PRIVACY NOTICE

Effective date of this Notice: 25 May 2018 Updated: 15.05.2024

Accent Hotels lays particular emphasis on personal data protection. Accordingly we wish to inform you about our data management and processing procedures involved in the provision of our services, our on-line booking system and our newsletter. Please see below what we do to protect your data and what data we record and process, and for what purposes.

1. INTRODUCTION:

Ambra Hotel Kft. (registered office: 1077 Budapest, Kisdiófa u. 13.; company registration number: 01-09-869558; tax number: 13716475-2-42) (hereinafter referred to as **"Controller"**), as the operator of **Ambra Hotel**, as Controller, acknowledges the contents of this Privacy Notice as binding upon itself in the course of the services it provides.

The personal data of guests, contracted partners, personal contributors, job applicants and employees who use the services of the Controller (hereinafter referred to as "**Data Subject**") shall be processed by the Controller. The Controller commits to ensure that the processing of data in relation to its services complies with the applicable legal regulations and the requirements of this Privacy Notice.

The Controller reserves the right to unilaterally amend this Notice. In this regard, those concerned should regularly visit https://accenthotels.com/hu/adatvedelem in order to monitor changes. The prevailing content of the Notice is available at and can be can be downloaded from the above site at any time. We will notify Data Subjects of changes by email upon their request in case we have their e-mail addresses.

We will send Data Subjects a copy of the current version of the Notice upon 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:

- Hungary's Fundamental Law (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 of Informational Self-Determination and on Freedom of Information – ("Info Act");
- Act V of 2013 on the Civil Code
- Act CLV of 1997 on Consumer Protection

1.1. The Controller's data

Ambra Hotel****

Registered office: 1075 Budapest, Kisdiófa u. 13.

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

E-mail: sales@hotelambra.hu

Mailing address: 1077 Budapest, Kisdiófa u. 13.

Telephone: +36 1 321 15 33

Website: www.hotelambra.hu

2. BASIC DEFINITIONS OF DATA PROTECTION

2.1. Personal data:

Any data that can be associated with a specific (identified or identifiable) natural person and any conclusion that can be drawn from the data concerning the data subject. Personal data continue to retain this quality during processing as long as its relationship with the data subject can be re-established. A person may, in particular, be considered identifiable if he or she can be identified, directly or indirectly, by name, an identification mark or one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity;

2.2. Consent:

Voluntary and explicit indication of the data subject's well-informed intent, whereby he or she gives his or her unambiguous consent to the processing of their personal data, either in general or in relation to specific operations;

2.3. Objection:

A statement by the data subject objecting to the processing of their personal data and requesting the discontinuation of processing or the erasure of the processed data;

2.4. Controller:

The natural or legal person or organisation without legal personality who or which determines the purposes of the processing of personal data, makes 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. Processing:

Regardless of the process used, any operation or set of operations performed on personal data, such as collection, recording, survey, organisation, storage, alteration, use, transmission, disclosure, alignment or combination, blocking, erasure and destruction, as well as the prevention of further use of the data. Processing also includes taking photographs, making 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 specific third party;

2.7. Disclosure:

If the data is made accessible for anyone;

2.8. Data erasure:

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

2.9. Blocking of data:

Making it impossible to transmit, access, disclose, transform, alter, destroy, erase, combine or align and use the data permanently or for a specified period;

2.10. Data destruction:

Complete physical destruction of the data or the medium containing the data;

2.11. Data processing:

Carrying out technical tasks related to data processing operations, regardless of the method and means used to carry out the operations and the place of application;

2.12. Processor:

The natural or legal person or organisation without legal personality who or which carries out the processing of personal data on behalf of the controller, including on the basis of a legal mandate;

2.13. Third person:

A natural or legal person or organisation without legal personality, other than the data subject, the controller or the processor;

2.14. EEA country:

A Member State of the European Union and another State that is 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 that is 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 that is not party to the Agreement on the European Economic Area;

2.15. Third country:

Any state that is not a member of the EEA.

3. DATA PROTECTION PRINCIPLES

Personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');
b) 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, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');
c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');
e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');
f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

The controller is responsible for compliance with the above and must be able to demonstrate such compliance ('accountability').

