registration (e.g., e-mail address or telephone number).

2. Furthermore, with the provisions of this information in mind, the Customer consents to the Service Provider handling his personal data necessary for sending advertising offers
3. The Service Provider does not send unsolicited advertising messages if the User indicates this, and the User can unsubscribe from the sending of offers free of charge without limitation or justification. In this case, the Service Provider will delete all personal data necessary for sending advertising messages from its records and will not contact the User with further advertising offers. Users can unsubscribe from advertisements by clicking on the link in the message.
4. Purpose of data management: sending electronic newsletters containing economic advertising messages to the User, information on current information and products.
5. Legal basis for data management: the voluntary consent of the person concerned and XLVIII of 2008 on the basic conditions and certain limitations of economic advertising activities. § 6 (5) of the Act.
6. Scope of processed data: name, e-mail address, date, time.
7. Duration of data management: until withdrawal of consent, i.e. until unsubscription.

Camera system

1. A video surveillance system operates in the Imola Hotel Platan, which records recordings for security and property protection reasons.
2. The legal basis for data management: the image material is used by Imola Vendeghaz Kft. exclusively in accordance with CXII of 2011 on the right to self-determination of information and freedom of information. in addition to the enforcement of data protection rights according to the law, as well as CXXXIII of 2005 on the rules for the protection of persons and assets, as well as private investigative activities. it is managed and recorded in compliance with the restrictive provisions defined by law.
3. Deletion of data: The service provider ensures the safe storage of recordings on site for a maximum of 30 days from the date of recording. The recordings are then automatically destroyed and deleted.
4. The recorded image information will only be released by the Service Provider to the court or other authorities within the time limit specified in point 3, upon their official request.
5. The person whose right or legitimate interest is affected by the recording of the image or other personal data may, within fifteen days from the recording of the image or other personal data, request that the Service Provider not destroy or delete the data by proving his right or legitimate interest.
6. By entering the area of the Imola Hotel Platan, the User gives his consent to the processing of his image as personal data by the Service Provider
7. Imola Vendeghaz Kft. protects the databases managing recorded recordings with a password and access to them from unauthorized access by establishing appropriate authorization levels. The protection measures taken are constantly checked for efficiency and safety.

Data security

1. The Service Provider takes all necessary security steps, organizational and technical measures to ensure the highest level of security of personal data and to prevent their unauthorized change, destruction, and use.

2. The Service Provider takes all necessary measures to ensure data integrity, i.e., to ensure the accuracy, completeness, and up-to-date status of the personal data it manages and/or processes.
3. The Service Provider uses appropriate measures to protect the data, especially against unauthorized access, alteration, transmission, disclosure, deletion, or destruction, as well as against accidental destruction, damage, and inaccessibility resulting from changes in the technology used. The Service Provider therefore reserves the right to inform its customers and partners about security holes in its system if it detects a security hole on the part of its customers or partners, and at the same time restrict access to the Service Provider's system and services until the security hole is eliminated.

The rights of the data subject

The data subject is entitled to, in relation to the personal data managed by the data controller and the data processor acting on its behalf or on its instructions:

- a)* receive information about the facts related to data management before data management begins (hereinafter: **right to prior information**),
- b)* at your request, the data controller will make your personal data and the information related to their management available to you (hereinafter: **right of access**),
- c)* at your request, as well as in other cases specified in Info TV, your personal data may be corrected or supplemented by the data controller (hereinafter: **right to correction**),
- d)* at your request, as well as in other cases specified in Info tv, the processing of your personal data is restricted by the data controller (hereinafter: **the right to restrict data processing**),
- e)* at your request, as well as in other cases specified in Info tv, your personal data will be deleted by the data controller (hereinafter: **right to deletion**).

Right to prior information

In order to enforce the right to prior information, the data controller shall immediately make available to the data subject before the start of the data processing operations carried out by him or by the data processor acting on his behalf or on his instructions, or at the latest after the start of the first data processing operation

- a)* the name and contact details of the data controller and, if a data processing operation is performed by a data processor, the data processor,
- b)* the name and contact details of the data protection officer,
- c)* the purpose of the planned data management and
- d)* description of the rights to which the data subject is entitled, as well as the method of enforcing them.

Right of access

To assert the right to access, the data controller shall inform the data subject at his request as to whether his personal data is being processed by the data controller himself or by a data processor acting on his behalf or at his direction.

