DATA MANAGEMENT POLICY

Date of entry into force: 25 May 2018

Review date: 1 August 2024

We place great emphasis on the protection of personal data. Of course, this applies even if you use our services. In this Data Management Policy, we would like to introduce you to the data management processes that we use during providing our services and our newsletter. Adhere we are informing you about the measures we have implemented in order to protect your data and about the types and purposes of the data we collect.

1. PREAMBLE:

Hotel Garden Kft. (**LOTUS THERME Hotel & SPA)** (registered office: 8380 Hévíz, Lótuszvirág u. 1., company registration number: 20-09-074756; tax number: 10804623-2-20) (hereinafter referred to as "**Data Controller"**) agrees to be bound by the contents of this Data Management Policy as Data Controller during providing its services.

The Data Controller shall manage the personal data of the guest, contract partner or personal contributor using the services of the Data Controller, as well as applicants and employees (hereinafter referred to as "**Affected Party**"). The Data Controller undertakes to ensure that the data management of its services complies with applicable law and the requirements of this Data Management Policy.

The Data Controller reserves the right to unilaterally amend this Data Management policy. It is recommended to visit https://lotustherme.net regularly to monitor changes. The effective content of the Data Management Policy is constantly available to access and download. We are happy send notification of the changes via email upon request.

Upon the request of the Affected party, we are happy to send a copy of the Data Management Policy currently in effect.

By providing such personal information, the Affected Party hereby declares that he/she has become aware of and expressly acknowledges this version of this Data Management Policy in effect at the time of the disclosure.

The requirements set out in this Data Management Policy are in accordance with applicable data protection legislation:

- Fundamental Law of Hungary (Freedom and responsibility, Article VI);
- Regulation of the European Parliament and of the Council (EU) 2016/679 (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, and repealing Directive 95/46/EC (General Data Protection Regulation, GDPR);
- Law CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information;

- Law V of 2013 on the Civil Code;
- Law CLV of 1997 on Consumer Protection.

1.1. Particulars of the Data Controller:

HOTEL GARDEN Kft. (LOTUS THERME Hotel & SPA)

Registered office: 8380 Hévíz, Lótuszvirág u. 1.

Contact details of the Data Controller through which the Affected party may exercise the rights contained in this data management policy:

Email: info@lotustherme.net

Mailing address: 8380 Hévíz, Lótuszvirág u. 1.

Telephone: +36 83 500 500

Web page: https://lotustherme.net

2. PRINCIPLES OF DATA PROTECTION:

2.1. Personal data:

Any data that can be associated with any specific (identified or identifiable) natural person is a deduction from the data of the Affected Party. Personal data will retain this quality during data management if the relationship with the Affected Party can be restored. A person shall be deemed to be identifiable if, directly or indirectly, if he is identifiable by name, identification mark or one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;

2.2. Consent:

Expressing, voluntarily and explicitly, the wishes of the Affected Party, based on appropriate information and giving unambiguous consent to the processing of personal data concerning him or her, whether full or specific;

2.3. Objection:

Statement of the Affected party in which he/she is expressing his/her objection against the management of his/her personal data and requesting the termination of the data management or the deletion of the data processed;

2.4. Data Controller:

Any natural or legal personality, or any entity without legal personality, which determines the purpose of the personal data management, makes and implements decisions on data management (including the device used), or has it executed by an authorized data processor;

2.5. Data management:

Any operation or combination of operations on personal data, such as collection, recording, filing, storing, altering, using, transmitting, disclosing, coordinating or linking, blocking, deleting and destruction of data, to prevent its further use, regardless of the procedure applied. Data management includes taking photos, sound or images, and capturing physical features (such as fingerprints, palm prints, DNA samples, iris images) that can be used to identify a person;

2.6. Data transmission:

If the data is made available to a specific third party;

2.7. Data disclosure:

If the data is made available to anyone;

2.8. Data deletion:

If the data made unrecognizable in such way that it is no longer possible to recover it;

2.9. Data blockage:

Disabling the transmission, access, disclosure, transformation, alteration, destruction, deletion, linking or reconciliation and use of data for a definitive or definite period of time;

2.10. Destruction of data:

The complete physical destruction of the data or the data medium containing it;

2.11. Data process:

Performing technical tasks related to data processing operations, regardless of the method and means used to perform the operations and the location of application;

2.12. Data processor:

Any natural or legal personality, or any entity without legal personality, who processes personal data on behalf of the controller, including as required by law;

2.13. Third party:

Any natural or legal personality, or any entity without legal personality, who is neither the Affected Party, nor the Data Controller or the Data Processor;

2.14. EEA state:

Member State of the European Union and other States party to the Agreement on the European Economic Area, whose citizen - by virtue of an international agreement between the European Community and its Member States and a State not party to the European Economic Area - enjoys the same status as a citizen of a State that is a party to the Agreement on the European Economic Area;

2.15. Third country:

Any State that is not an EEA State.