4. DETAILED RULES ON DATA PROCESSING

The following shall have access to data:

- employees of the Controller;
- employees of the Processors identified below;
- certain public authorities in relation to data requested by them in the course of official proceedings and which the Controller is legally obliged to provide;
- employees of a debt management company appointed by the Controller to manage overdue debts;
- other persons with the express consent of the Data Subject.

The Controller undertakes to maintain strict confidentiality of the personal data it processes, without limitation in time, and shall not disclose them to third parties, except with the consent of the Data Subject.
The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.

4.1. Processing of data related to registration for room reservation and the further use of the data provided upon registration:

The Data Subject must fill in a registration form in order to use the services of the Controller. When using certain services, the data processed will be used for other purposes.

In the case of online booking, some of the data are transferred to the Controller by the individual accommodation intermediaries, travel agencies and ACCENT HOTEL SOLUTIONS Szolgáltató Kft.

Scope of the data processed and the specific purposes of processing:

- Last name: for identification, communication, contract performance
- First name: for identification, communication, contract performance
  Services where this data is further used: e.g. wellness service, spa visit, greeting card, shuttle service, bike rental

- Nationality: for identification, contract performance
- ID card number or passport number: for identification, contract performance
  Services where this data set is further used: e.g. bicycle rental

- E-mail address: for communication
- Phone number: for communication
- Full address: for contract performance
- Invoicing address: for contract performance
  Services where this data can be further used: Provision of various hotel services at the request of the Data Subject

- Method of payment: to fulfil the contract
- Special dietary preference: to meet the tastes of the Data Subject, contract performance
- Vehicle plate number: for the performance of the contract
- Purpose of trip: for the performance of the contract
  Additionally, for guests from outside the European Union:

- Passport number: to fulfil legal obligations
- Visa number: to fulfil legal obligations
- Date and place of entry: to fulfil legal obligations

Legal basis for processing

The legal basis for the processing is the performance of a contract (Article 6(1)(b) GDPR), where the law requires the processing and transmission of data (to a local authority, police), the fulfilment of a legal obligation (Article 6(1)(f) GDPR).

Duration of processing

The data shall be rendered anonymous 5 years after the termination of the relationship with the Data Subject as specified in Section 6:22 of the Civil Code. We will retain the data for longer than this if required by law, for example if we are required to retain the data under Section 169 of Act C of 2000 on Accounting ("Accounting Act"), we will erase the data after 8 years following the termination of the relationship with the Data Subject. This is the case in practice if the data are part of documents underlying the accounts, for example in documents relating to the conclusion of the contract (in the contract itself, where applicable) or the invoice issued, or for 6 years in the case of a police report.

4.2. Compulsory recording and reporting relating to the check-in of users of the accommodation service

At the time of check-in at the accommodation, the Controller shall record the required data in the multiple asymmetric encryption protected IT system called VIZA, i.e. the system operated by the hosting provider designated by the relevant Government Decree. The purpose of the recording of the data is to protect the rights, safety and property of the Data Subject and others, and to monitor compliance with the provisions on the residence of third-country nationals and persons enjoying the right of free movement and residence. The primary purpose of the VIZA system is therefore to promote public order, public security, the order of the state border and the protection of the rights, safety and property of the data subject and others.

Purpose of processing

Personal data need to be processed in order to support the objectives set by the Government and to implement the legal obligation.

Scope of data processed

The following data of the Data Subject using the accommodation service:

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

The following data of the Data Subject using the accommodation service:

- the identification details of their identity document and/or travel document,
- a scanned image of their identity document
- for third-country nationals, visa or residence permit number,

- the date and place of entry,

Information related to accommodation services:

- the exact address of the accommodation,
- the start and expected and actual end dates of use of the accommodation.

Legal basis for processing

The legal basis for processing is compliance with a legal obligation (Article 6 (1) (c) GDPR). The process of data provision is prescribed and regulated by Act CLVI of 2016 on the State's Responsibilities Regarding the Development of Tourism Regions.

Duration of processing

Data processed for the purpose of data provision must be stored until the last day of the first year following the year in which they came to the knowledge of the controller. The controller will then delete the personal data in the register. The VIZA system will retain the data submitted to the system for up to two years.

