PRIVACY POLICY

HOTEL PEST INGATLANHASZNOSÍTÓ ÉS ÉPÍTŐIPARI LLC

Valid from: 25 May 2018

I. PRIVACY POLICY

II. Introduction & basic policies

When processing personal data, **HOTEL PEST Ingatlanhasznosító és Építőipari LLC** (head offices: 1065 Budapest, Paulay Ede. u. 31., Company Registration Number: 01-09-464967, hereinafter referred to as the "**Data Controller**" or the "**Company**") as Data Controller acts in compliance with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (hereinafter referred to as the "**Regulation**" or the "**GDPR**") as well as all applicable laws.

The Data Controller respects Your (hereinafter referred to as the "**Data Subject**") personal data protection rights. This Policy summarizes, in a compact and simple way, the type of information we collect, the ways we use them, the tools we use as well as the privacy and enforcement options of the Data Subject with respect of data protection.

Detailed regulation is contained in said Regulation and related legal acts. For further information, read the Regulation or contact the Data Controller using the contact information provided in this Policy.

The Data Controller acts in accordance with the following principles in its data management activities.

The Data Controller shall, before beginning the data management, inform the Data Subject of the data management rules as required.

The Data Controller collects, stores and uses personal data only in accordance with the requirements related to the purpose of data management.

The collected Personal Data is always suitable, relevant and appropriate for the given purpose, keeping the Data Controller in compliance with the principle of data minimization.

For reasons of data accuracy, the Data Controller shall take the reasonable steps necessary for ensuring that the personal data of the Data Subject are complete, accurate, up-to-date and reliable to the extent appropriate for the purpose.

The Data Controller uses personal data for marketing purposes solely with the consent of the Data Subject and provides an option for the Data Subject to prevent such communication.

The Data Controller shall take proportionate and comprehensive steps to ensure the protection of the personal data of the Data Subject, as detailed in this Privacy Policy, including the cases where such data are transmitted to third parties. Data must not be forwarded to third parties without the express prior consent of the Data Subject.

III. Interpretative provisions

- Regulation, GDPR: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data;
- Information Act: Act CXII of 2011 on informational self-determination and freedom of information
- Private Protection Act: Act CXXXIII of 2005 on persons and property protection and on the activity of private detectives
- Tax Administration Act: Act CLI of 2017 on the tax administration procedure
- Accounting Act: Act C of 2000 on accounting;
- VAT Act: Act CXXVII of 2007 on value added tax;
- The Civil Code: Act V of 2013 on the Civil Code;
- 'Personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
- Special data: personal data relating to racial origin, nationality, political opinion or party affiliation, religious or other beliefs, membership in an advocacy organization, sexual life, state of health, addiction or criminal records.
- 'Genetic data' means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;
- 'Biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;
- 'Data concerning health' means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;
- 'Processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
- 'Controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;
- 'Processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;
- 'Recipient' means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients;
- 'Third party' means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorized to process personal data;

- ‘Consent’ of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;
- 'Profiling' means any form of automated personal data processing where personal data are used to evaluate certain personal characteristics associated with a natural person, in particular those related to analyzing or forecasting indicators of work performance, economic status, health status, personal preferences, interests, reliability, behavior, residence or movement;
- ‘Personal data breach’ means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed;
- Authority: National Authority for Data Protection and Freedom of Information of Hungary, www.naih.hu

IV. Details and contact information of the Data Controller (Provider)

Designation of the Data Controller:	HOTEL PEST Ingatlanhasznosító és Építőipari Korlátolt Felelősségű Társaság
Registered office:	1065 Budapest, Paulay Ede.u.31.
Postal address:	1065 Budapest, Paulay Ede.u.31.
Company Registration Number	01-09-464967
Phone:	+36 (1) 343 11 98
Fax:	+36 (1) 343 11 98
E-mail:	info@casatibudapesthotel.com

V. The purpose of data management, the scope of controlled data, the duration of data management, the persons entitled to access the data with respect of the Data Subjects (hotel guests) using the services provided by the Data Controller, the use of the www.casatibudapesthotel.com website

1. The purpose and legal basis of data management

The Data Controller manages personal data during the provision of services primarily for reasons of **intending to conclude a contract**, **perform a contract** or **in its own legitimate interest** as well as for security reasons, such as ensuring the CCTV surveillance of its sites/head offices (additional information provided later in this document).