3. PRINCIPLES OF DATA PROTECTION:

Personal data:

a) administration must be conducted in a lawful and fair manner and in a manner that is transparent to the Affected Party ('legality, due process and transparency');
b) collection should serve a specific, explicit and legitimate purpose and not managed in a way that is incompatible with those purposes; further processing of data for archiving in the public interest, for scientific and historical research or for statistical purposes ("purpose limitation") is not considered incompatible with the original purpose under Article 89 (1) of the GDPR;

c) should be relevant to the purposes of the data management and limited to what is necessary ("data saving");
d) must be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data which are inaccurate for the purposes of the processing are immediately deleted or rectified ("accuracy");
e) it must be kept in a form which permits identification of Affected Party for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for a longer period only if they are processed for archival purposes in the public interest, for scientific and historical research purposes or for statistical purposes in accordance with Article 89 (1) of the GDPR; and subject to the implementation of appropriate technical and organizational measures to protect its freedoms ("limited storage");
f) shall be handled in a manner that ensures appropriate security of personal data, including protection against unauthorized or unlawful processing, accidental loss, destruction or damage, through appropriate technical or organizational measures ("integrity and confidentiality").

The Data Controller is responsible for compliance with the above and must be able to justify such compliance (“accountability”). The Data Controller does not collect personal information concerning minors.

4. DETAILED RULES FOR DATA MANAGEMENT:

The circle of people with access to data:

- co-workers of the Data Controller;
- co-workers of the data processors defined below;
- certain authorities in relation to data requested by them in the course of official proceedings and legally required by the Data Controller;
- employees of a claim’s management company appointed by the Data Controller for the management of overdue debts;
- other persons based on the express consent of the Affected Party.

The Data Controller undertakes to maintain strict confidentiality about the personal data handled by him/her for an indefinite time and - contrary to the Affected Party's consent - may not disclose them to any third party.

The withdrawal of consent shall not affect the legality of the previous processing.

4.1 Data management related to the registration for room reservation and the further use of the data provided during the registration:

The Affected Party must fill in a registration form in order to use the services provided by the Data Controller. The data will be further used in the course of the utilization of certain services. In case of online booking, some of the data will be transferred to the Data Controller from certain tour operators and travel agencies.

4.1.1. <u>The circle of the data and the detailed purposes of the data management:</u>

- Surname: required for identification, communication, contract performance
    - Services where this data set will be further utilized: wellness, spa, greeting card, shuttle service, bike rental
- First name: required for identification, communication, contract performance
    - Services where this data set will be further utilized: wellness, spa, greeting card, shuttle service, bike rental

- Nationality: required for identification, contract performance
- Identification number: required for identification, contract performance
    - Services where this data set will be further utilized: Bicycle rental
- Email address: required for correspondence
- Phone number: required for correspondence
- Full address: required for contract performance
- Billing address: required for contract performance
    - Services where this data set may be reused: fulfilment of various orders upon the request of the Affected Party
- Method of payment: required for correspondence
- Special dietary preference: serves to satisfy the taste of the Affected Party and required for contract performance
- Vehicle license plate number: required for contract performance
- Purpose of the trip: required for contract performance
- For guests outside the European Union:
- Passport number: compliance with legal obligation
- Visa Number: compliance with legal obligation
- Date and place of entry: compliance with legal obligation

4.1.2. Legal ground of the data management:
The legal ground for data management is the fulfilment of a contract (Article 6 (1) (b) of the GDPR), and to comply with legal obligation set out on Article 6(1) (f) of GDPR, where the law requires the handling and transfer of data (to the municipality, the police).

4.1.3. Duration of data management:

Data will be deleted 5 years after the termination of the business relationship with the Affected Party, pursuant to Article 6(22) of the Civil Code. Data will be kept for longer period if required by law, for instance, pursuant to Law C of 2000 on Accounting data will be deleted 8 years after the termination of the business relationship with the Affected Party. In practice, this is the case if the data is part of the financial records, such as the contract documents (in some cases the contract itself) or the invoice issued, or 6 years in the case of a police report.

4.2. Data management related to bank card details:

In the case of bank card payment, the Affected Party must provide this information in order to secure the booking and the financial performance of the service.

In case of online booking, some of the data will be transferred to the Data Controller from certain tour operators and travel agencies.

4.2.1. The circle of the data and the detailed purposes of the data management:
- Name on the bank card
- Number of the bank card
- Expiry of the bank card

4.2.2. Legal ground of the data management:
The legal ground of the data management is the performance of the contract (Article 6 (1)(b) of the GDPR.

4.2.3. Duration of the data management:

The Data Controller shall process the personal data for 8 calendar days after the departure of the Affected Party.

4.3. Data management of quotations and orders related to events:

The Affected Party (a personal contributor of a legal personality) may request a quotation from the Data Controller on organizing an event and may place an order on the accommodation.