Data transmission

The hosting service provider's activity, as processor of the accommodation provider, is limited to storing the data in encrypted form on the hosting service by a provider of encryption procedures designated by Government Decree and providing access to the data for the accommodation provider and persons or bodies authorised by law to do so through the accommodation provider. The recorded guest data are encrypted in the VIZA system and may only be accessed by the competent authorities; the hosting provider and the operator of the document scanning software that enables the upload cannot access the data stored in the hosting location.

4.3. Data processed during admission, check-in

Managing risks related to the admission and check-in of guests, visitors, customers, partners, employees and taking measures proportionate and necessary to those and, where justified, limiting their admission, is in the interest of the Controller. The Controller may use a variety of solutions to ensure secure visits, in accordance with applicable government regulations and based on an assessment of current risks.

Purpose of Processing

In the case of pandemic control measures: to identify the risks related to the health status of guests and visitors entering the premises, and to certify compliance with the legal requirements.

Scope of data processed

The personal data of a Data Subject guest, visitor, customer or partner are:

- the data contained in the document certifying proper health condition
- the data in the vaccination certificate
- the personal data in the identification document (e.g. identity card, driving licence, passport) required for accepting the vaccination certificate

Personal data related to the Data Subject's entry and visit:

- date of entry: identification, verification
- date of departure: identification, verification
- name of the host: identification, verification

Legal basis for processing

Legitimate interest of the Controller (Article 6(1)(f) GDPR) or compliance with a legal obligation (Article 6(1)(c) GDPR), where restrictions are stipulated by government regulations.

Designation of legitimate interest

The legitimate interest is real and current, as the controller actually receives a large number of external guests and visitors continuously, so there would be a security risk if entries to the premises were not monitored. The check-in process therefore effectively and immediately reduces the security risks posed by the check-in of large numbers of visitors.

Duration of processing

The personal data of the data subjects are not stored by default, but may be stored by the Controller only in special situations or on the basis of the regulations in force, until the purpose is fulfilled, or for a maximum of 1 year from the date of check-in.

4.4. Body temperature measurement upon check-in

The Controller may perform body temperature measurement as a standard protective measure for all persons intending to enter its premises, or buildings owned or used by it.

Measuring body temperature does not require the identification of the data subject for this specific purpose and does not involve the recording, further storage or transmission of data in any way. Only persons who may be authorised to enter on the basis of a body temperature measurement will thereafter be allowed to use the services.

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 Controller's staff will not draw any conclusions about the health status of the person based on the body temperature measurement at the time of entry, but are entitled to grant or deny access.

The Controller therefore does not store any personal and health data and will only decide whether to allow or deny access to a person wishing to enter its premises (because the results of the measurement indicate a risk to other persons).

If access is denied by the person acting on behalf of the Controller, it is the Data Subject's responsibility to deal with the situation (seek medical advice, arrange for sick leave and sick pay, inform the manager at work, etc.), and the Controller has no further duty or responsibility in this regard.

4.5. Processing of bank card data:

The Data Subject will be required to provide this information when paying by bank card to enable booking and its fulfilment.

In the case of online booking, some of the data are transferred to the Controller by the individual accommodation intermediaries, travel agencies and ACCENT HOTEL SOLUTIONS Szolgáltató Kft.

Scope of the data processed and the specific purposes of processing:

- Name on bank card
- Bank card number
- Bank card expiry date

Legal basis for processing

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

Duration of processing

The Controller processes personal data for 8 calendar days after the departure of the data subject.

4.6. Loyalty programme:

The Controller provides personalised services and discounts for Data Subjects participating in the loyalty programme. The Data Subject may make the data available to the Controller electronically on the website or in person at the service partners.

Scope of the data processed and the specific purposes of processing

- Surname: for identification, communication
- First name: for identification, communication
- Date of birth: identification
- E-mail address: contact
- Delivery details (country, postcode, town, street, house number): for sending the card by post
- Hotel booking habits (which hotel, year, month, etc. the Data Subject stayed in): for the compilation of statistics

Legal basis for processing

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

Duration of processing

The Controller processes personal data until the Data Subject's consent is withdrawn. You may withdraw your consent in a note sent to info@accenthotels.com at any time.

