



Data Management Policy

Last Updated on May 25, 2018

We consider the protection of personal data a top priority. This, of course, also applies for the case when you use our online booking system or subscribe to our newsletter. That is why we would like to inform you on the data management and data processing processes we use while providing our services in our online booking system or in our newsletter. We are informing you below about what we do to protect your data and what data we record for what purpose.

Hotel Lotus Therme Hotel & Spa Hévíz and its website, www.lotustherme.net is operated by Hotel Garden Kft.

Headquarters: 1 Lótuszvirág u. Hévíz, Hungary 8380.

Company Registry number: 20-09-074756

Postal address: 1 Lótuszvirág u. Hévíz, Hungary 8380

Phone: +36 83 500 500

Email: info@lotustherme.net

This Data Management Policy describes how **Hotel Garden Kft.** / Hereinafter is referred to as **Data Controller** / uses and protects your personal data. Data Controller is the manager of personal data that our guests or prospective guests provide when using the website, enter the hotel, and other groups of people who are identified as guests by this policy and who contact us through different channels, business contacts, and our colleagues. Data management was registered in the Data Protection Register kept by the National Authority for Data Protection and Freedom of Information under number NAIH-58840/2012.

This Data Management Policy explains how we provide the protection of your personal information. Many of the principles we follow derive from the EU's General Data Protection Regulation (GDPR). However, we comply with all applicable legal requirements regarding the protection of personal data and data protection. Data Controller declares that

1. it acts in accordance with the provisions of Act CXII of 2011 on the right to information self-determination and freedom of information during data management;
2. Personal data the Data Controller becomes aware of in the course of data management shall be disclosed only to those persons employed by the Data Controller who are appointed to carry out data management tasks.

3. The data controller organizes training for the data controllers in its application, and sets out the protocols for compliance with data protection regulations and legislation in a policy.
4. Ensures that the policy in force are accessible to those concerned at all times, thereby enforcing the principle of transparency.
5. The personal data of guests staying in the hotel operated by Data controller shall be handled confidentially, in accordance with the applicable legal regulations, and shall ensure their safety, and shall take technical and organizational measures and establish procedural rules in order to fully comply with the principles of data protection.
6. Data controller shall take all appropriate measures to facilitate all IT and other measures supporting secure data management in order to retain, store, process and transfer the data managed by him or her.
7. He or she makes every effort as expected to ensure that the personal data he or she manages are protected against unauthorized access, alteration, disclosure, deletion, damage or destruction, and to guarantee the necessary technical conditions.
8. Data controller does not check the personal provided given to him or her, and does not assume responsibility for their validity.
9. He or she communicates personal data to a third party, and links the database managed by him to another data controller only in exceptional cases and in the event that the data owners concerned grant their consents to it or it is permitted or required by law, and if the terms of data management are met for every single piece of personal data concerned.
10. Data controller carries out activities only in Hungary, does not transmit the data it manages to other countries.
11. He or she assumes no responsibility for the lawfulness of the data management of contractual partners of the Data Controller.
12. Data controller keeps records for the purposes of monitoring data-protection incidents and informing the data owners concerned, including the personal data concerned, the range and number of data owners affected by the data-protection incident, the date and time, circumstances, effects and actions taken to prevent the data protection incident, as well as other data specified by the relevant law on data management.
13. By using appropriate security measures to protect the personal data stored in automated data files, Data Controller shall ensure that accidental or unlawful destruction or accidental loss as well as unauthorized access, alteration or distribution of data are prevented.

Data Managed by Data Controller:

Requests for offers/Bookings

1. In the case of requesting and offer / booking through <https://www.lotustherme.net> website, the Controller requests / may request the following information from the guests:

- Last Name *
- First Name *
- Email *
- Email again *
- Phone number *
- Arrival Date *
- Check Out *
- Number of nights*
- Number of adults*
- Number of children
- Age of children
- Contents of the request for offer
- Subscribe to a newsletter

- Where did you find us?
 - Other comment
 - Data marked with * are mandatory.
2. The process is voluntary.
 3. The activity and process involved in data management is as follows:
 4. The offers or forms found on the Website concerned (Form for requesting an offer, Contact Form), or through the Roomz booking engine on the Website where you have the option to provide the information specified in this Clause, as well as the booking and cancellation conditions and this Data Management Policy. After entering the data, accepting the terms and conditions, and pressing the "Next" button, you can send the data specified above to the Data Controller.
 5. Data sent to the Data Controller are handled by the employees of the Data Controller authorized for the purpose of this job, recording the data received with the help of the Micros FIDELIO Front-Office program and develop an offer for the person concerned and send it by e-mail
- Last Name *
 - First Name *
 - Email address*
 - Email again *
 - Phone number *
 - Other
 - Where did you find us?