The Data Controller manages personal data **on the basis of statutory requirements** in the following cases: the fulfillment of invoicing, bookkeeping and accounting obligations (the Accounting Act, the VAT Act, the Tax Administration Act).

The Data Controller manages personal data **based on the express and voluntary consent given by the Data Subject** in the following cases: Sending a newsletter, keeping in touch – responding to requests made by the Data Subject via the web interface or in email, for marketing purposes, for recording and collecting information related to visitor behavior –, application of anonymous user IDs (cookies), filling out a satisfaction questionnaire.

2. The purpose of data management, the duration of data management, the persons entitled to access the data

With reference to the indicated legal basis, the Data Controller collects and manages the personal data as specified in the following table(s) for the designated retention period:

	Designation of personal data	Retention/storage period
Data managed for intending to conclude a contract or performing a contract	Full name, title, date of arrival, date of departure, number of adults in the same room, type of room, full credit card details (name on the card, number of the card, expiration date), arrival time, comments – eventual preferences, address, phone number, e-mail address, invoicing details (name, invoicing address), designation of service, service price, total invoice amount, personal ID number, passport number for visitors from third countries, birth data (place and time).	The retention period lasts until the termination of legitimate interest or, according to relevant statutory regulations (Article 6:22 of the Civil Code), 5 years

	Designation of personal data	Retention/storage period
Data managed for a legitimate interest	Name and e-mail address	3 days after contract fulfillment

The email address of the Data Subject will be managed in order to allow the Data Controller to send an e-mail after the Data Subject's stay, as "the data management is necessary to enforce the legitimate interests of the Data Controller, unless priority is given to the fundamental rights and freedoms of the Data Subject over such interests." In this case, the Data Controller's legitimate interest lies in providing high-quality service, and therefore the Data Controller considers that the email sent after the stay of the Data Subject does not violate the his/her fundamental rights.

Data managed due to statutory requirements	Designation of personal data	Retention/storage period
	Details of accounting documents	The retention period is the time stipulated in the applicable law (8 years after starting to use the service).

	Designation of personal data	Retention/storage period
Data managed with the voluntary consent of the Data Subject (*The options for withdrawing the consent are found in the later sections of this Policy*)	Name, email address, phone.	Retention period until subscription is cancelled or consent is withdrawn
	When using the Website: the IP address of the Data Subject's computer; starting and ending point of the time spent visiting the Website; depending on the settings of the Data Subject's computer, the type of the browser and operating system; the details related to the activity of the Data Subject on the Websites.	Until the expiry of the (technical or optional) cookie or until the cookie is deleted by the Data Subject.

3. The Data Controller forwards the data to the employees and agents of the Company performing customer service and commercial duties as well as employees and data processors performing accounting and taxation duties as recipients.

4. The Data Controller informs the visitors of the Website that, by using the Website (without contact by the Data Subject via the Internet), data collection and data management are carried out using anonymous User IDs (cookies) accepted by the Data Subject. The Data Controller summarizes the essentials of cookies in the following section.

The Data Controller may use alphanumeric information packages sent by the web server, with variable content and stored on the user's computer for a determined period of validity, known as cookies, for accessing the services and the Website.