4.7. Processing regarding event-related requests for proposals and orders:

The Data Subject (personal contributor of a legal person) may ask the Controller for a proposal concerning the organisation of an event and place an order with the Controller for such event in relation to the accommodation.

The data are transferred to the Hotel partly by ACCENT HOTEL SOLUTIONS Szolgáltató Kft.

Scope of the data processed and the specific purpose of processing

- Surname: identification, communication, contract performance
- First name: identification, communication, contract performance
- Company name: identification, communication, contract performance
- Name of personal contributor: identification, communication, contract performance
- Phone number: identification, communication, contract performance
- E-mail address: identification, communication, contract performance
- Request for meals: contract performance
- Programme: contract performance
- Request for rooms: contract performance
- Request for event rooms: contract performance
- Date of event: contract performance
- 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).

Duration of processing

If the Data Subject accepts the proposal, the data shall be blocked 5 years after the termination of the relationship with the Data Subject, as specified in Section 6:22 of the Civil Code. If we are required to retain the data under Section 169 of Act C of 2000 on Accounting ("Accounting Act"), we will block the data after 8 years following the termination of the relationship with the Data Subject. This is the case in practice if the data are part of documents underlying the accounts, for example in documents relating to the conclusion of the contract (in the contract itself, where applicable) or the invoice issued.

If the proposal is not accepted by the Data Subject, the Controller will store the data for the purposes of legitimate interests – the direct business interest in keeping the partners' previous offers – and will block the data after 3 years.

4.8. Processing related to contracting with partners

The Controller concludes contracts with various partners in order to provide them with services.

Scope of the data processed and the specific purpose of processing

- Last name of personal contributor: for identification, communication, contract performance

- First name of personal contributor: for identification, communication, contract performance
- Portrait: for the performance of the contract (in case of a contract specifically for photography)
- E-mail address: for identification, communication
- Telephone number: 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 processing is the performance of a contract (Article 6(1)(b) GDPR).

Duration of processing

The data shall be blocked 5 years after the termination of the relationship with the Data Subject as specified in Section 6:22 of the Civil Code. If we are required to retain the data under Section 169 of Act C of 2000 on Accounting ("Accounting Act"), we will block the data after 8 years following the termination of the relationship with the Data Subject. This is the case in practice if the data are part of documents underlying the accounts, for example in documents relating to the conclusion of the contract (in the contract itself, where applicable) or the invoice issued.

4.9. Processing in relation to complaint management:

Data Subjects may lodge complaints regarding the service provided by the Controller.

Scope of the data processed and the specific purpose of processing

- Surname: for identification, communication
- First name: for identification, communication
- Address: for identification, communication
- Content of complaint: for investigating the complaint
- E-mail address: for communication
- Telephone number: for communication

Legal basis for processing:

The legal basis for the processing is Section 17/A (7) of Act CLV of 1997 on Consumer Protection.

Duration of processing

The Controller shall keep the personal data related to the complaint, the recorded report and a copy of the response letter for 5 years from the date of the complaint, as defined by the Consumer Protection Act.

4.10. Processing in relation to evaluation

The Data Subject may evaluate the accommodation. The evaluation form may also be filled out anonymously, i.e. only for the evaluation.

Scope of the data processed and the specific purpose of processing

- Surname: for identification, communication
- First name: for identification, communication
- E-mail address: for identification, communication
- Date of stay: satisfaction survey, for statistical purposes
- Hotel evaluation: satisfaction survey, for statistical purposes

Legal basis for processing

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

Duration of processing

The Controller **processes** personal data **until the Data Subject's consent is withdrawn**. You may withdraw your consent in a note sent to sales@hotelambra.hu at any time.

4.11. Careers:

The Controller enables the Data Subject to apply for the job advertised by the Controller.

The purpose of the data transfer is to coordinate the activities of the members of the hotel chain, to facilitate the provision of services and to monitor them for quality assurance purposes.

Scope of the data processed and the specific purpose of processing

- Surname: identification, contact
- First name: identification, contact
- E-mail address: identification, contact
- Personal data provided voluntarily: may be necessary to select the right person for the position
- Personal data provided voluntarily in any document attached to the CV: may be necessary for the selection of the person suitable for the position

Legal basis for processing

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

Duration of processing

Following the selection of a suitable person for the vacant position, the 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 jobs of the Hotel Chain in a simplified manner. The explicit consent of the data subject allows the processing of their personal data for a period of 5 years, after which the data will be rendered anonymous.

