PRIVACY POLICY OF
Monastery Boutique Hotel

Date of entry into force: 25 May 2018
Updated: 1 September 2021, 21 March 2024, 31 August 2024, 5 November 2025

Monastery Boutique Hotel, as a member of the Accent Hotels chain, places great importance on protecting your personal data. This Privacy Notice provides information on how we collect, use, and protect personal data in connection with our services, including our online booking system and newsletter. Below we provide you with information about what we do to protect your data and what data we collect and process, for what purposes.

1. INTRODUCTION

KAPU VÁRALJA ÜZEMELTETŐ Kft. (registered office: 1011 Budapest, Fő utca 30.; company registration number: 01-09-290307; tax number: 25808984-2-41) (hereinafter referred to as **"Data Controller"**), as the operator of Monastery Boutique Hotel, acknowledges the contents of this Privacy Policy as binding on itself as Data Controller in the course of the services it provides.

Personal data of guests, contractors, personal contributors, job applicants and employees who use the services of the Data Controller (hereinafter referred to as "**Data Subject**") are processed by the Data Controller. The Data Controller undertakes to ensure that the processing of data relating to its services complies with applicable law and the requirements set out in this Privacy Notice.

The Data Controller reserves the right to unilaterally amend this Notice. In this regard, it is recommended that you regularly visit https://accenthotels.com/hu/adatvedelem in order to monitor any changes. The current content of this Notice can be consulted and downloaded at any time. If we have the e-mail address of the Data Subject, we will notify you of any changes by e-mail at your request.

We will send you a copy of the current version of the Notice at your request.

By providing the personal data concerned, the Data Subject declares that he or she has read and expressly accepted the version of this Notice in force at the time of providing the data.

The requirements set out in this Privacy Notice are in accordance with the applicable data protection legislation:

- The Fundamental Law of Hungary (Freedom and Responsibility, Article VI);
- REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of natural persons with regard to the processing of personal data and on the free movement of such

data, and repealing Regulation (EC) No 95/46/EC (General Data Protection Regulation);

- Act CXII of 2011 on the Right to Informational Self-Determination and Freedom of Information (Infotv.);
- Hungarian Civil Code, Act V of 2013;
- Hungarian Consumer Protection Act, Act CLV of 1997;
- Section 6 of Act XLVIII of 2008 on the Basic Conditions and Certain Restrictions of Economic Advertising Activity;
- Act CLVI of 2016 on State Tasks for the Development of Tourist Areas;
- Act C of 2003 on Electronic Communications.

1.1. Data Controller Information

Name: KAPU VÁRALJA ÜZEMELTETŐ Kft.
Location: 1011 Budapest, Fő utca 30.
Company registration number: 01-09-290307
Tax number: 25808984-2-41
Hotel name: Monastery Boutique Hotel
Hotel address: 1011 Budapest, Fő utca 30.

The contact details of the Data Controller through which the Data Subject may exercise the rights set out in this Notice:

E-mail: info@monasteryhotel.hu
Postal address: 1011 Budapest, Fő utca 30.
Telephone: +36 1 770 8210
Website: https://monasterybudapest.accenthotels.com/hu
Data protection officer: Nikoletta Kovács
Data protection officer contact: nikoletta.kovacs@accenthotels.com

2. BASIC CONCEPTS OF DATA PROTECTION

2.1. Personal data

Any data that can be associated with a specific natural person (identified or identifiable), including any conclusions or inferences that can be drawn from such data in relation to the data subject. The personal data shall retain this quality during processing for as long as the link with the data subject can be established. In particular, a person may be regarded as identifiable where he or she can be identified, directly or indirectly, by reference to a name, an identification mark or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity;

2.2. Consent

A voluntary and explicit indication of the data subject's wishes, based on appropriate information, by which he or she gives his or her unambiguous consent to the processing of personal data concerning him or her, either in full or in relation to specific operations;

2.3. Objection

A declaration by the data subject objecting to the processing of his or her personal data and requesting the cessation of the processing or the erasure of the processed data;

2.4. Data Controller

The natural or legal person or unincorporated body which determines the purposes for which personal data are processed, takes and implements the decisions concerning the processing (including the means used) or has the processing carried out by a processor on its behalf;

2.5. Data processing

Regardless of the process used, any operation or set of operations which is performed on personal data, such as collection, recording, organisation, storage, alteration, use, disclosure, transmission, alignment or combination, blocking, erasure and destruction, and prevention of further use of the data. Processing also includes the taking of photographs, audio or video recordings and the recording of physical characteristics that can be used to identify a person (e.g. fingerprints, palm prints, DNA samples, iris scans);

2.6. Data transmission

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

2.7. Data deletion

Making data unrecognisable in such a way that it is no longer possible to recover it;

2.8. Data storage

The act of retaining personal data in a form that permits identification of the data subject for no longer than necessary for the purposes for which the personal data are processed.

2.9. Technical data processing operations

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

2.10. Data processor

A natural or legal person or unincorporated body that processes personal data on behalf of the controller, including on the basis of a legal mandate;

2.11. Third party

A natural or legal person or unincorporated body other than the data subject, the controller or the processor;

2.12. Guest

A natural person who is authorised to be present on the real estate covered by the territorial scope of the Data Protection Policy and who is not an employee of the Data Controller.

2.13. EEA country

A Member State of the European Union and another State party to the Agreement on the European Economic Area, as well as a State whose nationals enjoy the same status as nationals of a State party to the Agreement on the European Economic Area under an international treaty concluded between the European Community and its Member States and a State not party to the Agreement on the European Economic Area;

2.14. Third country

Any state that is not an EEA state.

2.15. Data protection incident

A breach of security that results in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

2.16. Security incident

Any event that may have a detrimental effect on the confidentiality, integrity or availability of an IT device or the data stored on it.

2.17. Confidentiality (secrecy)

The characteristic of the data is that only a predefined group of users (authorised users) is allowed access, access by everyone else is illegal.

2.18. Intactness

The criterion of existence, authenticity, integrity, and intrinsic completeness of data, which ensures that the data, information or program can only be altered by those authorised to do so and cannot be altered without being detected.

2.19. Access, use and transfer of data

Personal data stored about data subjects may be accessed only by the person who needs to know them in order to fulfil his or her obligations. The name of the person who has access to the personal data or who is otherwise entitled to have access to the personal data, the reason for and the time of access to the data shall be recorded in a record.

Use is when personal data is used as evidence in judicial or other official proceedings. A person whose right or legitimate interest is affected by the recording of his or her personal data may, within 3 (three) working days of the recording of the personal data, request that the data not be destroyed or erased by the controller by providing evidence of his or her right or legitimate interest. At the request of a court or other authority, the personal data shall be transmitted to the court or authority without delay. If no request is made within thirty (30) days of the request for non-destruction, the recorded image and/or sound recording and other personal data shall be destroyed or erased.

Personal data may be disclosed to third parties only with the prior written consent of the data subject. This does not apply to the processing described in the Privacy Notice or to any transfers required by law, which may only take place in exceptional cases. We inform data subjects that we use data processors to process and store the data processed in our employer's human resources system. The Data Controller will inform the data subjects about the identity of the processors in this document.

2.20. Asset protection security system

Electronic signalling and image surveillance systems installed for the purpose of asset protection on the properties falling within the territorial scope of the Data Protection Regulation. It also includes electronic surveillance systems operated without recording for the purpose of surveillance or which also permit the recording of sound or images (surveillance), electronic access control systems, intrusion detection systems, remote monitoring systems, security systems for data and IT protection, and other electronic technical solutions which also permit the transmission of signals and images or the signalling of light or sound.

3. DATA PROTECTION PRINCIPLES

The processing of personal data must comply with the following principles:

a) must Lawfulness, fairness and transparency: Personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject.

b) Purpose limitation: Personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered incompatible, in accordance with Article 89(1) GDPR.

c) Data minimisation: Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

d) Accuracy: Personal data must be accurate and, where necessary, kept up to date. Reasonable steps must be taken to ensure that personal data that are inaccurate are erased or rectified without delay.

e) Storage limitation: Personal data must be kept in a form that permits identification of data subjects for no longer than is necessary. Longer storage is only allowed for archiving in the public interest, scientific or historical research or statistical purposes, subject to appropriate safeguards under Article 89(1) GDPR.

f) Integrity and confidentiality: Personal data must be processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The controller shall be responsible for, and be able to demonstrate compliance with, all of the above principles ("accountability").

4. DETAILED RULES ON THE PROCESSING OF PERSONAL DATA

The following parties may have access to personal data:

- employees of the Data Controller;
- employees of the Data Processors listed below;
- certain public authorities, where data is requested as part of an official procedure and the Data Controller is legally obliged to provide it;
- employees of debt collection agencies appointed by the Data Controller to manage overdue payments;
- other persons with the explicit consent of the Data Subject.

The Data Controller undertakes to treat all personal data as strictly confidential and shall not disclose such data to any third party unless the Data Subject has given prior explicit consent.
The withdrawal of consent shall not affect the lawfulness of the processing carried out before its withdrawal.

4.1. Data required for registration and management of additional data provided in the user account

In order to use the services of Monastery Boutique Hotel, the Data Subject must complete a registration form. The data provided will be used to access and utilise specific services. In the case of paper registration, the Data Controller will process the data under the same conditions as for online registration.

A user account is created in the online interface when you make a booking, allowing you to manage and track future bookings and easily provide customer service support. The account can be deleted, but the contractual data related to the booking will continue to be retained in accordance with applicable legal requirements. In the case of online bookings, some of the data is transferred to the Data Controller by the individual accommodation intermediaries, travel agencies and Accent Hotel Solutions Szolgáltató Kft, which acts as a data processor on behalf of the respective hotel.