A cookie is a sequence of signals used for unique identification and the storage of profile information that the service providers store on the Data Subject's computer. It is important to know that such sequences are not suitable for identifying the Data Subject in any way, but are capable of identifying the Data Subject's computer. On the Internet, information related to persons and personalized services can only be provided if service providers are able to uniquely identify their customers' habits and needs. Service providers use anonymous identification in order to learn more about the customers' information usage habits, for the further improvement of the quality of services and offering customization options to customers.

Cookies are used, for example, for storing the settings and preferences of Data Subjects, logging in, displaying personalized ads and analyzing the Website's operation. For these purposes, we use services to collect and track information about such activities of Data Subjects as relevance, recommendations, searches, access as well as the key and the most commonly used functions.

Flash cookies are used by website operators to tell, for example, whether the Data Subject has ever visited the website before or to identify the functions and services that the Data Subject is most interested in. Search and flash cookies improve the online experience by retaining the information preferred by the Data Subject while browsing on a specific page. Neither the search nor the flash cookies are suitable for identifying the person of the Data Subject, and the Data Subject has the option to reject browser cookies

through the settings of the browser; however, the Data Subject will not be able to take advantage of all the features of the Website without using such cookies.

If the Data Subject does not want to have such identifiers stored on his/her computer, the browser can be configured in such a manner as to prevent the storage of the unique identifier and the Data Subject has the possibility to withdraw his/her permission at any time and to delete the unique identifier; however, in this case, it is possible that the services will not be available or will be available in a different form than if the storage of identifiers were allowed.

Services are used by a large number of users in a variety of software and hardware environments with different uses and scope. Service development can best be tailored to the needs and facilities of users if the website operator gets a comprehensive view of their usage habits and needs. However, due to the large number of users, in addition to personal contact and request for feedback, collecting and analyzing information related to the running environment of habits and services is an efficient complementary method.

VI. The purpose of data management; the scope of managed data; the duration of data management; the persons entitled to access the data with respect of contact persons of business organizations working with the Data Controller as economic (business) partners as Data Subjects

1. The purpose and legal basis of data management

The Data Controller handles personal data **in its own legitimate interest** in the following cases: intending to conclude a contract, perform a contract or for security reasons, such as ensuring the CCTV surveillance of its sites/head offices (additional information provided later in this document).

The Data Controller manages personal data **based on the express and voluntary consent given by the Data Subject** in the following cases: Sending newsletters (marketing).

2. The purpose of data management, the duration of data management, the persons entitled to access the data

With reference to the indicated legal basis, the Data Controller collects and manages the personal data as specified in the following table(s) for the designated retention period:

	Designation of personal data	Retention/storage period
Data managed for a legitimate interest	Name, position held at the partner company, email address, phone number	The retention period is until the termination of legitimate interest or, according to relevant statutory regulations (Article 6:22 of the Civil Code), 5 years

Data managed with the voluntary consent of the Data Subject (*The options for withdrawing the*	Designation of personal data	Retention/storage period
	Name, position held at the partner company, email address, phone number	Retention period until subscription is cancelled or consent is withdrawn

consent are found in the later sections of this Policy)		

3. The Data Controller forwards the data to the employees of the Company performing customer service and commercial duties as well as employees and data processors performing accounting and taxation duties as recipients.

VII. The purpose of data management; the scope of managed data; the duration of data management; the persons entitled to access the data with respect of Data Subjects applying for a job at the Data Controller

1. The purpose and legal basis of data management

The Data Controller manages Personal Data **based on the express and voluntary consent given by the Data Subject** in the following cases: Recruitment.

Applications for a job posting via email is regarded by the Data Controller as expressed and voluntary consent as there is no technical possibility for demonstrating the voluntary character in any other way.

2. The purpose of data management, the duration of data management, the persons entitled to access the data

With reference to the indicated legal basis, the Data Controller collects and manages the personal data as specified in the following table(s) for the designated retention period:

Data managed with the voluntary consent of the Data Subject (*The options for withdrawing the consent are found in the later sections of this Policy*)	Designation of personal data	Retention/storage period
	name, email address, phone number, CV, photo	Until consent is withdrawn, but until the position is occupied at the latest

3. The Data Controller forwards the data to the employees of the Company performing customer service and commercial duties as well as employees performing the management of different business units at the Company as recipients.