If the Data Subject does not consent to the retention of their application or personal data, the data will be rendered anonymous **within 30 days** and CVs will be destroyed.

Recipient of the data transmission	Categories of data transmitted
Accent Hotel Management Szolgáltató Kft. (registered office: 1132 Budapest, Visegrádi utca 31. I. em.; company registration number: 01 09 689708; tax number: 12506527-2-41)	Surname, first name, e-mail address, voluntarily provided personal data, personal data provided voluntarily in any document attached to the CV: may be necessary for the selection of the person suitable for the position.

4.12. Newsletter:

The Data Subject may subscribe to the Controller's marketing newsletter. Accordingly, the Controller has the right to send to the Data Subjects who have subscribed to its newsletter, to the e-mail addresses they have provided, and, where applicable, subsequently modified, newsletters for direct marketing purposes, containing promotions and other information about the Controller's activities, subject to the frequency and with the content determined by the Controller.

The Controller will not send unsolicited commercial communications, and the Data Subject may unsubscribe from receiving offers without restriction and without having to specify their reasons, free of charge. In this case, all personal data necessary for sending the newsletter will be deleted from our records and we will not contact the Data Subject with further promotional offers. The Data Subject may unsubscribe from the newsletter at any time by clicking on the link contained in the message.

Scope of the data processed and the specific purposes of processing:

- Surname: identification, contact
- First name: identification, contact
- E-mail address: this is where we will send you the latest news.

Legal basis for processing

The legal basis for processing is your consent, and pursuant to Article 6 of Act XLVIII of 2008 on the Essential Conditions of and Certain Limitations to Business Advertising, the Data Subject may expressly consent in advance to being contacted by the Service Provider with advertising offers and other mailings at the contact details (e-mail) provided.

Duration of processing

The Controller will retain the personal data until the Data Subject's consent is withdrawn.

Data subjects' rights in relation to processing

The data subject may unsubscribe from the newsletter at any time, free of charge.

4.13. The Controller's presence in social media (Facebook, YouTube):

The hotel operated by the Controller is accessible on the social media portals Youtube and Facebook.

By clicking "like" on the Controller's Facebook page - https://www.facebook.com/hotelambra - the data subject consents to the publication of news and offers prepared by the Controller on their own Facebook page.

The operators of social media sites are separate controllers, independent of the Controller, and therefore the activities carried out there are covered by processing documents independent of the Controller.

For information about the Facebook Page's privacy practices, please read the privacy notice and guidelines at www.facebook.com.

4.14. Processing related to camera surveillance

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

- protection of property, assets and valuables, movable property of significant value;
- protection of the life and bodily integrity of persons, recording and investigating the circumstances of accidents;
- preventing, disrupting, clarifying, proving and documenting infringements;
- improving the services of the Controller, and its operation;
- dealing with customer complaints, handling and investigating related cases;
- supporting the implementation of measures in response to a pandemic.

Scope of the data processed and the specific purpose of processing

- Portrait: Protection of persons and property

Location of cameras

	Place of camera	Area monitored by the camera	Persons present in spaces being monitored
1	Hotel entrance left-hand side	street entrance	employees, guests, passers-by
2	-1st floor, on the wall	garage, -1st floor	employees, guests
3	Breakfast room	breakfast room	employees, guests
4	Lobby, next to the staircase	reception, lobby, entrance	employees, guests
5	Hotel entrance right-hand side	street entrance	employees, guests, passers-by
6	Lobby, reception back desk	reception, lobby, entrance	employees, guests

Legal basis for processing

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

Duration of processing

The Controller will record data for 8 days. In the event of a personal and property security incident, the Controller shall have the right to process the recordings for a period longer than 8 days.

4.15. Processing in relation to items lost and found:

The purpose of processing is: to administer items found in the area of the Hotel operated by the Controller and to notify the presumed owner or the finder.

Legal basis for processing: Sections 5:54, 5:55, 5:59 and 5:61 of Act V of 2013 on the Civil Code.

The data processed: date and place of finding, name and contact details of the finder, details of the item found.