The scope of the data processed and the detailed purposes of the processing:

- Data required for registration
  - Last name: necessary for identification, communication, contract performance
  - First name: necessary for identification, communication, contract performance
  - Sex of the Data Subject: necessary for identification, communication
  - E-mail address: identification
  - Password: authentication
- User account personal data
  - Address: necessary for identification, communication
  - Date of birth: required to send a greeting, unique gift discount
  - Name day: greetings, required to send a unique gift discount
  - Language: required for the provision of the convenience service
  - Number of children: necessary to provide the service of convenience, to fulfil the contract

- Contact details:
    - mailing address / home address: necessary for contacting you, providing you with a service of convenience
    - telephone: necessary for communication, to provide convenience services
    - e-mail address: required for contact and to provide convenience services
- Data on preferences, purchasing habits
    - requesting a barrier-free hotel service, necessary for the provision of amenities
    - special dietary requirements: to meet the Data Subject's tastes, to fulfil a contract, to provide a convenience service
    - other preferences, optionally provided, necessary for the provision of the amenities

Legal basis for processing

Data processing is carried out on different legal bases, depending on the purpose for which the data is used:

Performance of a contract (Article 6(1)(b) GDPR):
The processing of personal data provided during the booking is necessary for the performance of the contract between the Data Subject and the Data Controller. The creation of the account is linked to the booking process, and therefore the legal basis for the processing of the data is the performance of a contract. However, the processing of certain data related to the account requires the consent of the Data Subject (see below).

Consent of the Data Subject (Article 6(1)(a) GDPR):
Certain personal data (e.g. date of birth, name day, preferences) are processed only with explicit consent.

Legal obligation (Article 6(1)(c) GDPR):
In the case of invoices related to orders resulting from bookings, the legal basis is the fulfilment of a legal obligation under the provisions of the Accounting Act (Article 6(1)(c) GDPR).

Duration of processing

In order to protect the performance of the contract and the legal claims arising from it, the Data Controller keeps the data related to the reservations for 5 years from the last reservation of the Data Subject, after which, according to Section 6:22 of the Civil Code of Hungary, the data will be anonymised. The data will be kept for longer than this period if required by law, for example, if we are obliged to keep the data pursuant to Section 169 of Act C of 2000 on Accounting, the data will be deleted after 8 years following the termination of the relationship with the Data Subject. In practice, this applies when the data forms part of supporting accounting documents, such as the documents relating to the conclusion of the contract (the contract itself, where applicable) or the invoice issued.

The Data Controller shall store the data processed on the basis of consent until the account is closed or until the Data Subject requests its deletion. In response to such a request, the Data Controller shall delete the data without undue delay, unless it is required by law to continue retaining them. Consent may be withdrawn at any time in writing by sending a message to the Hotel info@monasteryhotel.hu e-mail address or postal address (1011 Budapest, Fő utca 30.).

4.2. Data processing, mandatory registration and reporting of registration of accommodation users

Upon check-in at the accommodation, the Data Controller records the required data in the VIZA system—a closed, multi-level asymmetric encryption-protected IT system—hosted on servers provided by the hosting service designated by the Government. The purpose of collecting this data is to protect the rights, safety, and property of the Data Subject and others, as well as to monitor compliance with regulations concerning the stay of third-country nationals and individuals with free movement and residence rights. Therefore, the primary aim of the VIZA system is to promote public order, public safety, border security, and the protection of the rights, safety, and property of the Data Subject and others.

Purpose of data processing

The purpose of the recording of guest data is to ensure the contractual performance of the accommodation service, to keep legal records of the service and to Support the objectives set by the Government and fulfilling legal obligations necessitate the processing of personal data.

Scope of data processed

The Data Subject using the accommodation service:

- surname and given name
- surname and given name at birth
- place and date of birth
- gender
- your nationality
- mother's maiden name and surname

The Data Subject using the accommodation service:

- identification details of your identity document or travel document,
- use of a motor vehicle: necessary for the provision of a service of convenience,
- vehicle registration number (necessary for providing convenience services and fulfilling the contract)
- a scanned image of your identity document
- for third-country nationals, the visa or residence permit number,
- the date and place of entry,

Information related to accommodation services:

- the accommodation booking confirmation identifier
- accommodation name, exact address, room number
- start, expected and actual end dates of use of the accommodation.

And for guests from outside the European Union:

- Citizenship: required for identification, contract performance
- Passport number: fulfilment of a legal obligation
- Visa number: to fulfil a legal obligation
- Date and place of entry: to fulfil a legal obligation

In the case of a minor or a legally incapacitated guest, the guest's personal data shall be provided by the legal representative on the registration form, who shall also complete and sign the data protection declaration. In this context, the following personal data of the legal representative may be recorded:

- name of the legal representative,
- signature,
- date of signature.

Registration of Minor or Legally Incapacitated Guests

The provision of personal data required for the use of accommodation services, as well as the completion of the related declarations, may only be carried out by the legal representative (parent, guardian or custodian) in the case of a minor or legally incapacitated guest. The declarations included in the registration form must also be signed by the legal representative in such cases. The accommodation provider is entitled to verify that the person making the declaration is indeed the guest's legal representative. The data provided in this manner shall be processed on the legal basis of the performance of the accommodation service contract and compliance with legal obligations.

Legal basis for processing

The legal basis for data processing is contract performance (Article 6(1)(b) GDPR) concerning data necessary for service provision, and legal obligation fulfillment (Article 6(1)(c) GDPR) regarding personal data uploaded to the VIZA system. The data provision process is prescribed and regulated by Act CLVI of 2016 on the State Tasks of the Development of Tourist Areas.

In the case of a minor or legally incapacitated guest, the data provided by the legal representative shall also be processed on the same legal bases — performance of a contract and compliance with legal obligations. The legal framework for representation is set out in the Hungarian Civil Code (Act V of 2013), Sections 2:10 (1) and 2:14.

Duration of processing

Data processed for data provision purposes are stored until the last day of the first year following their collection. Subsequently, the Data Controller deletes the personal data from the records. The VIZA system retains submitted data for a maximum of two years.

Group registration and arrival of children's groups

For reservations made by organized groups (e.g. school, sports, or cultural groups), the hotel may request personal data in advance from the group organizer or leader in order to streamline the check-in process and to prepare for data entry into the VIZA system. The group leader must confirm in writing that they are authorized to provide the data.

In the case of children's groups, the group leader (e.g. teacher or coach) must also declare in writing that they have obtained the legal guardians' consent for the processing of the children's personal data. The group leader is responsible for ensuring the validity of these consents. The hotel retains these declarations for five years after the purpose of the data processing has ended.

The legal basis for the processing of personal data is the performance of the accommodation contract (Article 6(1)(b) GDPR) and compliance with a legal obligation (Article 6(1)(c) GDPR). Health-related data (e.g. food allergies, sensitivities to medication, or other information needed for services such as massages) may only be provided with the explicit consent of the data subject or their legal representative. Separate information is available regarding the processing of such data.

4.3. Data processed during the check-in and check-out process

Guests, visitors, customers, partners and employees may enter the area operated and controlled by the Data Controller. In order to ensure secure access and arrival, the Data Controller may apply various measures based on an assessment of the associated risks.

Purpose of Data Processing

The Data Controller aims to minimise the security risks associated with the admission and arrival of guests, visitors, customers, partners and employees and to take necessary and proportionate measures. In special cases, where justified by law or security considerations, the Data Controller may restrict the access of data subjects. In order to ensure the secure management of the access process, the Data Controller may, on the basis of the current risk assessment, apply different solutions in accordance with the applicable legislation.

Scope of the data processed

Personal data concerning the entry of the Data Subject as a guest, visitor, customer or partner:

- name: required for registration
- time of entry: identification, verification
- date of departure: identification, re-verification
- name of the recipient: identification, verification

Information on documents proving good health (if required by applicable legislation or health regulations):

- the data on the vaccination certificate
- the personal data on the identification document (e.g. identity card, driving licence, passport) required to accept the vaccination certificate.

Legal basis for processing

Legitimate interest of the Data Controller (Article 6(1)(f) GDPR) to reduce security risks related to access, or to comply with a legal obligation (Article 6(1)(c) GDPR) where applicable legislation or government regulations impose data processing obligations related to access.

Designation of legitimate interest

The data controller receives a large number of external guests and visitors every day, which may pose an increased security risk. The access and arrival process allows for the verification and traceability of visits and thus contributes to the reduction of risks. The measures are proportionate to security, taking into account the rights and interests of visitors and employees.

Duration of processing

As a general rule, personal data of data subjects are not stored. If justified by law or security reasons, the controller may keep the data for a maximum of 1 year from the date of access. The data retention period will always be adapted to the legal requirements in force and the purpose of the processing.

4.4. Use of body temperature measurement on entry

The Data Controller may use body temperature measurement as a uniform protection measure for all persons intending to enter its premises or buildings owned or used by it.

Body temperature measurement is carried out without identifying the data subject and without storing or transmitting any related personal data. The services are then only used by those persons who can be authorised to access the services on the basis of the body temperature measurement.

Justification

The mere fact that someone has a higher body temperature does not in itself lead to the conclusion that they are infected with a pathogen, such as a new type of coronavirus, so the Data Controller's staff will not draw any conclusions about the health of the person based on the body temperature measurement at the time of entry, but is entitled to grant or deny access. The Data Controller therefore does not store any personal and health data and only decides whether to allow or deny access to a person wishing to enter its territory (because the results of the measurement indicate a risk to other persons).

If access is refused by the person acting on behalf of the Data Controller, it is the Data Subject's responsibility to deal with the situation (seeking medical advice, arranging sick leave, informing their manager at work, etc.), and the Data Controller has no further obligation or responsibility in this regard.

4.5. Processing of bank card data

The Data Subject is required to provide credit card details in order to guarantee and fulfil the booking. In case of online booking, part of the data is transferred to the Data Controller by the individual accommodation intermediaries, travel agencies and Accent Hotel Solutions Szolgáltató Kft, which acts as a data processor on behalf of the respective hotel.