4.3.1. The circle of the data and the detailed purposes of the data management:

- Surname: required for identification, communication, contract performance
- First name: required for identification, communication, contract performance
- Company name: required for identification, communication, contract performance
- Name of the personal contributor: required for identification, communication, contract performance
- Phone number: required for identification, communication, contract performance
- Email address: required for identification, communication, contract performance
- Program: required for contract performance
- Number of rooms required: required for contract performance
- Meal plan: required for contract performance
- Conference room requirement: required for contract performance
- Date of the event: required for contract performance
- Notes: required for contract performance
- Number of people: required for contract performance
- Contract value: required for contract performance
- Other performance criteria: required for contract performance

4.3.2. Legal ground of the data management:

The legal ground of data management is the performance of the contract (Article 6 (1) (b) of the GDPR), the fulfilment of the legal obligation for billing (Article 6 (1) (c) of the GDPR) and the legitimate interest of the Data Controller Article 6 (1) (f) of the GDPR).

4.3.3. Identification of a legitimate interest

In case of correspondence, the appropriate information is provided to the client via the point of contact. The fulfilment of the call for proposal is mutual business interest of the Hotel and the Affected Party. The Affected Party should be duly informed about the data processing at the first response of the correspondence.

Enforcement of claims during the limitation period.

4.3.4. Duration of the data management:

Should the Affected Party accept the proposal, his/her data will be deleted 5 years after the termination of the business relationship with the Affected Party, pursuant to Article 6(22) of the Civil Code. If the data is required to be retained under Section 169 of Accounting Act 2000 ("Accounting Act"), the data will be deleted 8 years after the termination of the business relationship with the

Affected Party. In practice, this is the case if the data is part of the financial records, such as the contract documents (in some cases the contract itself) or the invoice issued. Shall the offer not be accepted by the Affected Party, the Data Controller archives the data for 3 years in its legitimate interest - storing previous offers of the Partners is its direct business interest.

4.4. Data management in relation to contracting with partners:

The Data Controller contracts various partners to provide its services.

4.4.1. The circle of the data and the detailed purposes of the data management:

- Surname of the personal contributor: required for identification, communication, contract performance
- First name of the personal contributor: required for identification, communication, contract performance
- Photo: required for contract performance (specifically in case of contracts on photographic services
- Email address: required for identification, communication
- Phone number: required for identification, communication
- Details of legal personality (name, registered office, company registration number, tax number): required for contract performance

4.4.2. Legal ground of the data management:
Performance of the contract is the legal ground of the data management (Article 6 (1)(f) of the GDPR).

4.4.3. Duration of the data management:

Data will be deleted 5 years after the termination of the business relationship with the Affected Party, pursuant to Article 6(22) of the Civil Code. If the data is required to be retained under Section 169 of Accounting Act 2000 ("Accounting Act"), the data will be deleted 8 years after the termination of the business relationship with the Affected Party. In practice, this is the case if the data is part of the financial records, such as the contract documents (in some cases the contract itself) or the invoice issued.

4.5. Data management on complaint handling:

The Data Controller processes the personal data related to the complaint, the recorded minutes and the copy of the response letter for 5 years from the date of the complaint, in accordance with the Consumer Protection Act.

Our company's partner, CRERAG Kft., which is contracted to operate the internal abuse reporting system, guarantees the following:

Within the framework of the internal abuse reporting system,

(1)

a) the reporting party,

b) the person whose conduct or omission gave rise to the report,

and

c) the person who may have substantive information about the contents of the report, processes the personal data of the person who is indispensable for the investigation of the report solely for the purpose of investigating the report and remedying or terminating the conduct that is the subject of the report.

From the data processed within the framework of the internal abuse reporting system, it immediately deletes the personal data not falling within the scope of paragraph (1).

(2) The processing of personal data processed within the framework of the internal whistleblowing system shall be subject to Section 6(2) of Act XXV of 2023 and, with regard to data relating to the reporter, Section 6(4).

(3) If the report concerns a natural person, the person requesting the information shall not be made aware of the reporter's personal data in the exercise of the natural person's right to information and access under the provisions on the protection of personal data.

(4) The transfer of data processed within the framework of the internal whistleblowing system to a third country or an international organisation may only take place if the recipient of the transfer has made a legal commitment to comply with the rules on the report contained in this Act and in accordance with the provisions on the protection of personal data.

(5) In the internal whistleblowing system, the personal data of the whistleblower who reveals his or her identity and of the person concerned by the report shall not be disclosed to anyone other than those authorised to do so. Until the investigation is concluded or formal liability is initiated as a result of the investigation, the persons investigating the report shall share information on the content of the report and the person concerned by the report with other organisational units or employees of the employer to the extent strictly necessary for the conduct of the investigation, in addition to informing the person concerned by the report.

(6) At the start of the investigation, the person concerned by the report shall be informed in detail about the report, his or her rights regarding the protection of his or her personal data, and the rules governing the processing of his or her data. In accordance with the requirement of fair procedure, it shall be ensured that the person concerned by the report may also express his or her position on the report through his or her legal representative and support it with evidence. The person concerned by the report may exceptionally, in justified cases, be informed later if immediate information would frustrate the investigation of the report.