1. In case of a reservation, additional billing-address information:

- Country *
 - City *
 - Street, no.*
 - Data marked with * are mandatory
2. The activity and process involved in data management are as follows:
 3. If the client concerned accepts the offer and informs the Data Controller about it orally or in writing, the Data Controller will take the steps related to the reservation.
 4. The booking agents employed by the Data Collector enter the data provided by the client concerned in the booking program and use this software to link them to the specific room of the hotel to create the reservation.
 5. The client concerned shall be notified of the occupation of the room in writing / by e-mail by the employee specified above.
 6. The Roomz booking engine is operated by Confhotel Development Kft., the data controller of the Data Controller; for additional data protection information on the operation of the Roomz booking engine, see: <https://roomz.hu/gdpr>

Checking in and check-in registration form

1. Upon arrival at the hotel, the guest concerned fills in a hotel check-in registration form, a "Registration Card", whereby he or she agrees that the Data Controller will handle the data provided as specified below for performing its obligations in accordance with the relevant legislation (in particular legislation on aliens, and tourism tax) for proof of fulfilment and identification of the Guest as long as the competent authority can verify the fulfilment of the obligations specified in the relevant legislation:
- Last Name *
 - First Name *
 - Citizenship *

- Date of birth*
 - ID card Number *
 - Home address*
 - E-mail address
 - Arrival Date *
 - Date of departure *
 - License plate number*
 - Name and date of birth of children *
 - Signature*
 - I would like to receive newsletters (checkbox)
 - Data marked with * are mandatory
2. The provision of mandatory information by the Guest is a precondition for using the services of the hotel.
 3. By signing the checking-in registration form, the guest agrees that the Data Controller will manage and archive the data submitted by completing the registration form for the purpose of proving the conclusion or fulfilment of the contract, as well as for the possible claim enforcement within the time period specified above.
 4. By entering the email address in the registration form, guests have the opportunity to subscribe to the Data Controller's newsletter. Otherwise, regarding the newsletter, section VI.5. shall apply.
 5. The information provided in the Guest Registration form applies to all hotel services and rentals (bicycle rental, tennis court rental, etc.) used by the guest.

Newsletter

1. Guests concerned can sign up for the newsletter through the website, via the Roomz booking engine, by e-mail or at the Hotel upon check-in on the "Registration Card", as well as on paper when using the certain services by providing the information specified below.
2. Scope of data managed:
 - name*
 - Email address*
 - Data marked with * are mandatory.
3. Subscription to the newsletter is voluntary.
4. The purpose of data management related to sending newsletters sending is to provide the recipient with full or customized information about the latest promotions of the Data Controller.
5. Data Controller sends newsletters only with the consent of the addressee concerned.
6. The Personal details provided shall be stored in a separate list by the Data Controller separately from the data provided to the Data Controller for other purposes, and this list will be available only for the specifically authorised colleagues and data processors of the Data Controller. Data Controller's Data Processor for sending newsletters:

Zoltán Endre Szabó, Sole proprietor; 9/12 Harmat u. Gyenesdiás, Hungary 8315

Tax ID.: 65646531-3-40

7. Data controller shall not disclose the list or the data to a third party or to any unauthorized person, and shall take all security measures to prevent them from being disclosed to unauthorized persons.
8. Data Controller will only handle the personal data recorded for the purpose it was requested until the person concerned has unsubscribed from the newsletter.

9. One may unsubscribe from the newsletter at any time by clicking on the Unsubscribe button at the bottom of the emails or by sending a cancellation request to info@lotustherme.net.
10. Data Controller keeps statistics about the readings of newsletters sent through the clicks on the links included in newsletters. The statistics are anonymous and do not store personal data.
11. You can subscribe to the news feed posted on the Facebook page by clicking on the "like" link on the page, and can unsubscribe by clicking on the "dislike" link on the page or by using the settings on the message wall you can delete unwanted feeds on the message wall. The icon of Facebook social media can also be found on the Data Controller's website, and you can find more out about giving consent in section VI/12 of the Data Management Policy.