The scope of the data processed and the detailed purposes of the processing:

- Name on bank card: required to complete the payment.
- Bank card number: required for the transaction.
- Bank card expiry date: required to validate the payment.

Legal basis for processing

Performance of a contract with a Data Subject pursuant to Article 6(1)(b) of the GDPR. The Data Controller uses a financial service partner (bank, payment service provider) to process credit card payments, which acts as a data processor.

Duration of processing

Credit card data is not stored by the Data Controller. Online payment transactions and prior authorisations are processed by the financial service provider. The Data Controller will retain payment transactions and related personal data (e.g. date of transaction, amount, payment status) for up to 8 calendar days after the guest leaves the hotel for settlement and possible refund purposes.

4.6. Loyalty Program

Accent Hotels operates a Loyalty Program. The service is operated by Accent Hotel Solutions Kft., a member of the Accent Hotels Group, and the Privacy Policy is available at https://accenthotels.com/hu/adatvedelem. The Welcome Back Loyalty Card can be applied for by the Data Subjects on the Accent Hotels website and by filling in the paper form available at each hotel. Any comments or questions regarding the Loyalty Program will be forwarded to Accent Hotel Solutions Kft.

The Data Controller provides personalised services and discounts to Data Subjects participating in the Loyalty Program. In order to receive the services and discounts, the Cardholder first verifies his/her eligibility by means of the Magnetic Loyalty Card at the terminal located in the Hotel, which can be used for this purpose, and then he/she can use the desired service or discount. The system connected to the terminal checks the validity and the balance of the loyalty card and then the transaction is carried out. No external parties have access to personal data related to the programme, and Loyalty Card Owners can only use the loyalty card for bookings made through Accent, via its website, e-mail, fax or telephone.

The Loyalty Card Owners will receive Points for purchases and service requests made at participating Partners, which will be credited to the Loyalty Card's unique Points Account and, if used, will be deducted from the Points Account according to the specific transaction. If the card reader establishes an electronic connection with the central computer system when each transaction is executed, the Loyalty Card can be used for Points redemption or Points accumulation up to the amount of Points in the Points Account.

Scope of data processed and detailed purposes of data processing

- Surname: necessary for identification, communication
- First name: necessary for identification, communication
- Company name: identification, communication, contract performance
- Regular customer identifier: required for the performance of the contract concluded

- Provision of a vehicle (e.g. car, parking service): necessary for the provision of convenience services and the performance of the contract, covering services such as vehicle rental, parking, or any related services requested by the guest.
- Personal data related to provision of services, assets, or equipment (e.g. vehicle, other amenities): necessary for the provision of convenience services, loyalty program benefits, and the performance of the contract, covering all services offered by the hotel, including any additional or special services requested by the guest.
- Content of the services requested: performance of the contract
- Value of service required: contract performance
- Current account balance data: contract performance, points management
- Transaction data for a current account: monitoring of user behaviour (statistical use) and investigation of the termination of the right

Legal basis for processing

The legal basis for the processing of data necessary for the operation of the loyalty programme is the performance of a contract (Article 6 (1) (b) GDPR). After the termination or cancellation of the contract, the Data Controller stores personal data related to transactions and performances under the loyalty programme for the purpose of verifying the lawfulness of the performances on the basis of legitimate interest (Article 6 (1) (f) GDPR).

Legitimate interest

It is in the legitimate interest of the Data Controller (Article 6(1)(f) GDPR) to be able to provide evidence of the related performances and transactions under the programme even after the termination of the contract related to the loyalty programme. The loyalty programme provides opportunities for a long period of time, it is important that the Data Controller can provide accurate and credible answers to questions arising even years after the card expires.

Duration of processing

After the termination of the relationship with the Data Subject, the Data Controller shall store the personal data processed in connection with the performance of the contractual obligation in accordance with the provisions of Section 6:22 of the Civil Code. The data will be deleted after 5 years. If we are required to retain the data pursuant to Section 169 of Act C of 2000 on Accounting ('Accounting Act'), the data will be deleted 8 years after the relationship with the Data Subject has ended. In practice, this applies when the data is part of supporting accounting documents, such as those relating to the conclusion of the contract (the contract itself, where applicable) or the invoice issued. Based on legitimate interest, the Data Controller may store data related to performances and transactions for a maximum period of 10 years from the termination or cancellation of the contract related to the Loyalty Programme.

4.7. Data processing related to event-related requests for proposals and orders

The Data Subject (Name of the contact person of a legal person) has the possibility to request an offer for an event from the Data Controller and to place an order with the Data Controller for the accommodation in question. The data are partly transferred to the Hotel by Accent Hotel Solutions Service Provider Kft.

Scope of the data processed and detailed purposes of the processing

- Surname, first name: identification, communication, contract performance
- Company name: identification, communication, contract performance
- Name of the contact person: identification, communication, contract performance
- Phone number: identification, communication, contract fulfilment
- E-mail address: identification, communication, contract performance
- Meal preferences: performance of contract
- Event agenda: contract performance
- Room request: fulfilling the contract
- Space requirements: contract performance
- Date, type of event: execution of contract
- Note: contract performance

Legal basis for processing

The legal basis for the processing is the performance of a contract (Article 6(1)(b) GDPR) and the legitimate interest of the Controller (Article 6(1)(f) GDPR).

Designation of legitimate interest

It is in the legitimate interest of the Data Controller to retain and manage offers in order to ensure effective communication with its business partners, to provide personalised services and to have appropriate documentation in case of potential disputes related to offers.

Justification of legitimate interest

It is in the legitimate business interest of the Data Controller to keep the offers made for a certain period of time, giving the data subject the possibility to return to a previous offer. Archiving offers helps to document pre-contractual negotiations and contributes to efficient business administration. The retention period is proportionate and offers are stored for up to 3 years in the absence of a contract, after which they are blocked or deleted by the Data Controller. Data subjects have the right to object to the processing.

Duration of processing

If the offer is accepted by the Data Subject, the data will be stored after the termination of the relationship with the Data Subject in accordance with the provisions of the Civil Code. 6:22 of the Privacy Act, we will block the data after 5 years. If the offer is not accepted by the Data Subject, the Data Controller shall store the data for legitimate reasons - the direct business interest of preserving the partners' previous offers - and block the data after 3 years.

4.8. Data processing related to contracting with partners

The Data Controller contracts with various partners to provide its services.

Scope of the data processed and detailed purposes of the processing

- Last name, first name of the contact person: for identification, communication, contract performance
- Photo: required for identification or where the contract involves photographic services
- E-mail address: required for identification, communication
- Telephone number: required for identification, communication
- Data concerning the legal person (name, registered office, company registration number, tax number): performance of the contract

Legal basis for processing

The legal basis for the processing is the consent of the Data Subject prior to the conclusion of the contract (Article 6(1)(a) GDPR), and thereafter the performance of a contractual obligation (Article 6(1)(b) GDPR).

Duration of processing

The Data Controller shall retain the personal data processed on the basis of consent until the Data Subject withdraws their consent. Data Subjects may withdraw their consent at any time by sending an email to the hotel's email address and requesting the deletion of their personal data.
In the case of the performance of a contractual obligation, the data shall be processed after the termination of the relationship with the Data Subject in accordance with Section 6:22 of the Civil Code. The data will be deleted after 5 years. If we are required to retain the data pursuant to Section 169 of Act C of 2000 on Accounting (the "Accounting Act"), the data will be deleted 8 years after the termination of the relationship with the Data Subject. In practice, this applies when the data forms part of supporting accounting documents, such as the contract (if applicable) or the issued invoice.

4.9. Data processing in relation to complaint handling

The Data Controller attaches the utmost importance to the satisfaction of its guests and the provision of high quality services. Data Subjects have the opportunity to submit complaints about their experience with the hotel.

The Hotel handles both verbal and written complaints in accordance with its internal complaint management policy. The policy is available at the reception and can be provided upon request.

The Hotel registers each submitted complaint and maintains a register to ensure transparency of the complaint handling process, traceability of complaints, and compliance with legal requirements. The purpose of the register is also to enable the Hotel to meet the accountability obligations set out in consumer protection legislation.

The Monastery Boutique Hotel also operates an abuse reporting system, which is primarily intended for employees and business partners. Guests wishing to report an issue may inquire at the reception desk for detailed instructions, policies, and available forms.

Scope of the data processed and detailed purposes of the processing

- Surname, first name: for the purpose of identifying the data subject and contacting them during the complaint handling process.
- Address (if applicable): for delivery of the reply letter by post.

- E-mail address: for information about the complaint and communication with the person concerned.
- Phone number: for faster contact (optional).
- Content of complaint: information needed to investigate the complaint.

Legal basis for processing

The processing is based on the fulfilment of a legal obligation pursuant to Article 6(1)(c) of the GDPR. It is mandatory processing under Article 17/A(7) of Act CLV of 1997 on Consumer Protection.

Duration of processing

The Data Controller processes the personal data related to the complaint, the record of the complaint, the copy of the response letter, as well as the data included in the associated register for a period of 5 years from the date the complaint is submitted, in accordance with the provisions of Act CLV of 1997 on Consumer Protection.

4.10. Data processing in relation to evaluation

The Data Subject has the possibility to give a rating of the accommodation. The rating can be completed anonymously, i.e. only for the rating.

Scope of the data processed and detailed purposes of the processing

- Surname: necessary for identification, communication
- First name: necessary for identification, communication
- E-mail address: required for identification, communication
- Date of stay – for satisfaction analysis and statistical purposes
- Hotel rating – for service quality assessment and statistical evaluation

Legal basis for processing

The legal basis for processing is the consent of the Data Subject (Article 6(1)(a) GDPR).