(7) Paragraphs (1) and (2) shall also apply to the person who may have substantive information about the contents of the report.

(8) In the case of an oral report, the reporter shall be informed of the consequences of a bad faith report, of the procedural rules governing the investigation of the report and of the fact that his identity – if he provides the data necessary for its establishment – will be treated confidentially at all stages of the investigation.

(9) The operator of the internal abuse reporting system shall send a confirmation of the submission of the report to the reporter within seven days of receiving a written report made in the internal abuse reporting system. The confirmation shall include general information on the procedural and data processing rules under this Act.

XXV of 2023 Both our company and CRERAG Kft. fully comply with and act in accordance with the data protection and data management regulations of the Act. We recognize the above regulations as binding on ourselves.

Service provider: CRERAG Limited Liability Company

Registered office, postal address: 5143 Jánoshida, Kossuth Krt. 12.

Email address: zsuzsanna@drcrespo.hu

Telephone number: +36-30-952-8838

Tax number: 32320163-2-16

Registration number: Cg. 16-09-021745

Registration authority: Szolnok Court of Appeals

4.6. Data management on evaluation:

The Affected Party may give an evaluation on the accommodation. The evaluation shall be filled in anonymously.

4.6.1. The circle of the data and the detailed purposes of the data management:

- Surname: required for identification and communication
- First name: required for identification and communication
- Email address: required for identification and communication
- Date of stay: measuring satisfaction, statistics
- Evaluation of the hotel: measuring satisfaction, statistics

4.6.2. Legal ground of the data management:
Legal ground of the data management is the consent of the Affected Party (Article 6(1) of the GDPR).

4.6.3. Duration of the data management:

The Data Controller shall process the personal data until the Affected Party's consent is withdrawn. Consent may be withdrawn at any time via email to info@lotustherme.net .

4.7. Carrier:

The Data Controller shall provide an opportunity for the Affected Party to apply for the position he or she has advertised. Application may be done via email. The Affected Party applying for the vacancy shall be informed about personal data management in a reply letter in each case.

4.7.1. The circle of the data and the detailed purposes of the data management:

- Surname: required for identification and correspondence
- First name: required for identification and correspondence
- Email address: required for identification and correspondence
- Voluntarily disclosed personal information: may be required to select the appropriate person for the position
- Any document attached to the CV is voluntarily disclosed personal information: may be required to select the appropriate person for the position

4.7.2. Legal ground of the data management:
Legal ground of the data management is the consent of the Affected Party (Article 6(1) of the GDPR), during the period of enforcement of claims, the legal ground is the legitimate interest of the Data Controller (Article 6(1) (e) of the GDPR).

4.7.3. Identification of a legitimate interest
Enforcement of the claims against the applicant or the Data Controller based on the Labour Law or equal treatment.

4.7.4. Duration of the data management:

After selecting the appropriate person for the position to be filled, the Data Controller shall inform the other applicants concerned that the employer has

not selected him / her for the position and shall also request his / her explicit and voluntary consent in writing for the retention of the CV and related documents. The purpose of data management is to enable the Affected Party to participate in subsequent tenders of the hotel in a simplified manner. The explicit consent of the Affected Party will allow the processing of his/her personal data for a period of 5 years, after which time the data will be deleted.

Shall the Affected Party does not consent to the retention of his / her application or personal data, the data will be deleted within 30 days and the CVs will be destroyed.

4.8. Newsletter:

The Affected Party may subscribe to receive newsletters sent by the Data Controller with marketing purposes. Accordingly, the Data Controller shall be entitled to send direct marketing newsletters to the Affected Party who have subscribed to their newsletter, to the email address provided - and, if applicable, modified – on a regular basis with certain content as specified by the Data Controller, about the Data Controller's promotions, activities, calls to action.

The Data Controller does not send unsolicited advertising messages and the Affected Party may, without limitation and without justification, unsubscribe from receiving offers. In this case, all personal information necessary for sending the newsletter will be deleted from our records and we will not contact the Affected Party with further promotional offers. You can unsubscribe from the newsletter at any time by clicking on the link in the message.

4.8.1. The circle of the data and the detailed purposes of the data management:

- Surname: required for identification and correspondence
- First name: required for identification and correspondence
- Email address: to forward news updates

4.8.2. Legal ground of the data management:

Legal ground of the data management is the consent of the Affected Party, furthermore, pursuant to Article 6 of Law XLVIII of 2008 on the General Terms and Conditions of Certain Economic Advertising Activities the Affected Party may in advance and expressly consent to receive advertising offers and other mail sent by the service provider to the specified contact email address.

4.8.3. Duration of the data management:

The Data Controller will retain personal data until the Affected Party's consent is revoked.

4.8.4. Data protection rights of the Affected Parties:

The Affected Party may unsubscribe from the newsletters at any time, free of charge.