Duration of processing: 1 year.

5. PERSONS AUTHORISED TO PROCESS DATA:

The Controller employs the processors listed in the table below to perform technical tasks relating to data processing operations. The rights and obligations of the processor in relation to the processing of personal data are determined by the Controller within the framework of the GDPR and the specific laws applicable to processing. The Controller is responsible for the lawfulness of its instructions. The processor may not make any decision on the substance of processing. It may process the personal data that come to their knowledge only in accordance with the provisions of the Controller. It may not process data for its own purposes, and must store and retain the personal data in accordance with the Controller's instructions.

Names and contact details of the processors	**Activities performed during processing**
HostWare Kft. Contact: http://hostware.hu/fooldal	Storage and management of room booking data. Invoicing
VITAL-COMP Ügyvitelszervező és Kereskedelmi Kft. http://www.vitalcomp.info/	They have access to all personal data processed by the Controller under this Notice. Its task is to store the personal data processed by the Controller.
SiteMinder Contact: https://www.siteminder.com/contact/	Guest communication system
Progen Kft.	Partner management system

Contact: https://www.progen.hu/	
Szakértő Kft. Contact: kovespal@t-online.hu	They have access to all personal data processed by the Controller under this Notice. Its task is to perform the accounting and bookkeeping tasks of the Controller.
DigitDoc Kft. Contact: https://digitdoc.hu	They have access to all personal data processed by the Controller under this Notice. It is responsible for the operation of the Controller's invoicing program.
VTL Design Kft. Contact: https://www.vtldesign.hu/#contact	Website operation, providing the technical background for online hotel room reservations
GlobeRes AG Contact: https://www.globres.com/contact/	Online hotel room booking service
Myhotelshop Gmbh Contact: https://www.myhotelshop.com/	Performance of online marketing tasks
Budapest Capital District VII Erzsébetváros Municipality Contact: https://www.erzsebetvaros.hu/	Performance of mandatory data reporting.
ACCENT HOTEL SOLUTIONS Szolgáltató Kft. Contact: https://accenthotels.com/hu/adatvedelem	Website operation, sending newsletters, operation of the technical background for online hotel room booking, creating and operating a loyalty card system, operating the 'Szép Card' acceptance system.
ACCENT Hotel Management Kft. Contact: https://accenthotels.com/hu/management-szolgaltatasok	They have access to all personal data processed by the Controller under this Notice. Its task is to process and store the personal data processed by the Controller.
Bonomi Kft. Contact: https://app.bonomi.io/	Online Chatbot operation.
MGMT Group Kft (Everguest)	Examining online reviews.

Contact: https://www.everguest.net/	
Legenda Kft. Contact: https://legenda.hu/hu	Programme sales
Eurama Idegenforgalmi Kft. Contact: https://eurama.hu/	Programme sales
Hungária Koncert Kft. Contact: https://budapestguide.info/	Programme sales
Vintage Garden Kft. Contact: https://vintagegarden.hu/	Restaurant service
Program Centrum Utazásszervező Kft. Contact: https://www.programcentrum.com/	Programme sales
BAT Hungary Kft. Contact: https://bpairporttransfer.hu/	Transfer service
E-Magine Travel Services Kft. Contact: https://www.emaginetours.com/	Programme sales
CRB Cityrama Kft. Contact: https://www.cityrama.hu/	Programme sales
Travel agencies, accommodation agencies	Accommodation reservation mediation
The Controller informs the Data Subjects that they will be notified individually about other processors engaged in connection with certain services and other Controllers related to the process (e.g. accommodation intermediaries).	