Duration of processing

The Data Controller shall store the data processed on the basis of consent until the account is closed or until the Data Subject requests its deletion. In response to such a request, the Controller shall delete the data without undue delay, unless it is required by law to continue to retain them. Consent may be withdrawn at any time in writing by sending a message to the Hotel info@monasteryhotel.hu e-mail address or postal address (1011 Budapest, Fő utca 30.) requesting the deletion of their personal data.

4.11. Careers

The Monastery Boutique Hotel provides the opportunity for the Data Subject to apply for the jobs advertised by the Hotel Chain through the interfaces provided by the Hotel Chain (e.g. Profession.hu, Career Portal and other application options within the Hotel Chain). The interfaces for managing applications are provided and

supervised by the Hotel Chain's head office, Accent Hotel Management Service Kft., while the technical background and the operation of the internal IT systems are the responsibility of Accent Hotel Solutions Kft.
The hotel, as a member of the Accent Hotel Chain, handles the applications received as an independent data controller. The Hotel Chain headquarters may provide technical support and oversee the application process for quality assurance purposes. Accent Hotel Management Service Kft. does not make hiring decisions for individual hotels, but may review applications for internal coordination purposes.

Scope of the data processed and detailed purposes of the processing

- Surname, first name: identification, contact
- E-mail address: identification, contact
- Telephone contact: contact
- Citizenship
- Highest level of education
- Exact title of qualification
- Work experience
- Professional and work-related preferences
- Any personal data voluntarily disclosed in documents attached to the CV (e.g. motivation letter, references).

Legal basis for processing

The processing of the personal data provided by the data subject in the course of a job application is based on the data subject's consent pursuant to Article 6(1)(a) of the GDPR.

Duration of processing

Following the selection of a suitable person for the vacant position, the Data Controller will inform the other applicants concerned that the employer has not selected them for the position in question and will request their explicit and voluntary consent in writing to the retention of their CV and other related documents containing personal data. The purpose of the processing is to enable the Data Subject to participate in future applications for employment with the Hotel Chain in a simplified manner. The Data Subject's explicit consent allows the processing of his/her personal data for a period of 5 years, after which the data will be anonymised. requesting the deletion of their personal data.

The Data Controller shall store the data processed on the basis of consent until the account is closed or until the Data Subject requests its deletion. In response to such a request, the Controller shall delete the data without undue delay, unless it is required by law to continue to retain them. Consent may be withdrawn at any time in writing by sending a message to the Hotel info@monasteryhotel.hu e-mail address or postal address (1011 Budapest, Fő utca 30.) requesting the deletion of their personal data.

If the Data Subject does not give his/her consent to the further retention of his/her personal data, the data will be anonymised within 30 days and the CVs will be destroyed.

Access to data

The data of applicants is accessed by the relevant Hotel Chain members as independent data controllers. Accent Hotel Management Service Kft. supports the data management processes as a data processor, but also has internal access rights in its role as the coordinator of the Hotel Chain headquarters and may act as a data controller in certain cases, if it is looking for suitable persons based on its own staffing needs or on the criteria of other hotels in the chain. Job portals (e.g. Profession.hu, Career Portal) and Accent Hotel Solutions Kft., which provides other application facilities for the hotel chain, act as data processors, providing a platform for the submission and storage of applications.

4.12. Newsletter

The Data Subject may subscribe to the Controller's newsletter through various channels, including the website, during registration or booking, via the user profile, when requesting an offer, or by filling out the paper registration form available at the Hotel or the form for joining the Loyalty Program. The hotel chain centrally manages the data of the subscribers and sends out the newsletters, however, the Hotel that decides to send out the newsletter is the data controller. Accent Hotel Solutions Kft. is the technical data processor responsible for storing the database and sending the newsletters. The hotel chain keeps a record in the newsletter database of when each subscriber gave their consent to receive the newsletter.

Monastery Boutique Hotel is entitled to send newsletters for direct marketing purposes at specified intervals and with specified content to the Data Subjects (to the e-mail address they have provided (which may be changed later)) who have subscribed to the newsletter service. The purpose of sending newsletters is to communicate to Data Subjects the latest offers, promotions, events and other relevant information relating to the Hotel.

In the case of subscriptions on paper forms, the Data Controller may request confirmation by e-mail to guarantee the accuracy of the data and the authenticity of the consent. Nevertheless, the consent given on paper is valid without confirmation by e-mail and the sending of newsletters is still legal in such cases. If the Data Subject does not confirm the subscription within 1 year, the Data Controller reserves the right to delete the data or to request further confirmation from the Data Subject.

The Data Controller will not send unsolicited advertising messages, and Data Subjects may unsubscribe from receiving the newsletter at any time, free of charge, without any restriction and without giving any reason. In this case, the Data Controller will not send further advertising offers or direct marketing messages to the e-mail address provided by the Data Subject.

The scope of the data processed and the detailed purposes of the processing:

- Surname: identification, contact
- First name: identification, contact
- E-mail address: identification, contact
- Specifying your interest: providing the right service
- Language: send messages in the appropriate language
- Company name (to be used for B2B communication): identification
- Headquarters (to be managed for B2B communication): contact
- Date, method of subscription: identification
- In case of online subscription, the name of the online interface: identification of the source of the consent

- Date and circumstances of unsubscription: identification

Legal basis for processing

The legal basis for data processing is the consent of the subscribing Data Subject, in accordance with Article 6(1)(a) of the GDPR and Article 6 of Act XLVIII of 2008 on the Basic Conditions and Certain Restrictions of Economic Advertising Activity. Under these provisions, the Data Subject may explicitly consent in advance to being contacted by the Service Provider with advertising offers and other mailings at the electronic contact details (e-mail) provided.

After unsubscribing, the legal basis for processing is the legitimate interest of the Data Controller (Article 6(1)(f) GDPR). The data will then be kept solely for purposes corresponding to the legitimate interest and will not be used for sending further marketing messages.

Designation of legitimate interest

It is in the legitimate interest of the Data Controller (Article 6(1)(f) GDPR) to retain the data necessary to justify the previous consent and to demonstrate the lawfulness of sending newsletters in the event of a dispute or legal proceedings.

Duration of processing

The Data Controller will keep the personal data in the active (sending) newsletter database until the Data Subject withdraws their consent. If the Data Controller requests confirmation of consent from the Data Subject, the data will be deleted within 60 days after the expiration of the confirmation period.

The related personal data of the Data Subject will remain in the Passive database, which does not process the sending of newsletters and is used solely for record-keeping purposes, for a period of 5 years after unsubscribing from the newsletter. This is to enable the Data Controller to demonstrate the lawfulness of previously sent newsletters, if necessary.

4.13. The presence of the Data Controller on social networking sites

The hotel operated by the Data Controller is available on the Facebook and Instagram community portal. The Data Controller allows the Data Subjects to express their opinions by clicking on the "like" link on the social networking which it has created and uses - https://www.facebook.com/monasteryhotelbudapest and https://www.instagram.com/monasteryboutiquehotel -, or to publish news and offers prepared by the Data Controller on their own pages. The operators of the social networking sites are separate data controllers, independent from the Data Controller, and therefore the activities carried out there are covered by data management documents independent from the Data Controller.

Natural persons who voluntarily follow, share or like the social networking site of the Data Controller - https://www.facebook.com/monasteryhotelbudapest, https://www.instagram.com/monasteryboutiquehotel - and the content displayed on it.

Purpose of data processing

- Communication through the channels offered by social networking sites

The Data Controller communicates with data subjects through social networking sites only if the Data Subject has previously contacted the Data Controller through the social networking site, and thus the purpose of the scope of the data processed becomes relevant.

- Sharing and disseminating information

  The purpose of the presence on social networking sites and the related data processing is to share, publish and promote the given content. On social networking sites, Data Subjects can find out about the latest offers and opportunities.

The Data Controller publishes textual content, images and videos on the social networking sites it manages, which may subsequently be published on other social networking sites in accordance with the rules of the social networking sites. Once published, the Data Controller has no way of monitoring and controlling further publications in any way. However, where the images published include specific individuals, unless they are crowd shots or public appearances, the Data Controller will always seek the written consent of the data subject before publishing the images.

Scope of data processed and detailed purposes of data processing

- Public name of the data subject: identification, communication
- Public e-mail address of the data subject (available for certain pages): contact
- Message sent by the person concerned: the element related to the implementation of the communication
- The result of an action by the data subject (e.g. evaluation, response, etc.)

Legal basis for processing

The use of the social networking sites operated by the Data Controller and the contacting, communication and other operations permitted by the social networking site are based on voluntary consent.

In each case, the Data Subjects give their consent to the processing of their data on the relevant social networking site, where they can unsubscribe and where they can delete, modify or contact the various messages, signals and activities.

The operators of social networking sites are independent data controllers, separate from the Data Controller. Therefore, any data processing activities on those platforms are governed by the respective social networking site's own privacy policy, which is not controlled by the Data Controller.

Who is affected

Natural persons who voluntarily follow, share or like the social networking sites used by the Data Controller or the content displayed on them.

Duration of processing

Until you unsubscribe from the social networking site concerned or disconnect from the social networking site.

4.14. Processing of data related to camera surveillance

The Data Controller operates an electronic monitoring and recording system in areas marked with a camera pictogram or a warning notice (monitored areas). The camera system monitors only the common areas of the hotel. The camera surveillance system records the images and actions of persons entering the monitored area. The camera surveillance system does not record sound.

The current Accent Hotels Hotel chain camera policy is available on the Accent Hotels Hotel chain website - https://accenthotels.com/hu/adatvedelem, can be requested at the reception desk or in writing by sending a request to info@monasteryhotel.hu.

Purpose of data processing

The Controller processes the images recorded by the cameras for the following purposes:

- protection of property, assets and valuables, movable property of significant value;
- protecting the life and physical safety of persons, recording and investigating the circumstances of accidents;
- prevent, disrupt, clarify, prove and document violations;
- to improve the services of the Data Controller, to improve its operation;
- dealing with customer complaints, handling and investigating related cases;
- support the implementation of pandemic measures.