4.9. Social media presence of the Data controller (Facebook, YouTube, Instagram, Google):

The Data Controller is available on Facebook, Instagram, YouTube and Google.

The operators of social networking sites are separate data controllers, independent of the Data Controller, so their activities are contained in the data management documents independent of the Data Controller.

4.10. Data management related to camera surveillance:

For personal and property protection purposes, the Data Controller shall carry out camera surveillance on the premises. The use of the surveillance camera system as data management was registered by the National Authority for Data Protection and Freedom of Information under NAIH-69604/2013.

4.10.1. The circle of the data and the detailed purposes of the data management:

- Photographs: personal and property protection

4.10.2. Location of the cameras:

The following cameras operate on the premises of the Data Controller:

26 outdoor cameras covering the whole area of the guest car park.

1. Location of the CCTV cameras monitoring the guest car park:

long car park 01 - car park

long car park 02 - car park

long car park 03 – car park

long car park 04 - car park

long car park 05 - car park

long car park 06 - car park

long car park 07 - car park

long car park 08 – car park

long car park 09 - car park

long car park 10 - parking

dispatcher 11 - car park

dispatcher 12 - car park

dispatcher 13 - car park

dispatcher 14 - car park

dispatcher 15 - car park

dispatcher 16 - car park

dispatcher 17 - car park

dispatcher 18 - car park

dispatcher 19 - car park

dispatcher 20 - car park

dispatcher 21 - car park

dispatcher 22 – car park

on the outside wall, in the direction of the pedestrian path, top right 23 - car park, pedestrian path

next to the canal 24 - parking, pedestrian path

next to the restaurant, on the top of the electrical pole 25 - parking, on the road to the stables

outside parking lot, top right 26 - gate, barrier

2. The front door of the hotel's wellness centre is monitored by 10 cameras.

The location of the cameras:

next to the elevator, top 01 - therapy corridor

in front of the door, top 02 - Jacuzzi

on the wall to the left, top 03 - relax pool

on the wall to the right, top 04 - large seating pool

on the wall to the right, top 05 - small seating pool

outside chemical storage, on the top of the wall 06 - therapy back service entrance

in front of beauty, top 07 - beauty corridor

top the beauty centre 08 - beauty reception

top the beauty centre 09 - beauty reception

fitness room top right corner 10 - fitness room

3. The outside and inside entrances and various parts of the hotel are monitored by 46 cameras.

The location of the cameras:

Ground floor, outside:

ground floor ramp, top left 01 - service entrance

ground floor gardener's garage left top 02 -service entrance

ground floor exterior wall top 03 - emergency exit

ground floor sport office, exterior wall, top right 04 – musicians' entrance

ground floor exterior wall 05 - outdoor pool

Ground floor, inside:

ground floor opposite to the main entrance, top 06 - guest area

ground floor reception left corner 07 - reception

ground floor reception right corner 08 - reception

ground floor in front of reception, top 09 - reception

ground floor front of reception, top 10 - reception

ground floor front of reception, top 11 - reception

ground floor above Guest Relation 12 – guest area

ground floor bar over cash register 13 - bar

ground floor in front of the bar, top 14 - bar

ground floor in front of the door, top 15 - bar

ground floor Agra top 16 - bar

ground floor above counter 17 - staff canteen

ground floor on the left in front of the door, top 18 - staff entrance

ground floor opposite the door, top 19 - luggage inspection

ground floor hallway to the left, top 20 – changing rooms hallway

ground floor in front of the general storage room, top 21 - storage room corridor

ground floor in front of the general storage room, top 22 – cold storage corridor

ground floor in front of a beer storage room, top 23 - storage room corridor

ground floor in front of the scale, top 24 - scale

ground floor staff corridor, top 25 – goods entrance

ground floor in front of salt cave, top 26 - staff lift, secretarial bureau

I. floor:

1st floor blue corridor, top right (circular corridor) 27 - corridor leading to hotel rooms

1st floor corridor, top left (staircase) 28 - corridor leading to hotel rooms

II. floor:

2nd floor blue corridor, top right (circular corridor) 29 - corridor leading to hotel rooms

2nd floor blue corridor, top left (staircase) 30 – corridor leading to hotel rooms

2nd floor yellow corridor, top right (circular corridor) 31 - corridor leading to hotel rooms

2nd floor yellow corridor, top left (staircase) 32 - corridor leading to hotel rooms

2nd floor burgundy corridor, upper right (circular corridor) 33 – corridor leading to hotel rooms

2nd floor burgundy corridor, top left (staircase) 34 - corridor leading to hotel rooms

III. floor:

3rd floor blue corridor, top right (circular corridor) 35 - corridor leading to hotel rooms

3rd floor blue corridor, top left (staircase) 36 - corridor leading to hotel rooms

3rd floor yellow corridor, top right (circular corridor) 37 - corridor leading to hotel rooms

3rd floor yellow corridor, top left (staircase) 38 - corridor leading to hotel rooms