The Controller transfers data in connection with its services, to the entities listed in the table below:

Name and contact details of the recipient	**Description of data transmission**
VIZA system (Closed Guest Information Database) **Magyar Turisztikai Ügynökség Zrt.** 1027 Budapest, Kacsa u. 15-23.; 1525 Budapest, Postafiók 97.; Telephone: +36 1 488 8700; E-mail address: info@mtu.gov.hu;	The Controller will transmit the personal data of the guests in the way prescribed by law, i.e. by recording them in the VIZA system. The purpose of recording and at the same time transmitting the data is to protect the rights, safety and property of the Data Subject and others, and to monitor compliance with the provisions on the residence of third-country nationals and persons enjoying the right of free movement and residence.
NTAK (National Tourist Information Centre) **Magyar Turisztikai Ügynökség Zrt.** 1027 Budapest, Kacsa u. 15-23.; 1525 Budapest, Postafiók 97.; Telephone: +36 1 488 8700; E-mail address: info@mtu.gov.hu;	In the system operated by MTÜ, data from the accommodation management software is used to produce analyses to support data-driven decision making in the tourism industry. Competent local authorities and the NTCA also have access to the relevant data sets.
Competent authorities (the NTCA, the NHF, local governments, investigative authorities, counter-terrorism agencies, national security services, the public prosecutor's office and the courts)	The accommodation provider keeps a register of entry and stay of third-country nationals in accordance with the relevant law. It forwards these and other personal data contained in the register and guest log to the competent authority (e.g. police, national security authority, court, authority dealing with administrative offences, the public prosecutor's office) in cases specified by law (e.g. in connection with a crime or suspected crime or a request for data in connection with a specific procedure). In all cases, a record is kept of the transfer and transmission of data.

6. DATA SECURITY MEASURES

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

The Controller shall take all reasonable measures to ensure the security of the data, and shall ensure an adequate level of protection, in particular against unauthorised access, alteration, transmission, disclosure, erasure or destruction, accidental destruction or damage. The Controller shall ensure the security of the data by appropriate technical (e.g. logical protection, in particular encryption of passwords and communication channels) and organisational measures (physical protection, in

particular training of the Controller's employees regarding data security, restriction of access to information).

The Controller requires all of its employees who choose to work from home to use the required security features at their workstations. The Controller shall provide all employees with the necessary IT support to ensure that the data are used in a sufficiently secure manner.

7. INFORMATION ON CHILDREN

In the case of Data Subjects under the age of 14, only their legal representatives or guardians may provide personal data or make a legal declaration on their behalf.

A Data Subject over the age of 14 but under the age of 18 may provide personal data and make a legal declaration only with the consent of their legal representative or guardian. The Data Controller must fulfil its legal obligations for all hotel guests, i.e. scan and forward the related documents in accordance with the regulations. If the consent given by the legal representative, parent, guardian or custodian is not available in relation to the Data Subject under the age of 18, the Controller cannot provide the requested service because the related processing in accordance with the legal requirements cannot be carried out.
By providing the information, you represent and warrant that you will act in accordance with the foregoing and that your capacity to act in relation to the provision of the information is not restricted. If you do not have the legal right to provide the information, you must obtain the consent of the third party Data Subjects concerned (e.g. legal representative, guardian). In this context, you must consider whether the consent of a third party is required in connection with the provision of the information concerned. The Controller shall not have any personal contact with you, so you are responsible for ensuring compliance with this paragraph and the Controller shall not be held liable in this regard.

We will use all reasonable endeavours to delete any information that is unlawfully provided to us and will ensure that such information is not passed on to or used by anyone else (whether for advertising or other purposes). Please notify us immediately if you become aware that a child provided information about himself or herself without authorisation. You may contact us using the contact details highlighted at the beginning of this Policy.

8. DATA SUBJECTS' RIGHTS IN RELATION TO PROCESSING

The Data Subject's data protection rights and remedies and the relevant provisions and limitations of the GDPR in this regard are set out in detail in the GDPR (in particular Articles 15, 16, 17, 18, 19, 20, 21, 22, 77, 78, 79 and 82 of the GDPR). The following is a summary of the most important relevant regulations.

Right of access by the data subject

The Data Subject has the right to obtain from us confirmation as to whether or not personal data concerning him or her are being processed. Where that is the case, the Data Subject has right of 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 recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;

d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

e) the existence of the right to request from us rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;

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

g) where the personal data are not collected from the data subject, any available information as to their source;

h) the existence of automated decision-making, including profiling, and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

Where personal data are transferred to a third country, the data subject shall have the right to be informed of the appropriate safeguards relating to the transfer.

We shall provide a copy of the personal data undergoing processing to the Data Subject. Where the Data Subject makes the request by electronic means, and unless otherwise requested by the Data Subject, the information shall be provided in a commonly used electronic form.