Scope of the data processed and detailed purposes of the processing

- the image and behaviour of employees
- the image and behaviour of contractual (business) partners
- the image and behaviour of visitors

Legal basis for processing

The legal basis for processing is the legitimate interest of the Controller (Article 6(1)(f) GDPR).

Detailed justification of the legitimate interest

Data processing is justified by the legitimate interest of the protection of the data subjects (employees, guests) staying in the hotel premises and the protection of the Hotel and the property of the guests. Prior to the introduction of the camera system, the Data Controller carried out an interest balancing test to assess the legal basis, which is available on the Accent Hotels website.

Duration of processing

The Data Controller keeps the data for 3 days. Access to the camera recordings is limited to security or legal staff designated by the Data Controller.

Camera recordings are automatically deleted after 72 hours (i.e. 3 calendar days), unless it becomes evident within this period that the footage is required to protect the legitimate interests of the Data Controller or a third party — for example, in the event of an incident involving the safety of persons or property. In such cases, the relevant recordings are securely backed up and may be transferred to the entitled authority or person. Once deleted, recordings cannot be recovered.

Rules for Viewing and Releasing Surveillance Footage

Only persons designated by the Data Controller are authorized to access surveillance footage, in line with the scope of their authorization. All instances of viewing, locking, or releasing footage are recorded in writing, and a protocol is created that includes the date, time, reason, cameras involved, and names of those present. These protocols are retained by the Data Controller for five years.

If footage is needed as evidence in connection with an incident, complaint, or legal proceedings, the Data Controller will lock the relevant footage and retain it for up to 90 days, or until the conclusion of the legal process.

Footage may only be released on the basis of a lawful, documented request (e.g. by an authority, a data subject, or a legal representative). The Data Controller keeps a record of every disclosure.

Location of cameras

	Camera location	Area covered by the camera	People in the monitored space
1	Hotel Reception	Hotel reception, lobby	employees, guests, suppliers
2	Although	Although foreground	employees, guests, suppliers
3	Rear entrance	rear courtyard entrance lobby	employees, guests, suppliers
4	2nd floor	2nd floor lift lobby	employees, guests, suppliers
5	Luggage storage	Square in front of the luggage storage	employees, guests

4.15. Data management of found objects

Items found on hotel premises must be handed in at the reception, where a record is kept of all items received. Accessing or opening personal devices (e.g. mobile phones, USB drives) is strictly prohibited.

The hotel may attempt to identify the owner in justified cases, such as when an incoming call is received, but personal content will not be accessed or processed. Upon claiming the item, the owner must complete a form providing the necessary details. If the item is returned by post, the hotel also keeps a record of relevant email correspondence and postal delivery information (date, name of the service provider).

Purpose of data processing

To ensure proper handling of lost and found items, notification of the rightful owner, and compliance with legal obligations.

Scope of the data processed and detailed purposes of the processing

- Data related to finding:
    - the date of finding,
    - place where the object was found,
    - name and contact details of the finder,
- Name and other details of the object found,
- The fact of whether the owner has been reached,
- The exact location of storage.
- In case of transfer:
    - the signature of the recipient,
- In case of postal delivery:
    - the date of dispatch,
    - an indication of the postal service provider.

Legal basis for processing

The processing is necessary to fulfill a legal obligation (Article 6(1)(c) GDPR), in accordance with the Hungarian Civil Code (Act V of 2013, Sections 5:54, 5:55, 5:59, and 5:61). The retention of related records and declarations is based on the hotel's legitimate interest (Article 6(1)(f) GDPR), supported by a balancing test available upon request at the reception or electronically.

Duration of processing

Lost items are kept for a maximum of one year. If unclaimed, they are either destroyed or handed over to the local notary, documented in an official report. All related documentation is retained for five years to allow for accountability in case of later claims or disputes. Guests may object to this processing, which the hotel will evaluate individually.

4.16. Managing requests for tenders

Monastery Boutique Hotel will prepare individual offers for its business partners and transmit information related to the requests for offers.

Scope of data processed and detailed purposes of data processing

- Personal details of the contact person:
    - full name: identification, contact
    - e-mail address: identification, contact
    - telephone number (if provided by the Data Subject): for the purposes of communication between the Data Controller and the Data Subject
- Other personal data collected in the course of the consultation relating to the request for proposal

Legal basis for processing

The personal data provided in the course of the requests for proposals are processed by the Data Controller on the basis of legitimate interest (Article 6(1)(f) GDPR), as the Data Subject has expressed an interest in the services of the Data Controller by submitting a request for proposal. The processing is necessary for the preparation, transmission and further communication of the offer. The purpose of the processing is to maintain business contacts and to follow up offers.

Designation of legitimate interest

The Data Controller has a legitimate interest in ensuring that potential customers are aware of the offers and have the opportunity to be properly informed about the services. The processing of requests for quotations is necessary for the operation of the business, as it is initiated by customers and it is to the benefit of Data Subjects to receive adequate information to make decisions. The processing is minimal and proportionate and the Data Subjects' right to object is fully ensured by the Data Controller.

Duration of processing

If the request does not lead to a contract, the personal data related to the business processes will be stored by the Data Controller for a maximum of 3 years, after which it will be deleted.

If a contract is concluded, the related data will be processed in accordance with the legal retention obligations related to the performance of the contract (e.g., under Section 6:22 of the Civil Code, until the expiry of the statute of limitations, i.e., 5 years).

4.17. Issuing a financial document, invoice

Purpose of data processing

The Data Controller processes these data for the purpose of issuing documents and invoices related to the Data Subject (subcontractor or their appointed representative).

Legal basis for processing

The processing is necessary for compliance with a legal obligation to which the Data Controller is subject (Article 6(1)(c) GDPR). Pursuant to Article 159(1) of Act CXXVII of 2007 on Value Added Tax, invoices are mandatory and must be kept for 8 years, in accordance with Article 169(2) of Act C of 2000 on Accounting.

Categories of personal data

Data directly required for invoicing.

- Full name of data subject: identification, contact, verification
- Address of data subject: identification, contact
- Tax number: identification

Duration of data storage

The Data Controller shall process the data for the period necessary to fulfill the obligation to keep supporting documents as required by Section 169 of Act C of 2000 on Accounting (the "Accounting Act"), i.e., for at least 8 years from the date of issue of the supporting document. After this period, the Data Controller shall delete the data within one year.

4.18. Use of other hotel services

The Data Controller provides various services to its guests, in some cases personal data is processed in connection with the use of the service.

Purpose of data processing

The purpose of the Data Controller is to provide the services offered by the hotel to the Data Subjects, to administer the provision of the service, to provide payment facilities and to maintain contact, for which the processing of personal data is necessary.

Scope of the data processed and detailed purposes of the processing

- For some services (e.g. wellness service, spa visit, greeting card, shuttle service, bicycle rental) the following data set is used:
  - e-mail address: required for contact
  - telephone number: required for contact
  - full address: required for the performance of the contract
  - billing address: required for contract performance
  - method of payment: required to fulfil the contract
  - ID card number, passport number: required for identification, contract performance
- Other data processed in connection with table reservations
  - Date of reservation of the table: execution of the contract
  - Planned number of guests: contract implementation

Legal basis for processing

The legal basis for processing is the performance of a contract (Article 6(1)(b) GDPR).

Duration of data storage

After the termination of the relationship with the Data Subject, the data shall be processed in accordance with the provisions of Section 6:22 of the Civil Code. The data will be deleted after 5 years. If we are obligated to retain the data pursuant to Section 169 of Act C of 2000 on Accounting ("Accounting Act"), we will delete the data 8 years after the termination of the relationship with the Data Subject. In practice, this applies when the data forms part of the supporting accounting documents, such as those relating to the conclusion of the contract (the contract itself, where applicable) or the issued invoice.

Processing of Health Data Related to Certain Services

When using certain services—especially dining (e.g. food allergies), wellness, or massage—guests may voluntarily provide health-related data. This information is processed solely based on the explicit consent of the data subject and is used to provide the service safely, protect the guest's health, and support both parties in case of a complaint or damage claim.

The Data Controller retains this data for a maximum of 15 days after the service is provided, unless legal proceedings or a complaint require extended storage. A separate consent form details the processing conditions, retention period, and data subject rights. Consent may be withdrawn at any time without justification.

Legal basis: The processing is based on the data subject's consent (Article 6(1)(a) and Article 9(2)(a) GDPR) and the hotel's legitimate interest in ensuring legal protection (Article 6(1)(f) GDPR), as documented in a balancing test available at the reception or electronically upon request.

4.19. Data management in relation to gift vouchers

The Data Subject (or, in the case of a legal person, his/her personal representative) has the possibility to purchase vouchers both on the website and in person at each hotel.
A tripartite agreement is established between the Customer, the Beneficiary, and the Data Controller.

Purpose of data processing

The processing of personal data is necessary for the sale and delivery of gift vouchers to the Customer and to ensure the redemption of the voucher.

Scope of the data processed and detailed purposes of the processing

- Personal data of the Data Subject who purchased the gift voucher:
  - Surname, first name: necessary for identification, communication, performance of the contract for the issue of the gift voucher
  - Name of contact person (in case of purchase by a legal person): identification, communication, performance of contract
  - Postal/billing address: required for delivery and invoicing
  - E-mail: required for electronic delivery
- Gift Voucher/Voucher details:
  - Voucher number: required to fulfil a contract for the issue of a gift voucher
  - Beneficiary name: contract performance

- Details of the service included: performance of contract
- Value of service: contract performance

Legal basis for processing

The legal basis for processing the data required for the purchase and delivery of gift vouchers is the performance of a contract (Article 6(1)(b) GDPR). The storage of billing and accounting data related to gift vouchers is based on the Accounting Act and legal obligations (Article 6(1)(c) GDPR).