Healthcare-Wellness-Beautician services

1. Purpose of data management:
To Promote the care, improvement, and maintenance of your health.

Legal background for data management:

As you have contacted us for medical treatment, your consent to the management of your healthcare and personal identification data related to your treatment, unless otherwise stated, shall be deemed to have been given. You may revoke your consent at any time, however, the revocation does not affect the prior lawful management of the data. If you withdraw your consent, unfortunately, you will not be able to use our medical services.

Duration of Data Management:

In accordance with Act paragraph 30. § (1) of Act XLVII of 1997 on the Management and Protection of Healthcare and Personal Data Related to them, we will keep the health records for 30 years from the date of the data collection.

2. Only physicians involved in the treatment can have access to the health-related data required for the provision of health service. Health data may be handled by other persons (e.g. assistant, dispatcher, masseur, etc.) engaged in the medical treatment of the patient concerned in accordance with the instructions of the treating physician or to the extent necessary for the performance of their duties.
3. Recording health data is part of medical treatment. The physician involved in the treatment will decide which medical data is required to be taken in accordance with the professional rules. The consent to the management of the health and personal data of the person subject to the treatment shall be deemed to have been given, unless stated otherwise. The purpose of data management is to provide safe and professional treatment.
4. Health information may only be communicated to another physician or a third party at the request of the Guest, and the Guest's consent shall be requested in order a physician who has not previously been treated the Guest have access to the information recorded thereby; noting that the health data concerned may not be transmitted to the GP of the Guest only if the Guest gives specific instruction to prevent it.
5. Data controller and the person acting on his/her behalf and the data processor shall keep the medical secrets became known to him or her.
6. Data controller or his authorised agent shall be exempt from the obligation of confidentiality if:
 - a. the data subject or his or her legal representative has given his / her written consent to the transfer of the health and personal data, within the limitations set forth therein
 - b. the transfer of health and personal data is a legal obligation.
7. Data subject is entitled to receive information on the management of the data in the context of his or her medical treatment, to have access to his / her health and personal

identification data, to access the medical documentation and to receive a copy at his own expense.

8. Such right shall also be exercised by a person duly authorized by the data subject in writing for the duration of his or her care; after the completion of the care of data subject, by a person he or she authorises in a private document of full probative value.
9. Data Controller manages health data in accordance with the Data Protection Act and the related Act XLVII of 1997 on the Handling and Protection of Health and Personal Data.
10. Data Controller provides further information on the management of data collected during healthcare services at a request submitted to info@lotustherme.net. The deletion of data can be initiated by the data subject at the same email address.

Bank card details

1. Data Controller shall only use and use the bank / credit card / bank account details provided to him or her to the extent and for the time necessary for the exercise of his or her rights and fulfilment of his or her obligations. The data concerned are managed by the contractual banking partners of the Data Controller. You can find more information about this data management on the websites of the Bank concerned.
2. For more information on bank card data managed by certain subsystems of the Data Controller, guests may obtain further information at info@lotustherme.net.
3. The hotel operated by Data Controller and is a szép-kártya and egészségkártya (szép card and health card) acceptance point, subject to the same privacy protection as Bank Cards.
4. The Hotel is entitled to request bank card pre-authorization or authorization to secure future service charges.

Lotus Privilege Card Frequent Guest Program

1. Data Controller Frequent Guest Program is an exclusive service provided to hotel guests - natural persons – aiming at providing discounts to returning guests.
2. Participants in the program concerned give their explicit consent to the Data Controller to process their personal data provided for this purpose for the purpose of operating the Frequent-Guest System, or specifically for the purpose of sending newsletters to frequent guests. Based on this consent, the personal data transferred will be handled until the data subject participates in the program.
3. Data Controller is entitled to forward the data thus provided to its authorized agents, subcontractors, data processors and foreign affiliates for the purpose of operating the program concerned, under the condition that no personal data thus received will be disclosed to third parties other than their data controllers. If the recipients of the data transfer differ from the provisions of this clause, the Data Controller shall provide information about their identity before the data management and consent thereto.
4. The organization managing the storage, operation, and system management of the Data Controller's frequent guest program:

CARDNET Kft. 46-48 Reitter Ferenc u. Budapest, Hungary 1135

Company registry number:01-10-042150

5. If the guest concerned does not approve the data transfer, it will make it impossible for him / her to participate in the program, which will result in his / her removal from the program.
6. Membership status of the Frequent Guest Program becomes inactive after 4 (four) years of the last use of hotel services. The Data Controller stores the personal data of the member for a period specified in the relevant tax and accounting regulations and deletes them after that deadline.