Right to rectification

The Data Subject shall have the right to obtain from us without undue delay the rectification of inaccurate personal data concerning him or her. The Data Subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

Right to erasure ('right to be forgotten')

(1) The Data Subject shall have the right to obtain from us the erasure of personal data concerning him or her without undue delay where one of the following grounds applies:

a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

b) the Data Subject withdraws consent on which the processing is based, and there is no other legal ground for the processing;

c) the Data Subject objects to the processing and there are no overriding legitimate grounds for the processing;

d) the personal data have been unlawfully processed;

e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which we are subject; or

f) the personal data have been collected in relation to the offer of information society services.

(2) Where the Controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the Controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the Data Subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

(3) Paragraphs 1 and 2 shall not apply to the extent that processing is, *inter alia*, necessary:

a) for exercising the right of freedom of expression and information;
b) for compliance with a legal obligation which requires processing by Union or Member State law to which we are subject;
c) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or
d) for the establishment, exercise or defence of legal claims.

Right to restriction of processing

(1) The Data Subject shall have the right to obtain from us restriction of processing where one of the following applies:

a) the accuracy of the personal data is contested by the Data Subject, for a period enabling us to verify the accuracy of the personal data;
b) the processing is unlawful and the Data Subject opposes the erasure of the personal data and requests the restriction of their use instead;
c) we no longer need the personal data for the purposes of the processing, but they are required by the Data Subject for the establishment, exercise or defence of legal claims; or
d) the Data Subject has objected to processing, pending the verification whether the legitimate grounds of the Controller override those of the Data Subject.

Where processing has been restricted under paragraph 1, such personal data shall, with the exception of storage, only be processed with the Data Subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State.

The Data Subject shall be informed by us before the restriction of processing is lifted.

Notification obligation regarding rectification or erasure of personal data or restriction of processing

The Controller shall communicate any rectification or erasure of personal data or restriction of processing to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. We shall inform the Data Subject about those recipients if the data subject requests it.

Right to data portability

(1) The Data Subject shall have the right to receive the personal data concerning him or her, which he or she has provided to us, in a structured, commonly used and machine-readable format and

have the right to transmit those data to another controller without hindrance from the Controller, where:

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

(b) the processing is carried out by automated means.

In exercising his or her right to data portability pursuant to paragraph 1, the Data Subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.

Right to object

The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her, including profiling. We shall no longer process the personal data unless we demonstrate compelling legitimate grounds for the processing which override the interests, rights and freedoms of the Data Subject or for the establishment, exercise or defence of legal claims.

Where personal data are processed for direct marketing purposes, the Data Subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.

Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.

In the context of the use of information society services, and notwithstanding Directive 2002/58/EC, the Data Subject may exercise his or her right to object by automated means using technical specifications.

Where personal data are processed for scientific or historical research purposes or statistical purposes, the Data Subject, on grounds relating to his or her particular situation, shall have the right to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

Right to lodge a complaint with a supervisory authority

The Data Subject may assert their rights before the courts under the GDPR and the Civil Code, and may also contact the National Authority for Data Protection and Freedom of Information (NAIH) (1125 Budapest, Szilágyi Erzsébet fasor 22/C; postal address: 1530 Budapest, Pf. 5; phone: +36 1 391 1400; e-mail: ugyfelszolgalat@naih.hu) in case of complaints about the controller's data processing practices. Detailed rights and remedies regarding processing are set out in Articles 77, 79 and 82 of the GDPR.

Right to an effective judicial remedy against a supervisory authority

The Data Subject shall have the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning the Data Subject.

The Data Subject shall have the right to an effective judicial remedy where the supervisory authority does not handle a complaint or does not inform the Data Subject within three months on the progress or outcome of the complaint lodged.

Proceedings against a supervisory authority shall be brought before the courts of the Member State where the supervisory authority is established.

Right to an effective judicial remedy against a controller or processor

The Data Subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under the GDPR have been infringed as a result of the processing of his or her personal data in non-compliance with the GDPR.

Proceedings against a controller or a processor shall be brought before the courts of the Member State where the controller or processor has an establishment. Alternatively, such proceedings may be brought before the courts of the Member State where the Data Subject has his or her habitual residence.

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