VIII. Operating an electronic surveillance system.

1. The purpose and legal basis of data management

The Data Controller manages the Data Subject's personal data based on **expressed and voluntary consent and** (for employees) **legitimate interest** in order to ensure the security of the Data Controller's head office/sites, to safeguard the assets of the Data Controller, to safeguard the physical integrity and property of the Data Controller's employees and visitors or to investigate the circumstances of accidents and legal offenses. The consent of the Data Subject is manifested in the act that he/she enters the premises

of the Data Controller in spite of being informed about active camera surveillance, as there is no technical possibility for demonstrating the voluntary character in any other way.

The Data Controller carries out the activity in compliance with provisions contained in Act CXXXIII of 2005 on persons and property protection and on the activity of private detectives (the Private Protection Act).

2. The purpose of data management, the duration of data management, the persons entitled to access the data

With reference to the indicated legal basis, the Data Controller collects and manages the personal data as specified in the following table(s) for the designated retention period:

Data managed with the voluntary consent of the Data Subject or in legitimate interest (*The options for withdrawing the consent are found in the later sections of this Policy*)	Designation of personal data	Retention/storage period
	Picture or video recording of a natural person	Termination of legitimate interest or 3 days after the date of recording according to relevant statutory regulations

At the request of the Data Subject, he/she may access recordings of his/her own person in the presence of one of the persons indicated above. In all cases, access must be requested in writing from the administrator. In all cases, the Data Controller is required to record the access and the record must be stored by the company for 1 year.

3. The Data Controller may forward data to the following recipients:

The records may only be accessed by the employees of the Data Controller and the designated employees of the Data Processor(s). Footages recorded previously by the electronic surveillance system may only be accessed by the designated Data Protection Officer, the system administrator and the managing director.

IX. Social media (Facebook, Instagram)

Facebook/Instagram users may subscribe to the feed posted on the message board of the user account maintained by the Company by clicking on the 'like' or 'follow' link, they may unsubscribe by clicking on the 'dislike' link and they may delete unwanted news posted on the message board by changing the settings of the message board. The Company has access to the profile of its 'followers', but does not record or manage any related details in its internal system.

The purpose of data management: Sharing the contents related to services offered by the Company/the Company's operation; announcing diverse news; contact. By using Facebook pages, the Data Subject may receive the latest news about the Company.

The legal basis for data management is the voluntary consent of the Data Subject, which can be withdrawn at any time by cancelling the subscription. The withdrawal will not affect the earlier legal data management. If consent is withdrawn, the Data Subject will cease to receive news alerts and the Company's news will not appear in the Data Subject's feed, but the feed will remain accessible as the site is public.

The data management lasts until the Data Subject terminates his/her subscription. Data is not forwarded and Data Processors are not employed.

Facebook and Instagram are data controllers who are independent from the Data Controller. For information about the data management policies of Facebook, please see the privacy policy posted on the following links:

1. https://www.facebook.com/policies/cookies/
2. https://www.facebook.com/about/privacy/update

Instagram's data management policy is accessible at the following link:

help.instagram.com

X. Lottery

From time to time, the Data Manager organizes prize games in cooperation with a third party partner company. Participation in the lottery is possible after an application on paper or online (on the website or the Facebook page), usually requiring the following information: Name, address, phone number, email address.

In certain cases, not all details listed above are required, such as in Facebook lotteries, or the list of required information might be different, meaning that the scope of data is subject to change.

The purpose of data management: Organizing a prize game and keeping in touch to ensure that the winner safely receives the prize.