7. Personal data managed in the programs serve to keep contact. Personal data managed by programs are the same as guest checking-in registration details.
8. Data Controller stores the personal data provided in a separate file system, separately from other data provided. This dataset can only be accessed by employees authorized by the Data Controller.
9. Employees shall not transmit individual data or entire data files to a third party and takes all security measures to prevent them from being disclosed to an unauthorized person.
10. Additional personal data may be required to participate in the programs, in which case the Data Controller shall inform the person concerned about the purpose, method and duration of the data management at the same time as the data is requested.
11. The data of the frequent guests (natural persons) can be used for market research purposes, however, frequent guests have to be informed beforehand and their prior consent must be obtained.
12. At the request of the guests concerned sent to info@lotustherme.net, the data controller deletes the data managed by the frequent guest program.

Gift Vouchers

1. Data Controller allows guests to purchase various gift vouchers for the hotel operated by him or her, which can be used for hotel services according to their value.
2. Ordering and using the gift voucher is voluntary.
3. Ordering a gift voucher and a range of data affected by data management:

The person concerned may order vouchers of the amount specified by him or her by contacting the hotel in person, by phone, by email, or through the website <http://lotustherme.net/ajanlatok/ajandekutalvany> while providing the following details:

When ordering in person:

- name*
- billing name and address *

When ordering by phone, website or e-mail

- name*
- address*
- e-mail address*
- Phone Number *
- means of payment*
- number and value of the gift vouchers
- mailing name and address if different from the billing address
- comment
- Data marked with * are mandatory.

4. Data Controller will issue an invoice for the amount of the agreed and ordered voucher and issue a numbered voucher upon receipt of the amount and deliver it to the address provided.
5. Data Controller stores the personal data provided in a separate file system, separately from other data provided. This dataset can only be accessed by employees authorized by the Data Controller.
6. Employees shall not transmit individual data or entire data files to a third party and takes all security measures to prevent them from being disclosed to an unauthorized person.

7. Data Controller shall store the data for a period of time in accordance with the applicable tax and accounting regulations and shall delete them after the expiry of the time limit concerned.

Guest questionnaire, assessment system

1. Guests can provide their opinions via online, e-mail and paper-based guest questionnaires, as well as through the use of a complaint management system operated by Data Controller as part of the quality assurance process.
2. When completing the questionnaire, guests shall provide the following personal information:
 - name
 - date of arrival and departure
 - room number
 - Email address
 - mailing address
3. Provision of data is not mandatory; it only serves to investigate possible complaints and to provide the Data Controller a chance to respond to the guest.
4. Opinions obtained in this manner and any related data that may not be related to the Guest concerned, and may not be associated with the name of the Guest may also be used by the Data Controller for statistical purposes.
5. The personal data given here are destroyed by the Data Controller after possible response or statistical recording of the parts may not be associated to the reviewing guest.
6. Employees shall not transmit individual data or entire data files to a third party and takes all security measures to prevent them from being disclosed to an unauthorized person.

Facebook site

1. Data Controller and hotel operated by the Data Controller and their services are available separately as well on the Facebook social network portal.
2. The purpose of data management is to share content on the website. With the Facebook page, the Guest can find information about the latest promotions.
3. By clicking on the "like" link on the Facebook page of the Data Controller, the data subject contributes to the publication of the Data Controller's news and offers on its own message wall.
4. Data Controller also publishes images / videos on various current events on its relevant Facebook page. Unless it is a recording depicting a crowd of people, Data Controller will request the written consent of the data subject before publishing the images.

Website Visiting Data

1. Links
 - 1/1. Data Controller's website may contain links that are not operated by the Data Controller, but serve only to inform visitors. Data Controller has no influence on the content and security of the websites operated by the partner companies, so it is not responsible for them.
2. Cookies
 - 2/1. Cookies are important for the proper functioning of the site. In order to enhance user experience, Data Controller uses cookies on his or her website that remind the User of his or her order details and provide secure room reservation, request for offer, collect statistical data to optimize the functions of the site, and display customized

content according to the user's interests. Cookies are accepted by clicking on the "I agree and continue" button, and then go directly to the page: a detailed description of the types of cookies can be accessed by clicking on the "More Info" button, where you can choose to accept the use of each cookie while staying on the site. Please note that if you choose to disable cookies, you have to give up using certain features of the website.