3rd floor burgundy corridor, top right (circular corridor) 39 - corridor leading to hotel rooms

3rd floor burgundy corridor, top left (staircase) 40 - corridor leading to hotel rooms

IV. floor:

4th floor blue corridor, top right (circular corridor) 41 - corridor leading to hotel rooms

4th floor blue corridor, top left (staircase) 42 - corridor leading to hotel rooms

4th floor yellow corridor, top right (circular corridor) 43 - corridor leading to hotel rooms

4th floor yellow corridor, top left (staircase) 44 - corridor leading to hotel rooms

4th floor burgundy corridor, upper right (circular corridor) 45 - corridor leading to hotel rooms

4th floor burgundy corridor, top left (staircase) 46 - corridor leading to hotel rooms

4.10.3. Legal ground of the data management:

Legal ground of the data management is the legitimate interest of the Data Controller (Article 1 (f) of the GDPR).

4.10.4. Identification of a legitimate interest

With regards to the number of employees, hotel guests and other persons in motion and the considerable value of the assets to be protected at the headquarters and branches of the employer and in order to guarantee uninterrupted and secure work and service, areas that can't be kept under 24-hour surveillance in other way, e.g. involving manpower, are to be monitored by security cameras. The recordings may serve as conclusive evidence of possible legal processes. Employees are not under video surveillance by the employer.

4.10.5. Duration of the data management:

Records will be kept by the Data Controller for 3 days. In the event of a personal and security incident, the Data Controller shall be entitled to manage the recordings for more than 3 days.

4.11 Data management of object found:

4.11.1. Purpose of data management:

Administration of objects found in the territory of the Hotel operated by the Data Controller, notification of the alleged owner or finder.

4.11.2. Legal grounds of the data management:

Pursuant to Section 5(54), 5(55), 5(59) and 5(61) of Law V. of 2013 of the Civil Code.

4.11.3. Circle of the data handled:

Date and place of finding, name and contact details of the finder, details of the found object.

4.11.4. Duration of the data management:

One year from the date of return to the rightful owner.

4.12 Recording Data in the Guest Information Closed Database

4.12.1. The purpose of data management: From 1 September 2021, the data on the photo ID card will be recorded on arrival using a document reader. A 414/2015. (XII. 23.) of the Government, the obligation of the recipients of the accommodation service to present their personally identifiable document to the accommodation provider on the spot.

4.12.2 Legal basis for data management: 2016 CLVI. Based on the amendment of the Act, the accommodation service providers are obliged to record the data of the guests specified in the Act in the storage provided by the hosting provider designated by the Government (Hungarian Tourism Agency) (Guest Information Closed Database).

4.12.3. Scope of data managed:

- surname and first name
- Birth surname and first name
- place of birth
- date of birth he is not
- citizenship
- Mother's birth surname and first name
- personal identification or travel document identification data
- in the case of a third-country national *, the number of the visa or residence permit, the date and place of entry.

* third-country national: Annex II to the 2007 Act on the entry and residence of third-country nationals persons under the law.

The necessary condition for using the accommodation service is the presentation of an identity document, regardless of the age of the guests.

5. PEOPLE AUTHORISED TO PROCESS DATA:

For execution of technical tasks related to data management operations the Data Controller employs data processors listed in the table below. The data processor's rights and duties relating to processing personal data are specified by the Data Controller, according to the GDPR and special laws regarding data management. The Data Controller is responsible for the lawfulness of the directions/commands made. The data processor cannot make a substantial decision regarding data management, the personal data come to their notice must be processed exclusively according to the directions of the Data Controller, they cannot do data processing for own purposes, they must store and keep the personal data according to the directions of the Data Controller, respectively.

Names and contacts of data processors	**Activity in the course of data processing**
Szabó Zoltán Endre E.V. Contact: 8315 Gyenesdiás, Harmat u. 9/12	Sending newsletters for the Affected Parties
Morgens Design Kft. 8800 Nagykanizsa, Csányi László utca 2.	Technical background of online services: booking engine, voucher service, webshop.
CARDNET Kártyarendszerek és Szolgáltatások Korlátolt Felelősségű Társaság (Ltd.) http://www.cardnet.hu/kapcsolat/	Establishment and management of „Lotus Privilege Card" loyalty program and card system
Hostware Kft. Registered office: 1149 Budapest, Róna u. 120.	Has access to all the personal data managed by the Data Controller based on the present data management policy. Its task is to store personal data managed by the Data Controller, through operating its IT management system.
4 Clean Kft. Registered office: 1155 Budapest, Tóth István u. 108.	Property protection, security, event security and reception service.
dr. Pallag Péter Registered office: 1016 Budapest, Számadó u. 15.	Claims management, legal administration
Siam Center Lotus Kft. Registered office: 8360 Keszthely, Lovassy u. 8.	Thai massage service.