The legal basis for data management: **The consent of the Data Subject**. The Data Subject may, at his/her sole discretion, withdraw his/her consent by way of a letter sent to the Data Controller's e-mail address or any other contact. The withdrawal will not affect the earlier data management.

The consent is a prerequisite for participating in the lottery.

The duration of data management: Data management lasts until the end of the prize game and the managed data is deleted within 30 days after the draw, with the exception of the winner(s) and the substitute winner(s). If necessary, the personal data of winners/substitute winners will be kept by the Company for 8 years, in accordance with the applicable tax and accounting regulations, and will be deleted when the term expires.

Information about eventual data transmission and data processors as well as any details related to data processing other than those contained in this Policy will always be provided by the Data Controller in the context of the lottery.

XI. Data security

In accordance with its obligation under the Information Act, the Data Controller will do its utmost to ensure the security of the Data Subject's information and takes all necessary technical and organizational measures and establish all procedural rules that are required for the implementation of the Information Act as well as all other relevant data protection and confidentiality rules. Information stored in the Data

Controller's database about the Data Subjects may only be accessed by the Data Controller's authorized personnel.

The services contain cloud-based applications as well. Cloud applications are typically of an international or cross-border nature and are used for data storage, among other things, when the information is not stored on the Data Controller's computer/corporate IT center, but a server center located elsewhere in the world. The main advantage of cloud applications is that they provide substantially independent, highly secure and flexible storage and processing capacity that is independent of geographic location.

The Data Controller shall select its cloud service providers with the utmost care and makes every effort to conclude a contract that is in line with the data security interests of the Data Subjects, to be transparent to their data management principles and to check data security on a regular basis.

It is possible that the Data Controller's website contains references or links to pages maintained by other providers (including buttons or logos for login or sharing options), where the Data Controller has no influence whatsoever on the practices of the management of personal information. The Data Controller draws the attention of those concerned that by clicking on such links, they may be transferred to other service providers. In all such cases, we recommend reading the data management policies of the respective pages. This Privacy Policy applies only to data management carried out by the Data Controller. If you modify or delete any of your data on said external websites, it will not affect data management by the Data Controller, and all such modifications must be made on the Website as well.

XII. Access, modification, correction and portability of personal data

1. Access

The Data Subject is entitled to receive feedback from the Data Controller as to whether his/her Personal Data is being processed and, if such processing is in progress, he/she has the right to access any such Personal Data as well as the following information:

1.1. the purpose of data management;
1.2. the affected categories of Personal Data; and
1.3. the categories of recipients with whom the Personal Data may be or will be shared.

2. Modification and correction

The Data Subject is entitled to request the Data Controller to correct any inaccurate Personal Data without undue delay. Taking into account the purpose of data management, the Data Subject is entitled to request the completion of any incomplete Personal Data, including by means of a supplementary statement.

3. Portability

The Data Subject has the right to receive the Personal Data provided by him/her to a Data Controller in a commonly used, machine-readable format, and has the right to transmit any such data to another Data Controller without this being obstructed by the Data Controller who had initially received his/her Personal Data, if:

3.1. the data management is based on a voluntary contribution or a contract where the Data Subject is one of the parties; and
3.2. the data management is automatic.

XIII. The deletion and limitation of personal data and the right to object

1. Deletion

(1) The Data Subject is entitled to request the Data Controller to delete his/her Personal Data without undue delay, and the Data Controller is obliged to delete all Personal Data of the Data Subject without undue delay, for one of the following reasons:

a) the Personal Data is no longer required for the purpose for which they were collected or otherwise managed;
b) the Data Subject has contacted the Customer Service to withdraw the voluntary consent given for data management and there is no other legal basis for the data management;
c) the Data Subject objects to the data management due to concerns related to his or her own situation or direct business acquisition and there is no overriding legitimate reason for data management;
d) the Personal Data have been unlawfully managed;
e) the EU or national law on Personal Data with respect to the Data Controller requires the deletion for compliance with legal obligations; or
f) the Personal Data was collected in connection with the direct provision of information society-related services for children.