STORING PERSONAL DATA, INFORMATION SECURITY

1. Personal data may only be managed in accordance with the activities described above, for the purpose of data management.
2. The purpose of data management: getting into contact and keeping contact with the data subject, marketing, increasing the level of service matching the Data Controller's profile, conducting market research and assessing consumer habits.
3. Legal grounds for data management: voluntary consent of the data subject based on prior information by the Data Controller.
4. Duration of data management: Personal data is stored at the level of the individual data fields, not at the level of all the data relating to the particular guest. For example, we may keep your name and login day longer than your email address. Data managed to provide services will be stored for 2-8 years depending on the data concerned. In some cases, we have a legal obligation to keep personal information for longer. The main categories included are as follows:

If the data is required for billing or other tax records, we have a legal obligation to keep the data for at least 8 years from the end of the calendar year concerned.

The hotel has a legal obligation to report all the guests to local government and all guests arriving from outside the EU must be reported to the police. We have a legal obligation to keep the data included in these reports for 6 years from the date of checking-in.

By ticking the appropriate box to keep your data in order to simplify future bookings (data management purpose), the legal grounds for data management will be your voluntary consent. Therefore, if you do not give your consent to the management of your data by ticking the box, you will need to re-enter it when making your next booking. You may revoke your consent at any time; however, the revocation does not affect the prior lawful processing of the data. In such cases, your personal information will be stored for 8 years from your last booking.

After the expiry of the longest period of time of the data storage durations above, the data will be deleted from the relevant retention periods.

5. Duration of data management: 15 business days after the termination of the customer relationship, if they do not have to be used to enforce the rights and obligations arising from the customer relationship or until the data are deleted to the request of the data subject or until he or she revokes his or her consent to data management.
6. You can change or cancel your personal data, revoke your voluntary consent, and request information about the management of your personal data by contacting info@lotustherme.net
7. Data Controller shall ensure that the IT environment used for the provision of personal information in the provision of the service is provided in such a way that the personal data provided by the data subject is only linked to the data and in the manner specified in this policy, and make sure that only those colleagues of the Data Controller could access such data whose job responsibilities makes it inevitably necessary. All the changes to the data will be made by indicating the date and time of the amendment.

Defective data will be deleted within 24 hours based on the relevant request of the person concerned.

Data are backed up.

8. Data Controller provides the required level of protection in the course of the management of the data, in particular in the course of storage, correction, deletion and the data requesting or protesting by the data subject.
9. Data transfer shall be carried out with the consent of the data subject, without the injury to his or her interests, confidentially, and in full compliance with the proper purpose, legal grounds and principles of the data management by using perfectly appropriate IT system. Data Controller shall not forward the personal data of the data subject without his or her consent, and shall not make it available to a third party, unless required by law.
10. Other unidentifiable data, considered as anonymous in the following, that cannot directly or indirectly related to the data subject are not considered personal data.
11. Operator of the hotel IT system of the Data Controller, based on the contract concluded between the parties

ORACLE Hungary Kft. 7 Lechner Ödön fasor, Budapest, Hungary 1095

Tax ID.:10845606-2-44

Represented by Balázs Megyesi

ELECTRONIC SURVEILLANCE SYSTEM

1. Data Controller also operates an electronic surveillance system on the area of the Lotus Therme Hotel & Spa Hévíz.

2. Please note that the rules for the use of the electronic surveillance are set out in the provisions of Act CXXXIII of 2005 on the Rules of Personal and Property Protection and Private Investigation activity (SzvTV) as well the provisions of Act CXII of 2011 on the Right to Information Self-Determination and Freedom of Information (Info tv.) are applicable. Accordingly, the operation of the electronic surveillance system is governed by the provisions of chapter 30. § (2) of SzvTV. in order to protect human life, physical integrity and property, as well as to prevent, detect, and prove violations of the law and offenses, as detailed below, as well as to intercept perpetrators. As the use of the electronic surveillance system also involves data management, this activity is under the control of the National Authority for Data Protection and Freedom of Information (NAIH).

3. Please note that if you enter the room monitored by the camera in the knowledge of the present policy, it is considered a definite consent to data management.

4. The registration number of data management by Hotel Garden Kft. is: NAIH-69604/2013

5. The scope of the data managed: the visitor's portrayal visible in camera recordings and other personal information.

6. The electronic surveillance system operates 24 hours a day, 7 days a week.

Areas monitored by a camera are also indicated by pictograms and warning labels.

7. Only authorised persons can view the recordings of the camera recordings of the surveillance camera system operated by Hotel Garden Kft. in order to prove the violation of human life, bodily integrity and property and to identify the perpetrator, or to discover other events or accidents affecting human life or physical integrity.