Szakonyi László Egyéni Vállalkozó Registered office: 8353 Zalaszántó, Zsidi út 3.	Yumeiho massage, massage therapy and reflex zone therapy service.
KAMLESH Kereskedelmi Kft. Registered office: 1125 Budapest, Gyöngyvirág út 3/A.	Indian massage service.
Medical services, doctors	Healthcare and specialized medical services
Fly Car Group Kft. Registered office: 8360 Keszthely, Epreskert u.6.	Car services
Eni Travel Agency Kft. Registered office: 8380 Hévíz, Vörösmarty u. 91.	Reservation and arrangement of accommodation
Travel agencies	Reservation and arrangement of accommodation
Accomodation platforms	Reservation and arrangement of accommodation
Magyar Turisztiaki Ügynökség 1027 Budapest, Kacsa utca 15-23	Has access to all the personal data managed by the Data Controller based on the present data management policy. Its task is to store personal data managed by the Data Controller, through operating its IT management system named "VIZA".
The Data Controller reminds the Affected Party that they will receive distinct information about the data processors employed for each services.	

6. DATA SECURITY MEASURES:

The Data Controller deals with the personal data provided by the Affected party keeping the guidelines of the "Regulation of the European Parliament and of the Council (EU) 2016/679" and the "Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information" in mind.

The Data Controller makes every necessary arrangement required of him/her to secure data, takes care of their appropriate protection especially against unauthorised access, modification, forwarding, publication, deletion or destruction, as well as accidental eradication and damage. The Data Controller ensures the security of data by appropriate technical (e.g. logical protection, especially encryption of passwords and communication channels) and organizational measures (physical protection, especially data security training of the Data Controller's employees, limitation of access to information).

Please help us keeping information safe by not using obvious login name and password, as well as by changing your password regularly, in addition, we ask you not to make your password accessible for another person.

7. INFORMATION REGARDING CHILDREN:

By providing the information, you represent and warrant that you are acting in accordance with the foregoing, and your ability to act in relation to the provision of the

information is not limited. If you are not legally entitled to make this information available, you must obtain the consent of the Affected Third Party (e.g. legal representative, guardian). In this context, you are required to consider whether third party consent is required in connection with the provision of that information. The Data Controller may not make any personal contact with you, and you are responsible for ensuring compliance with this clause and the Data Controller is not responsible for it.

We make every reasonable effort to delete any information that has been made available to us unauthorizedly and to ensure that such information is not transmitted to or used by anyone else (for advertising or other purposes). Please let us know immediately if you find that a child has unauthorized access to information about themselves. You can contact us through the contact information highlighted at the beginning of this data management policy.

8. RIGHTS RELATED TO DATA PROCESSING:

The data protection rights and remedies of the Affected Party, as well as the relevant GDPR provisions and restrictions, are set forth in detail in the GDPR (including, in particular, Article 15, 16, 17, 18, 19, 20, 21, 22, 77, 78, 79 and 82 of the GDPR). The most important provisions are summarized below.

8.1. The right of access of the Affected Party:

The Affected Party is entitled to receive feedback from us as to whether the processing of your personal data is ongoing. If such data processing is in progress, the Affected Party shall have the right to access personal data and the following information:

a) the purposes of the processing;

b) the categories of personal data of the Affected Party;

c) the recipients or categories of recipients to whom the personal data have been or will be communicated, including in particular third-country recipients or international organizations;

d) where applicable, the intended period for which the personal data will be stored or, if this is not possible, the criteria for determining this period;

e) the Affected Party's right to request the rectification, deletion or restriction of processing of personal data concerning the Affected Party and to object to the processing of such personal data from us;

f) the right to lodge a complaint to a supervisory authority; and

g) if the data were not collected from the Affected Party, all available information on their source;

h) the existence of automated decision-making, including profiling, and, at least in these cases, clear information on the logic used and the significance and likely consequences for the Affected Party of such processing.

If personal data are transferred to a third country, the Affected Party is entitled to be informed of the appropriate guarantees regarding the transfer.

Copies of the personal data subject to the data processing will be provided to the Affected Party. If the Affected Party has submitted the request electronically, the

information shall be provided in a widely used electronic format, unless otherwise requested by the data subject.

8.2. Right to rectification:

Affected Party has the right to correct inaccurate personal information about Affected Party without undue delay upon his/her request. The Affected Party has the right to request the completion of incomplete personal information, including through a supplementary statement.

8.3. The right to erasure ("the right to forget"):

8.3.1. The Affected Party shall have the right to delete upon his/her request without undue delay, personal data relating to the Affected Party if any of the following applies:

a) personal data are no longer required for the purpose for which they were collected or otherwise processed;

b) the Affected Party withdraws its consent to the data processing and there is no other legal basis for the data processing;

c) the Affected Party objects to the processing of the data and, there is no overriding legitimate reason for the processing;

d) unlawful processing of personal data;

e) personal data must be deleted in order to fulfil a legal obligation under the laws of the European Union or Member State which applies to us; or

f) personal data have been collected in connection with the provision of information society services.