Duration of data storage

Contractual data related to the gift voucher will be stored by the Data Controller for 5 years after the termination of the relationship with the Data Subject, at which point the data will be deleted. Accounting data (e.g., invoices, accounting documents) will be kept for 8 years in accordance with Section 169 of the Accounting Act. Data containing the name of the Beneficiary will be deleted after the expiration of the voucher's validity period.

5. DATA PROCESSING, DATA TRANSMISSION

5.1. Data processing

The Data Controller uses the data processors listed in the table below to perform the technical tasks related to the data processing operations. The rights and obligations of the data processor in relation to the processing of personal data shall be determined by the Data Controller within the framework of the GDPR and the specific laws applicable to data processing. The Controller is responsible for the lawfulness of the instructions given by it. The processor shall not take any substantive decision regarding the processing, shall process personal data of which it becomes aware only in accordance with the Controller's instructions, shall not process personal data for its own purposes and shall store and retain personal data in accordance with the Controller's instructions.

Data Processor Info	The activity performed in the processing of data
Accent Hotel Management Kft. Address: Visegrádi utca 31, 1. emelet, 1132 Budapest, Hungary Phone: +36 1 780 4593 Email: info@accenthotels.com Privacy Policy: https://accenthotels.com/hu/adatvedelem	Provides accounting and payroll services, with access to business-related transactions, supporting documents, agreements, and associated personal data.
Mews Systems B.V Wibautstraat 137D, Scalehub 2nd floor, 1097DN Amsterdam E-mail: privacy@mews.com Adatkezelési tájékoztatója: https://app.mews.com/Platform/Document/Pr	Has access to personal data required for room reservations, invoicing, accounting, order processing, and related documentation. Processes personal data provided directly by the Data Subject.

ivacyPolicy?language=en-GB	
REVOLUTION Software Kereskedelmi Kft. Address: Váci út 76., V. torony, VII. emelet, 1133 Budapest, Hungary Phone: +36 1 461 8090 / +36 1 461 8030 Email: websales@revolution.hu Privacy policy: https://www.revolution.hu/adat	As the operator of the accounting software, has access to transaction records, supporting vouchers, agreements, and the personal data involved.
Magyar Posta Zrt. Address: Dunavirág u. 2-6, 1138 Budapest, Hungary Phone: +36 1 767 8282 Email: ugyfelszolgalat@posta.hu Privacy Policy: posta.hu/adatkezelesi_tajekoztato	Handles postal mail and parcel deliveries for Monastery Boutique Hotel, with access to the personal data necessary for delivery.
MOHU MOL Hulladékgazdálkodási Zrt. Address: Galvani utca 44, 1117 Budapest, Hungary Phone: +36 94 200 610 Email: ugyfelszolgalat@stkh.hu Privacy Policy: mohu.hu/media/dokumentumtar	Provides delivery and logistics services to Monastery Boutique Hotel, with access to the personal data necessary for the performance of delivery tasks (e.g. name, address, contact details).
Accent Hotel Solutions Kft. Address: Visegrádi utca 31, 1132 Budapest, Hungary Phone: +36 1 780 4593 Email: info@accenthotels.com Privacy Policy: accenthotels.com/hu/adatvedelem	Operates the customer relationship management (CRM) system, storing personal data of employees and business contacts.
One Magyarország Zrt. Address: 1112 Budapest, Boldizsár utca 2. Mailing: H-1519 Budapest, P.O. Box 543 Phone: 1270, +36 70 700 1270 (from abroad) Email: ugyfelszolgalat@one.hu Privacy policy: https://www.one.hu/adatvedelem	Provides telecommunications and internet services, with potential access to communication-related personal data and telephone usage details.
Assist Intelligence Kft. Registered address: Nyár utca 12. 1st floor, door 4., 2132 Göd, Hungary Tax number: 26306825-2-13 E-mail: info@assistintelligence.com	Provides services related to the operation of the Peak Plus Cloud Software, which supports occupancy monitoring, optimization, and reporting for the Hotel. In this context, it may access employee data and, to a limited extent, guest data.

CloudSoft Kft. Address: Ribizli utca 14., 2000 Szentendre, Hungary Phone: +36 1 700 2600 E-mail: kapcsolat@clsft.hu Privacy Policy: https://cloudsoft.ie/adatvedelmi-tajekoztato	Provides support related to the Hotel's internal IT systems, email services, office software, and cloud platforms. In this context, it may access the personal data and correspondence of employees and business partner contacts.
MiniCRM Zrt. Address: Madách Imre út 13-14., 1075 Budapest, Hungary E-mail: help@minicrm.hu Phone: +36 1 999 0402 Privacy Policy: https://www.minicrm.hu/adatvedelem	Operates the customer relationship management (CRM) system used by the Hotel. In this context, it may access the personal data of employees and the contact persons of business partners. The Data Controller stores personal data related to business processes.
SimplePay Zrt. Address: Váci út 135–139., Building B, 5th floor, 1138 Budapest, Hungary Tax number: 32835155-2-41 E-mail: ugyfelszolgalat@simple.hu Phone: +36 1 3-666-611 / +36 20 3-666-611 / +36 30 3-666-611 / +36 70 3-666-611 Privacy Contact: dpo@simplepay.com Privacy Notices: https://simplepay.hu/adatkezelesi-tajekoztatok	As the Hotel's online payment service provider, SimplePay acts as a data processor during the execution and processing of credit card transactions and related technical operations. By using the service, the following data may be transferred to the provider: the data subject's name, email address, transaction details, and technical information related to the payment (e.g. IP address, device identifier).
Opennetworks Kft. Cím: 1125 Budapest, Kiss Áron utca 9. Telefonszám: +36 1 999 6000 E-mail: info@opennet.hu Adatkezelési tájékoztatója: https://www.opennet.hu/wp-content/uploads/ON_ASZF_4.sz_melleklet_adatkezelesi_tajekoztato_20240607.pdf	Operates the call centre, with access to personal data during customer interactions.
Accent Hotel Solutions Kft. Address: Visegrádi utca 31, 1132 Budapest, Hungary Phone: +36 1 780 4593 Email: info@accenthotels.com Privacy Policy: accenthotels.com/hu/adatvedelem	Provides technical support for the newsletter system and has access to personal data included in newsletters sent by the Data Controller.
EOX Kft. Address: Francia út 57/A/1 , 1146 Budapest,	Ensures secure storage of data files managed by the Data Controller and may access all personal data processed

Hungary Phone: +36 1 783 2273 Email: info@eox.hu Privacy Policy: https://www.eox.hu	under this Privacy Notice.
Accent Hotel Solutions Kft. Address: Visegrádi utca 31, 1132 Budapest, Hungary Phone: +36 1 780 4593 Email: info@accenthotels.com Privacy Policy: accenthotels.com/hu/adatvedelem	Provides technical services for the hotel's website, supports online booking, loyalty programme integration, and Nice Card acceptance, with access to related personal data.
EOX Kft. Address: Francia út 57/A/1, 1146 Budapest HU Phone: +36 1 783 2273 Email: info@eox.hu Privacy Policy: https://www.eox.hu	Supports the operation of the hotel's email and office software systems, with access to personal data as part of service delivery.
Intren Informatikai Tanácsadó és Szolg. Kft. Address: Lajos utca 78, 3. emelet, 1036 Budapest, Hungary Phone: +36 1 201 5468 Email: office@intren.hu Privacy Policy: intren.hu/adatkezelesi-tajekoztato	Delivers online marketing services, with access to customer data as required for campaign implementation.
NEXUM Magyarország Kft. Address: Lehel u. 17/B/C, 1134 Budapest HUN Phone: +36 62 55 88 99, +36 1 288 8000 Email: info@nexum.hu Privacy: nexum.hu/adatkezelesi-tajekoztato	Participates in recruitment processes, with access to the personal data of applicants and hired employees.
Profession.hu Kft. Address: Nagyenyed utca 8–14, 4. emelet, 1123 Budapest, Hungary Phone: +36 1 224 2070 Email: ugyfelszolgalat@profession.hu Privacy Policy: profession.hu/gdpr	Participates in recruitment processes, with access to the personal data of applicants and hired employees.
OTP Bank Nyrt. Address: Nádor utca 16, 1051 Budapest HUN Phone: +36 1 366 6666 Email: informacio@otpbank.hu Privacy Policy: otpbank.hu/adatvedelemtatok	Provides account management and financial services for Monastery Boutique Hotel. In the case of bank transfers, it has access to personal data related to the transaction. The financial institution performs its activities and processes personal data in accordance with the applicable strict legal and regulatory requirements.

MORGENS Design Kft. Address: Magyar utca 79, 8800 Nagykanizsa Phone: +36 30 648 0047 Email: sales@morgens.hu Privacy Policy: morgens.hu/adatvedelem	As a partner of the Monastery Boutique Hotel, it acts as an intermediary for the reservation of accommodation and has access to the reservation data related to a successful booking.
Accent Hotel Solutions Kft. Address: Visegrádi utca 31, 1132 Budapest, Hungary Phone: +36 1 780 4593 Email: info@accenthotels.com Privacy: accenthotels.com/hu/adatvedelem	Acts as a booking intermediary for Monastery Boutique Hotel, with access to personal data related to confirmed reservations.
OTP Bank Nyrt. – Széchenyi Card Address: P.O. Box 564, 1243 Budapest, Hungary Phone: +36 1 3666 100 Email: info@otpszepkartya.hu Privacy Policy: kereskedo.szepkartya.otpportalok.hu/adatkezelesi-tajekoztato **MBH Bank Nyrt. – SZÉP Card** Address: Váci utca 38, 1056 Budapest, Hungary Phone: +36 1 268 7272 Email: szolgaltato.mbhszepkartya@mbhbank.hu Privacy: mbhbank.hu/MBH_SZEP_kartya.pdf **K&H Bank Zrt. – SZÉP Card** Address: Lechner Ödön Sétány 9, 1095 Budapest, Hungary Phone: +36 1/20/30/70 335 3355 (Press 7) Email: szepkartya@kh.hu Privacy Policy: kh.hu/adatvedelem	The Széchenyi Card acceptance partners provide the services to ensure the acceptance of the Széchenyi Cards, during which they have access to the Data Subjects' personal data. The financial institutions carry out their activities and process personal data in accordance with domestic legislation, in particular the strict regulations applicable to financial institutions.
Booking.com B.V. Address: Oosterdokskade 106, 1011 Amsterdam, Netherlands Email: dataprotectionoffice@booking.com Privacy notice: https://www.booking.com/content/privacy.hu.html **Other travel agencies and accommodation intermediaries**	Acts as a booking intermediary for Monastery Boutique Hotel, with access to personal data related to confirmed reservations.