(2) If the Data Controller has disclosed the Personal Data and is required to delete them under paragraph (1), the Data Controller is required to take all reasonable steps with respect of the available technology and implementation costs, including the technical measures, to inform the Data Controllers managing the data that the Data Subject has requested the deletion of links to these Personal Data and all copies of these Personal Data.

(3) Paragraph (1) and (2) shall be voided if the data management is required for any of the following purposes:

a) exercising the right to freedom of expression and information;
b) the fulfillment of an obligation under EU or Member State law for the processing of Personal Data by the Data Controller or for the execution of a task in the public interest or in the context of exercising a public authority;
c) in the public interest related to workplace or public health and safety;
d) archiving in the public interest, for scientific or historical research, or for statistical purposes, where the right referred to in paragraph (1) is likely to seriously compromise or make any such data management impossible; or
e) for presenting, enforcing or protecting legal claims.

2. Limitation

(1) The Data Subject is entitled to request that the Data Controller restricts the data management if either of the following conditions is met:

a) the Data Subject disputes the accuracy of the Personal Data; in this case, the limitation concerns the period of time during which the Data Controller is able to verify the accuracy of Personal Data;
b) the data management is illegal and the Data Subject opposes the deletion of data and asks for the limitation of their use instead;
c) the Data Controller no longer needs the Personal Data for data management purposes, but the Data Subject requires to use them for the submission, enforcement or protection of legal claims; or

d) the Data Subject objects to data management for reasons related to his/her own situation; in this case, the limitation applies to the period of determining whether the legitimate reasons of the Data Controller have priority over the legitimate reasons of the Data Subject.

(2) If data management is subject to limitation under paragraph (1), such Personal Data may only be used for purposes other than storage with the consent of the Data Subject or for the submission, enforcement or protection of legal claims or for the protection of the rights of other natural or legal persons or in the significant public interest of the EU or any Member State.

(3) The Data Controller shall give prior notice to the Data Subject on whose request the data management was limited under paragraph (1) about the discontinuation of such limitation.

3. **Objection**

The Data Subject is entitled to object to the handling of his/her Personal Data for reasons related to his/her own situation in case of tasks performed in the context of the exercise of a public authority vested in the Data Controller or data management in the legitimate interests of the Data Controller or a third party, including profiling based on any such provisions. In this case, the Data Controller may not continue managing the Personal Data unless the Data Controller proves that the data management is justified by coercive legitimate reasons that prevail over the interests, rights and freedoms of the Data Subject or for the submission, enforcement or protection of legal claims.

If the Personal Data is managed for the direct acquisition of business, the Data Subject is entitled to object to the management of his/her Personal Data for that purpose at any time, including profiling, if related to the direct acquisition of business.

If the Data Subject objects to the management of Personal Data for the direct acquisition of business, the Personal Data may no longer be managed for that purpose.

XIV. Options for the enforcement of user rights

If the user's privacy rights are violated and in the cases specified in the Regulation, the user may request the assistance of the National Authority for Data Protection and Freedom of Information and shall have the right to sue before the court of his/her domicile or place of residence:

Name: National Authority for Data Protection and Freedom of Information
Mailing address: 1530 Budapest, PB: 5.
Address: 1125 Budapest, Szilágyi Erzsébet fasor 22/c.
Phone: +36 (1) 391-1400
Fax: +36 (1) 391-1410
Web: naih.hu
E-mail: ugyfelszolgalat@naih.hu

XV. Changes of the Policy

The Data Controller reserves the right to modify or update this Policy at any time, without prior notice, and to publish the updated version on its websites. Any modification applies only to Personal Data collected after the publication of the revised version. The current Policy is available at the following link: www.casatibudapesthotel.com

Please check our Policy regularly to monitor the eventual changes and know how these changes might affect you.

Last update: 25.05.2018.