8. The operation of the electronic surveillance system is performed by the hotel's contracted property-protection partner:

NBH Vagyonvédelmi Kft.

8. Fekete u. Vác, Hungary 2600

Company Registry Number: 13-09-176293

9. Hotel Garden Kft. records insights into the recordings, the name of the person involved in them, the reason and time of getting to know the data. In order to manage personal data securely, the protection of the data stored on the servers detailed below will be provided by a personal username and password that can be used to identify which authorised person accessed to the data and when.

10. The transfer of data is only possible in the case of proceedings in progress related to unlawful conduct or breach of obligations, to the authorities or courts conducting such proceedings. The scope of data provided may include recordings of relevant information taken by the camera system, as well as the names of persons who may be involved in the recording concerned.

11. Please note that those affected by the right or legitimate interest in capturing an image may request a copy of the images taken by the electronic surveillance system and may request the deletion of the recordings in accordance with the relevant legal provisions. In addition, all those whose right or legitimate interest is affected by the recording of the image, can request within 3 working days of the date the recording was taken by proving his or her legitimate interest, that the data concerned be not destroyed or deleted by Hotel Garden Kft..

We also inform you that you can request information from Hotel Garden Kft. at any time about the management of your personal data. You may also request the rectification or blocking of your personal data in accordance with the applicable legal provisions. You may also object to the processing of your personal information.

Please be advised that in the event of the violation of your rights, you may go to court in accordance with the provisions of the applicable law, and, through notifying NAIH (National Authority for Data Protection and Freedom of Information), anyone may initiate an investigation by claiming that there has been a violation or a direct threat to the processing of personal data.

OPTIONS OF LEGAL REMEDY

1. Data subject may request information on the management of his or her personal data and may request the rectification or blocking of his / her personal data, with the exception of the data processing provided by law, by email at info@lotustherme.net, as or regarding certain activities covered by the data management according to the rules set there.
2. At the request of the data subject, Data Controller shall provide information on the data it manages, the purpose of the data processing, its legal grounds, duration, details of data processor, if it has used a data processor, the circumstances and effects of the data protection incident and the measures taken to prevent it, and - in case of transfer

- of the personal data of the data subject - the legal grounds, the purpose and the recipient of the data transmission concerned.
3. Data Controller corrects or erases inaccurate personal data if:
 - a. their management is unlawful;
 - b. it is requested by the data subject;
 - c. they are incomplete or erroneous – and this cannot be legally remedied – provided that the cancellation is not prevented by law;
 - d. the purpose of the data management has ceased to exist or the statutory deadline for storing the data concerned has expired;
 - e. it has been ordered by the court or the National Authority for Data Protection and Freedom of Information.
 4. Data Controller shall notify the person concerned of the correction and deletion, as well as all those to whom the data was previously transferred for data management purposes. The notification may not be necessary if it does not violate the legitimate interest of the data subject with respect to the purpose of data management.
 5. Data subjects may object to the processing of their personal data if
 6.
 - a. the processing (transfer) of personal data is only necessary for the purpose of enforcing the data subject's right or legitimate interest, except in the case of mandatory data management;
 - b. the use or transfer of personal data has taken place for direct marketing, opinion polling or scientific research;
 - c. exercising the right of objection is permitted by law anyway.
 7. Data Controller shall – with the simultaneous suspension of data management – investigate the protest as soon as possible after the submission of the request, but within a maximum of 15 working days, and shall inform the requestor in writing of its outcome. If the requestor's objection is well founded, Data Controller shall terminate the data management concerned, including further data collection and data transfer, and locks the data, and notifies the persons to whom the personal data affected by the protest has previously been transmitted of the protest or measures taken based on it, and who are obliged to take action in order to enforce the right of protest.
 8. If the data subject disagrees with the Data Controller's decision or the Data Controller fails to comply with the time limit referred to in Section 6, he / she shall have the right to apply to the court within 30 days of its notification.
 9. Judicial Enforcement: The person concerned may apply to a court for violation of his rights. The court acts in the case as a matter of urgency. Data Controller must prove that the data management complies with the relevant provisions of the law.
 10. In the event of violation of your right to self-determination, you may file a complaint with the National Authority for Data Protection and Freedom of Information and at the Court.
 11. In addition to these rights, if you believe that the Data Controller has acted inappropriately with regard to your personal data or data protection, please contact us so that we could remedy the situation and improve our services provided to our guests.

Hévíz, Hungary

25 May 2018

The Hotel Management