C&S Cleanforte Kft. Address: 1108 Budapest, Sibrik Miklós utca 79/105. Phone: +36 20 393-0273 Email: gaborcarmen1@gmail.com	Provides cleaning services within the premises and may have incidental access to personal data during the performance of its duties
The Data Controller informs Data Subjects that, in connection with specific services, they will be individually notified about any additional data processors or joint controllers involved in the process (e.g. accommodation intermediaries).	

5.2. Data transmission

The Data Controller transfers data in connection with the services it provides to the entities listed in the table below:

List of Recipients of Data Transfers	**Description of the data transfer**
Hungarian Tourism Agency Ltd. (Magyar Turisztikai Ügynökség Zrt.) Kacsa Street 15–23, H-1027 Budapest, Hungary Mailing address: P.O. Box 97, H-1525 Budapest Phone: +36 1 488 8700 Email: info@mtu.gov.hu	The Data Controller transmits guests' personal data in the legally prescribed manner, by recording them in the VIZA system. The purpose of this data transfer is to protect the rights, safety, and property of the Data Subject and others, as well as to monitor compliance with the regulations regarding the stay of third-country nationals and persons entitled to free movement and residence.
NTAK (National Tourist Information Centre) **Hungarian Tourism Agency Ltd. (Magyar Turisztikai Ügynökség Zrt.)** Kacsa Street 15–23, H-1027 Budapest, Hungary Mailing address: P.O. Box 97, H-1525 Budapest Phone: +36 1 488 8700 Email: info@mtu.gov.hu	The NTAK system operated by the Hungarian Tourism Agency (MTÜ) collects and analyses data from accommodation management software in order to support data-driven decision-making in the tourism sector. Relevant data sets are also accessible to local authorities and the National Tax and Customs Administration (NAV).
Competent Authorities e.g. the National Tax and Customs Administration of Hungary (NAV), National Health Insurance Fund, OEP, local governments, law enforcement agencies, counter-terrorism units, national security services, the public prosecutor's office, and the courts	Personal data contained in the guest register, including records of entry and residence of third-country nationals, are forwarded to the competent authorities in accordance with the applicable legal provisions. Such data transfers occur in cases specified by law, including suspected or actual criminal offences or upon official request as part of a specific legal procedure. Each data transfer is documented in accordance with legal requirements.

6. DATA SECURITY MEASURES

The Data Controller shall act in accordance with the provisions of Regulation (EU) 2016/679 of the European Parliament and Council, and Act CXII of 2011 on the Right to Informational Self-Determination and Freedom of Information, in relation to the personal data provided by the Data Subject.

To ensure the security and lawful processing of personal data, the Data Controller implements all reasonable technical and organisational measures, including but not limited to the following:

- maintaining an adequate level of protection against unauthorised access, alteration, disclosure, transmission, deletion, destruction, accidental loss or damage;
- ensuring that data records are managed in compliance with applicable legal requirements;
- limiting access to personnel records strictly to employees or other individuals acting on behalf of the Data Controller who require such access to perform their duties;
- storing paper-based records securely, in compliance with data security standards;
- protecting IT systems against unauthorised access on both software and hardware levels;
- applying appropriate technical safeguards (e.g. password encryption, secure communication channels) and organisational measures (e.g. staff training, role-based access control);
- monitoring and logging data access and processing activities;
- ensuring the permanent deletion of data after the applicable retention period has expired;
- protecting IT equipment and servers against viruses and other malware;
- enforcing security protocols for remote work (e.g. safe use of IT devices at home);
- providing continuous physical protection of IT assets, including protection from environmental or physical damage.

Please help us protect your data by choosing a secure password, updating it regularly, and never sharing it with anyone else.

7. INFORMATION ABOUT CHILDREN

Personal data of Data Subjects under the age of 14 may only be provided by their legal representative or guardian, who is also entitled to make legal declarations on their behalf.

Data Subjects aged between 14 and 18 may only provide personal data or make legal declarations with the consent of their legal representative or guardian. The Data Controller is required by law to verify and, where necessary, transmit related documentation in accordance with applicable guest registration regulations. If such consent is not provided, the Data Controller is unable to deliver the requested service, as the related data processing would not be legally compliant.

By submitting personal data, you confirm that you are acting in compliance with the above requirements and that you have the legal capacity to provide such information. If you do not have this legal capacity, you must obtain the consent of a third party (e.g. a parent or legal guardian).

It is your responsibility to determine whether third-party consent is required. The Data Controller may have no direct contact with you and therefore cannot verify this independently; responsibility for compliance rests with you. The Data Controller shall not be held liable in this regard.

If we become aware that personal data has been provided without appropriate authorisation, we will make every reasonable effort to delete such data and ensure that it is not further used or disclosed.

If you believe that a child has provided personal data without the necessary consent, please contact us immediately using the contact details provided at the beginning of this Privacy Notice.

8. ANALYTICAL SERVICES

The Data Controller uses cookies and tracking technologies provided by third-party service providers (notably Google and Facebook) to collect information about user interests, demographic data, and behaviour on the website. This data is used for statistical analysis to improve the quality and effectiveness of the services provided. It is not used for profiling or automated decision-making.

The Data Controller may also use anonymised or aggregated data obtained from interest-based advertising services (e.g. age, gender, interests) to generate reports, statistics, and advertising or marketing lists.

These activities are intended to continuously improve the Data Controller’s online platforms and to increase the effectiveness of advertising campaigns.

8.1. Google Analytics

Accent Hotels uses Google Analytics (both Universal Analytics and Google Analytics 4) on its websites to monitor user activity. The data is processed by Google LLC (1600 Amphitheatre Parkway, Mountain View, CA 94043, USA). Google ensures compliance with the GDPR and commits to protecting data subject rights.

Google Analytics uses cookies—text files stored on the visitor's device—to analyse website usage. These are considered third-party cookies in the relationship between the Data Controller and the Visitor. Google Analytics is implemented with IP anonymisation enabled, meaning that IP addresses of users from EU or EEA countries are truncated before being transmitted to Google's servers. In exceptional cases, the full IP address may be sent to the USA and anonymised there. Google does not associate the truncated IP address with other data.

The Data Controller uses Google Analytics for statistical analysis to improve services. The resulting usage profiles do not identify individual users. Processing is governed by Google's Shared Responsibility Agreement.

The Data Controller has also enabled data-sharing settings for “Google products and services,” allowing Analytics features like advertising reports, remarketing, cross-device reports, and demographic statistics. This data may be used by Google to enhance its services, based on a separate agreement between the parties.

The Data Controller has no insight into or control over any additional processing carried out by Google.

8.2. Google Signals

Google Signals, part of Google Analytics (Consent Mode 2), enables cross-device tracking. If the visitor has signed into a Google account and enabled personalised ads, Google may generate cross-device activity reports. For example, Google may detect if a user views a product on a smartphone but completes the purchase later on a laptop. This feature allows for cross-device remarketing, enabling the delivery of targeted ads across multiple devices. The collected data is anonymised and used in aggregate for statistical purposes only, in compliance with the GDPR and the California Consumer Privacy Act (CCPA).

No personal data is shared with the Data Controller. Users may manage or delete this data via their Google Account.

Scope of data processed:

- IP address
- Date and time of visit
- Device and browser information
- Website usage data

Legal basis: The use of Google Signals is based on the consent of the Data Subject (Article 6(1)(a) GDPR). Consent is requested upon first visit to the website via the cookie banner.

Retention periods:

- Cookie data: 2 months
- Google Analytics data: 4 months
- Universal Analytics data: 14 months

(Data is deleted cyclically, once per month.)

8.3. Google Ads conversion tracking / remarketing

With the Data Subject's consent, the Data Controller may use Google Ads conversion tracking and remarketing tools to measure and improve the performance of online advertisements. Google uses cookies (valid for 30 days) to track ad interactions. These cookies do not allow identification of individuals but enable Google to associate interactions with specific browsers or devices.

The Data Controller does not collect or process any personal data during this process but may access aggregated reports for advertising optimization. Google's remarketing feature allows relevant ads to be shown across Google's advertising network (e.g. Google Search, YouTube) based on prior visits to the website.

Visitors can disable tracking in various ways:

- Via browser settings (disable third-party cookies)
- Using Google's opt-out plugin: https://www.google.com/settings/ads/plugin
- Via About Ads campaign settings: https://www.aboutads.info/choices
- By disabling interest-based ads in browser extensions (Chrome, Firefox, etc.)

More info on Google's privacy practices: https://policies.google.com/privacy, https://services.google.com/sitestats

Google participates in the EU–US Data Privacy Framework: https://www.dataprivacyframework.gov

8.4. Google Tag Manager

The website uses Google Tag Manager, which allows easy management of website tags through a unified interface. Google Tag Manager does not use cookies and does not collect personal data itself.

It may, however, load other tracking tags that process personal data under their own responsibility. Google Tag Manager does not access this data. If data collection is disabled at the cookie or domain level, this restriction applies to all tags managed via Google Tag Manager.