8.3.2. If the Data Controller has disclosed the Personal Data and shall delete them pursuant to Section 8.3.1., the Data Controller shall take reasonable steps - including technical measures – taking into consideration the available technology and implementation costs, in order to inform the data controllers that the Affected Party has requested the deletion of the links to access the personal data in question or their copies or duplicates.

8.3.3. Section 8.3.1. and 8.3.2. shall not be applied where data processing is necessary, including:

a) to exercise the right to freedom of expression and information;

b) in order to comply with an obligation under the laws of the European Union or Member State which applies to us with regards to the processing of personal data;

c) for archiving in the public interest, for scientific and historical research or for statistical purposes, provided that the right referred to in Section 8.3.1. is likely to render impossible or seriously undermine such processing; or

d) for filing, enforcement or defence of legal claims.

8.4. Right to restrict data management:

8.4.1. The Affected Party shall have the right to restrict the data processing request if any of the following is true:

a) the Affected Party disputes the accuracy of the personal data, in which case the limitation applies to the period of time allowing us to verify the accuracy of the personal data;

b) the data processing is unlawful, and the Affected Party opposes the deletion of the data and instead requests a restriction on their use;

c) we no longer need personal data for the purpose of data management but are required by the Affected Party to make, assert or defend legal claims; or

d) the Affected Party protested against the data processing; in this case, the restriction shall apply for a period until it is ascertained whether the legitimate reasons of the Data Controller take precedence over the legitimate reasons of the Affected Party.

If the data management is restricted in accordance with Section 8.4.1., except of the storage of such personal data may only be processed with the consent of the Affected Party, or for the purpose of submitting, enforcing or defending legal claims, or protecting the rights of any other natural or legal personality, or for important public or by the interest of the European Union or any Member State.

The Affected Party will be informed in advance of the lifting of the privacy restriction.

8.5. Notification obligation to correct or delete personal data or to restrict data management:

Unless it proves impossible or requires a disproportionate effort, the Data Controller shall inform all recipients of any rectification, erasure or restriction of data management with whom or to whom the personal data have been communicated. Upon request, the Affected Party will be informed of these recipients.

8.6. The right to data portability:

8.6.1. The Affected Party has the right to receive the Affected Party's personal information made available to us in a structured, widely used, machine-readable format and to transmit such data to another data controller without being hindered by the Data Controller if:

a) the processing is based on consent or a contract; and

b) the data are processed in an automated way.

Pursuant to Section 8.6.1. on the right to data portability, the Affected Party shall have the right to request, where technically feasible, the direct transfer of personal data between data controllers.

8.7. Right to object:

The Affected Party has the right to object at any time to any legitimate interest in the processing of your personal information, including profiling, for reasons related to his/her own situation. In this case, we will not process the Affected Party's personal data unless we demonstrate that the processing is justified by compelling legitimate reasons that override the interests, rights and freedoms of the Affected Party, or that are related to the filing, enforcement or defence of legal claims.

If personal data is processed for the purpose of direct business acquisition, the Affected Party shall have the right at any time to object to the processing of personal data relating to the Affected Party for this purpose, including profiling, if it is related to direct business acquisition.

If the Affected Party objects to the processing of personal data for the purpose of direct business acquisition, personal data may no longer be processed for this purpose.

In connection with the use of information society services and, by derogation from Directive 2002/58 / EC, the Affected Party may exercise the right to protest based on technical specifications of automated tools.

If personal data are processed for scientific and historical research or statistical purposes, the Affected Party shall have the right to object to the data processing for reasons related to his/her own situation, unless necessary for the performance of a task in the public interest.

8.8. Right to file a complaint to the supervisory authority:

The Affected Party may enforce his or her rights before the courts pursuant the GDPR and the Civil Code, as well as the National Data Protection and Freedom of Information Authority (NAIH) (1125 Budapest, Erzsébet fasor 22 / C, mailing address: 1530 Budapest, Post Box 5; telephone: +36 1 391 1400; email: ugyfelszolgalat@naih.hu). The detailed rights and remedies on data management are detailed in Article 77, 79. and 82 of GDPR.

8.9. Right to effective legal remedy against the supervisory authority:

The Affected Party shall have the right to an effective legal remedy against a legally binding decision of the supervisory authority concerning the Affected Party.

The Affected Party shall have the right to an effective legal remedy if the competent supervisory authority does not deal with the complaint or fails to inform the Affected Party within three months of the procedural developments or the outcome of the complaint.

Proceedings against the supervisory authority shall be brought before the courts of the member state where the supervisory authority is registered.

8.10. Right to an effective judicial remedy against the controller or the processor:

The Affected Party is entitled to effective legal remedy if he or she considers that his or her personal data have been violated under the GDPR as a result of improper GDPR treatment.

Proceedings against the Data Controller or the processor shall be brought before the courts of the member state where the Data Controller or processor is registered. Such proceedings may also be brought before the courts of the member state in which the Affected Party is resident.

It is advisable to send the complaint to the Data Controller before initiating any procedure.