Right to rectification

In order to enforce the right to rectification, if the personal data managed by him or by a data processor acting on his behalf or on his instructions is inaccurate, incorrect or incomplete, he shall - especially at the request of the data subject - clarify or correct it immediately, or if it is compatible with the purpose of the data management, supplemented by additional personal data provided by the data subject or a statement attached to the personal data processed by the data subject.

The data controller is exempted from the obligation defined here if

- a) accurate, correct or complete personal data are not available to you and the data subject does not make them available to you, or
- b) the authenticity of the personal data provided by the data subject cannot be established beyond doubt.

Right to restriction of data processing

To assert the right to restrict data processing, the data controller shall limit data processing to the data processing operations defined in law, international treaty, or a mandatory legal act of the European Union for the purpose of asserting the legitimate interests of the data subject,

- a) if the data subject disputes the accuracy, correctness or completeness of the personal data processed by the data controller or by the data processor acting on his behalf or at his direction, and the accuracy, correctness or completeness of the processed personal data cannot be established beyond doubt, for the duration of the clarification of the existing doubt,
- b) if, as defined in the scope of the right to erasure, the data should be deleted, but based on the written statement of the data subject or the information available to the data controller, it can be reasonably assumed that the deletion of the data would harm the legitimate interests of the data subject, for the duration of the existence of the legitimate interest justifying the non-deletion,
- c) if, as defined in the scope of the right to erasure, there is room for erasing the data, but it is necessary to preserve the data as evidence during investigations or procedures defined by law - especially criminal proceedings - carried out by or with the participation of the data controller or other body performing public duties, this investigation or procedure is final, or until its final closure,
- d) if, as defined in the scope of the right to erasure, there is room for erasure of the data, but in the case of international data transfer or data management for the purpose of law enforcement, the data must be preserved for the purpose of fulfilling the documentation obligation, for 10 years after the erasure of the processed data.

Right to erasure

To enforce the right to deletion, the data controller shall immediately delete the personal data of the data subject if

- a) data management is illegal, so especially if the data management
 - aa) contrary to the basic principles of handling personal data,
 - ab) its purpose has ceased, or the further processing of the data is no longer necessary to achieve the purpose of the data processing,
 - ac) the period defined by law, international treaty or a binding legal act of the European Union has passed, or
 - ad) its legal basis has ceased and there is no other legal basis for processing the data,
- b) the data subject withdraws his consent to data processing or requests the deletion of his personal data unless the data is processed by Info tv. It is based on point a) or c) of paragraph (1) of § 5 or point b) of paragraph (2),
- c) the deletion of the data has been ordered by legislation, a legal act of the European Union, the Authority, or the court, or
- d) within the framework of the right to limit data processing, the period specified in points b) -d) listed there has passed.

Legal remedy

1. If the data controller rejects the data subject's request to correct, delete or limit the processing of personal data handled by the data controller or the data processor acting on his or her behalf, the data controller shall inform the data subject in writing immediately.
 - a) about the fact of rejection, its legal and factual reasons, as well as
 - b) about the rights of the data subject, as well as how to enforce them, and about whether the right to correct, delete or limit the processing of personal data handled by the data controller or the data processor acting on his or her behalf or at the request of the **National Data Protection and Freedom of Information Authority**
(1055 Budapest, 9-11. Street Falk Miksa; postal address: 1363 Budapest, Pf.: 9.; hereinafter: Authority).
2. To assert his rights, the data subject
 - a) the Authority may initiate an investigation in order to examine the legality of the data controller's action if the data controller restricts the enforcement of the data subject's rights or rejects his request to enforce these rights, and
 - b) you can request the conduct of the official data protection procedure of the Authority if, in your opinion, the data manager, or the data processor acting based on his or her mandate, violates the regulations regarding the handling of personal data, as defined in legislation or in a binding legal act of the European Union, during the processing of your personal data.
3. The data subject may go to court against the data controller or - in connection with the data processing operations within the scope of the data processor's activities - the **data processor**, if, according to his judgment, the data controller or the data processor entrusted by him or acting on the basis of his instructions has used his personal data in accordance with the law or treats it in violation of the regulations defined in the binding legal act of the European Union. The lawsuit may be initiated by the person concerned - at his or her choice - before the competent court based on his or her place of residence.

IMOLA VENDEGHAZ KFT.