8.5. Cookie management

A cookie is a small text file consisting of letters and numbers that is sent by a web server to the visitor's browser upon first visit to https://monasterybudapest.accenthotels.com/hu. The cookie is stored on the visitor's device for a period defined by the entity that placed it.

On subsequent visits, the browser returns the cookie to the server, allowing the system to recognise the device and recall certain information about the user's previous interactions with the website. A web beacon is a tiny, typically invisible image placed on a website that enables user activity to be tracked and contributes to the generation of anonymous statistics.

The Data Controller uses cookies and web beacons for the following purposes:

- to recognise returning visitors,
- to understand visitor interests and behaviour,
- to improve user experience,
- to display personalised advertisements,

- and to enhance website security.

In accordance with Act C of 2003 on Electronic Communications, the use of cookies requires the visitor's prior and informed consent. Upon first visit, the website displays a cookie consent banner with a link to this policy. Visitors may choose to:

- accept all cookies,
- allow only essential cookies necessary for the site's operation, or
- customise their cookie preferences.

It is important to note that cookies do not personally identify users and are deleted according to the browser's settings after the session ends.

In some cases, anonymised data may still be transmitted to Google's systems even if consent is not given; however, such data is processed without pseudo-identifiers and is stored separately, used solely for statistical modelling purposes.

Types of Cookies Used

Essential Cookies
These are necessary for the proper functioning of the website and cannot be disabled. They support basic functions such as secure login, load balancing, and resource delivery.

Preference Cookies
These remember user settings such as language preferences or regional display options.

Statistical Cookies
These cookies collect anonymised data to help the website owner understand how visitors interact with the site.

Marketing Cookies (Targeting Cookies)
Set by advertising partners, these cookies track browsing behaviour and enable personalised, interest-based advertising across websites.

Managing Cookies

For more information on cookies and how to manage or delete them, please visit https://www.allaboutcookies.org. Instructions for deleting cookies on mobile devices can be found in your device's user guide or browser documentation.

8.6. Facebook remarketing

The Data Controller uses Facebook's remarketing service to display targeted ads on the Facebook platform. Visitors can opt out of this feature by adjusting their Facebook ad settings to disable interest-based ads.

The Data Controller does not have access to personal data collected by Facebook.

8.7. Facebook pixels (Facebook pixel)

The website uses Facebook Pixel, a tool that allows Facebook to collect or receive data from the website via cookies, tracking signals, or similar technologies. This data is used for analytics and the delivery of targeted advertisements on Facebook platforms.

Users can disable this feature via their Facebook account settings. The Data Controller does not have access to detailed data collected through Facebook Pixel, including personal data.

9. RIGHTS OF THE DATA SUBJECT IN RELATION TO DATA PROCESSING

The rights of the Data Subject and the related remedies are set out in detail in the General Data Protection Regulation (GDPR), particularly in Articles 15–22 and Articles 77–82. The most important rights are summarised below.

Right of Access

The Data Subject has the right to obtain confirmation as to whether or not personal data concerning them are being processed, and, if so, access to the personal data and the following information:

a) the purposes of the processing;

b) the categories of personal data concerned;

c) the recipients or categories of recipients to whom personal data have been or will be disclosed, in particular recipients in third countries or international organisations;

d) the envisaged period for which the personal data will be stored, or the criteria used to determine that period;

e) the existence of the right to request rectification, erasure or restriction of processing, or to object to such processing;

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

g) where the data were not collected directly from the Data Subject, any available information about the source;

h) the existence of automated decision-making, including profiling, and meaningful information about the logic involved, as well as the significance and potential consequences of such processing.

If personal data are transferred to a third country, the Data Subject has the right to be informed of the appropriate safeguards in place.

The Data Subject may request a copy of the personal data processed. If the request is made electronically, the information will be provided in a commonly used electronic format, unless otherwise requested.

Right to Rectification

The Data Subject has the right to obtain without undue delay the rectification of inaccurate personal data. They also have the right to have incomplete personal data completed, including by providing a supplementary statement.

Right to erasure ("right to be forgotten")

The Data Subject has the right to request the erasure of their personal data without undue delay where one of the following applies:

- the data are no longer necessary for the purposes for which they were collected;
- the Data Subject withdraws consent and there is no other legal basis for processing;
- the Data Subject objects to processing and there are no overriding legitimate grounds;
- the data have been unlawfully processed;
- erasure is required to comply with a legal obligation under Union or Member State law;
- the data were collected in relation to information society services offered to children.

If the Controller has made the data public, it will take reasonable steps, including technical measures, to inform other controllers processing the data of the Data Subject's erasure request.

This right does not apply where processing is necessary:

- for exercising the right to freedom of expression and information;
- to comply with a legal obligation;
- for archiving in the public interest, scientific or historical research or statistical purposes;
- for the establishment, exercise, or defence of legal claims.

Right to Restriction of Processing

The Data Subject has the right to request restriction of processing if:

- the accuracy of the personal data is contested, for a period enabling verification;
- the processing is unlawful but the Data Subject opposes erasure;
- the Controller no longer needs the data, but the Data Subject requires them for legal claims;
- the Data Subject has objected to processing, pending verification of overriding legitimate grounds.

Where processing is restricted, such data may only be processed (except for storage) with the Data Subject's consent, or for legal claims, or to protect the rights of another person, or for important public interest.
The Data Subject will be informed before any restriction is lifted.

Obligation to Notify

The Controller shall inform all recipients to whom personal data have been disclosed of any rectification, erasure or restriction of processing, unless this proves impossible or involves disproportionate effort. Upon request, the Controller will inform the Data Subject of these recipients.

The right to data portability

The Data Subject has the right to receive personal data provided to the Controller in a structured, commonly used, machine-readable format and to transmit those data to another controller, where:

- the processing is based on consent or contract, and
- the processing is carried out by automated means.

The Data Subject also has the right to request direct transmission of the data from one controller to another, where technically feasible.

Right to Object

The Data Subject has the right to object, on grounds relating to their particular situation, to the processing of personal data based on legitimate interest, including profiling. In such cases, the Controller will no longer process the data unless compelling legitimate grounds can be demonstrated.

Where data are processed for direct marketing, the Data Subject may object at any time. In this case, the personal data may no longer be used for such purposes.

This right can be exercised using automated means where applicable (e.g. through browser settings).

For scientific or historical research or statistical purposes, the right to object applies unless the processing is necessary for public interest tasks.

Right to Lodge a Complaint

The Data Subject may enforce their rights before the court under the GDPR and the Civil Code. Additionally, the Data Subject may turn to the National Authority for Data Protection and Freedom of Information (NAIH) (Falk Miksa Street 9-11, 1055 Budapest; mailing address: 1363 Budapest, P.O. Box: 9; phone: +36 1 391 1400; email: ugyfelszolgalat@naih.hu) in case of a complaint regarding the data controller's data processing practices. Detailed rights and remedies related to data processing are provided in Articles 77, 79, and 82 of the GDPR.

Right to an Effective Judicial Remedy

The Data Subject has the right to an effective judicial remedy:

- against a legally binding decision of a supervisory authority;
- if the authority fails to act on a complaint within 3 months.

Proceedings must be brought before the courts of the Member State where the supervisory authority or controller is established, or where the Data Subject resides.

It is recommended that any issues be addressed first by contacting the Controller directly.

10. COMPLAINTS HANDLING

10.1. Oral complaint

Complaints received in person or by telephone must be investigated immediately. A record shall be made, and appropriate action must be taken.

The record shall contain the following:

- name and address of the customer,
- method and time of receipt of the complaint,
- description of the complaint,
- list of any supporting documents provided,
- the Data Controller's position on the complaint (if an immediate response is possible),
- customer's signature,
- place and date of the record,
- in case of a telephone complaint, a reference or case number.

If the customer disagrees with how the complaint is handled, the Data Controller shall document the complaint, the steps taken, and its position, and shall provide a copy to the customer. From this point onward, the complaint will be handled as a written complaint under the same rules.

10.2. Written complaint

Written complaints must be handled in accordance with applicable legal requirements. The Data Controller shall maintain a record similar in content to that of an oral complaint. Unless otherwise required by directly applicable EU legislation, the Data Controller shall respond to the written complaint in writing within 30 days of receipt and take appropriate action to communicate the outcome.

The head of the organisation or a designated staff member may meet with the complainant (or whistleblower) or consult external experts if the complaint requires further investigation.

The Data Controller shall act without undue delay, either initiating an investigation or rejecting the complaint in accordance with legal requirements. A written decision shall be sent to the complainant, providing clear reasoning and addressing all relevant concerns. If the complaint is rejected, the Data Controller shall inform the complainant in writing about the competent authority or conciliation body to which the complaint may be submitted, depending on the nature of the issue.

Records of the complaint and the Data Controller's response shall be kept for five years and made available to supervisory authorities upon request.

11. LEGAL REMEDIES

If you have any questions or concerns, please do not hesitate to contact us. You may submit your request by post at Monastery Boutique Hotel, 1011 Budapest, Fő utca 30. or electronically at info@monasteryhotel.hu, and we will do our best to respond promptly and fulfil your request as soon as possible.

If you remain dissatisfied, or if you believe that your rights regarding the processing of your personal data have been violated, you may bring the matter before the competent court — in Budapest, the Metropolitan Court — or initiate an investigation with the National Authority for Data Protection and Freedom of Information.

National Authority for Data Protection and Freedom of Information (NAIH)
President: Dr. Attila Péterfalvi
Address: Hungary, 1055 Budapest, Falk Miksa Street 9-11.
Postal address: 1363 Budapest, PO Box 9.
Phone number: +36 (1) 391-1400
Central e-mail address: ugyfelszolgalat@naih.hu

Budapest, 5 November 2025

Monastery Boutique Hotel
KAPU VÁRALJA ÜZEMELTETŐ Kft.