

DATA PROCESSING POLICY

I. PREAMBLE, LEGAL BASIS FOR PROCESSING

The Data Controller, the Gyáli-Városgazda Gazdasági-Műszaki Ellátó Korlátolt Felelősségű Társaság (located at: 2360 Gyál, Ady Endre utca 22., company registration number: 13-09-160450, tax number: 24184409-2-13, represented by Gábor Zsigovits, Managing Director, hereinafter referred to as "Data Controller" or "Gyáli-Városgazda Kft. "), in accordance with the provisions of the Fundamental Law of Hungary and Act CXII of 2011 on the Right to Informational Self-Determination and Freedom of Information (hereinafter referred to as "Info tv.") and the European Parliament and Council (EU) 2016/679 (2016. (hereinafter referred to as "GDPR"), and in accordance with the Hungarian legislation applicable to hotel services, in particular the Government Decree No. 239/2009 (X. 20.) on the detailed conditions for the provision of accommodation services and the procedure for issuing accommodation operating licences, and in order to ensure the protection of personal data, the following data management and data security policy is established.

The Gyáli Városgazda Kft. mainly processes personal data provided by our hotel or restaurant guests or prospective guests when making reservations, as well as data provided on our website. Personal data may not be collected directly from the data subject, but may be transmitted to us using an accommodation booking system operated by another party.

The processing of personal data is lawful only if and to the extent that at least one of the following conditions is met:

- (i) the data subject has given his or her consent to the processing of his or her personal data for one or more specific purposes;
- (ii) the processing is necessary for the performance of a contract to which the data subject is a party or is necessary for the purposes of taking steps at the request of the data subject prior to entering into that contract;
- (iii) processing is necessary for compliance with a legal obligation to which the controller is subject;
- (iv) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
- (v) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- (vi) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require the protection of personal data, in particular where the data subject is a child.

II. SCOPE OF THE RULES

II.1. Personal scope

The scope of the Rules covers

- the data controller;
the data processor;
- all employees and collaborating partners (agents and contractors) of Gyáli-Városgazda Kft. as the data controller;
- hotel guests of the Gyáli-Városgazda Kft. on the basis of their consent and other valid title.

For the purposes of this Policy, the data controller is Gyáli-Városgazda Gazdasági-Műszaki Ellátó Korlátolt Felelősségű Társaság (located at: 2360 Gyál, Ady Endre utca 22. , company registration number: 13-09-160450, tax number: 24184409-2-13, represented by Gábor Zsigovits, Managing Director), which determines the purpose of the processing of data, takes and implements the decisions concerning the processing (including the means used), or implements them through the data processor it has appointed (hereinafter referred to as "Data Controller", Gyáli-Városgazda Ltd.).

The Data Controller entrusts data processing to the following companies::

- Provides hosting and web hosting services to the Data Controller: Nethely.hu (Nethely Kft., 1115 Budapest, Halmi utca 29.)
- The following booking systems provide the online booking for the Data Controller: booking.com (Booking.com B.V.,located at: Oosterdokskaade 163, 1011 DL, The Netherlands), szallas.hu (Szallas.hu Zrt.,located at: 3525 Miskolc, Régiposta utca 9.), SabeeApp (thePass Kft.,located at: 1075 Budapest, Madách Imre út 13-14.);
- A The Facebook page is hosted by Meta Platforms Inc. (1601 Willow Road Menlo Park, CA 94025, USA) and operated by www.facebook.com, whose Hungarian language site is maintained by Meta Platforms Ireland Ltd.

II.2. Substantive scope

The scope of the Policy covers the processing by the Controller of personal data which form part of a filing system operated by the Controller or the Processor or which are intended to form part of a filing system, in particular

- data stored on the information technology system of the Controller;
- data stored by the Controller on paper documents;
- all documents, data and data media recorded and stored in the information technology system or produced as a result of processing, irrespective of the way in which they are processed or produced and irrespective of the medium in which they are presented;
- documents, data media and data carriers containing personal data of third parties provided by the Data Controller's contractual partners;
- the storage and use of data media.

III. PRINCIPLES GOVERNING THE PROCESSING OF PERSONAL DATA

Personal data are processed by the Data Controller in accordance with the following principles:

The processing is lawful, fair and transparent to the data subject.

The processing shall be carried out lawfully, fairly and lawfully, and in accordance with the law and the data subject's legitimate interests.

The processing must be accurate and, where necessary, kept up to date. In this context, the Controller and the Processors shall take all reasonable steps to ensure that inaccurate data are erased or rectified without undue delay.

Personal data shall be kept for a limited period of time necessary to achieve the purposes for which they are processed. Personal data are stored for a limited period of time necessary to achieve the purpose of the processing.

In processing personal data, the Data Controller ensures protection against unauthorised or unlawful processing and accidental loss, destruction or damage. The processing of personal data shall be

carried out in such a way as to ensure adequate security of personal data, including protection against unauthorised or unlawful processing, accidental loss, destruction or damage ("integrity and confidentiality"), by implementing appropriate technical or organisational measures.

Personal Data shall be processed by the Controller only for the purposes and in the manner specified in this Policy and for the exercise of the rights and obligations set out in this Policy. The processing must comply with this purpose at all stages.

The Controller shall only process personal data which is necessary for the purpose of the processing, which is adequate for the purposes for which it is processed and only to the extent and for the duration necessary for the purposes for which it is processed.

The Controller shall be responsible for compliance with the above and shall be able to demonstrate such compliance ("accountability").

IV. THE SCOPE OF THE DATA PROCESSED

Purpose of data processing: the purpose of data processing is to record room reservations made online, in person at the hotel or by telephone, as well as to provide hotel services and lobby bar services. Details of each service are available at www.a22hotel.hu.

In the case of room reservations, the purpose of the processing is to record the reservation, to identify the guest who made the reservation and to provide payment facilities.

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

Data processed: name, date of arrival, date of departure, ID card number, full credit card details, service package to be used, email address, postal address, other requests (e.g. registration number in case of parking)

For online bookings, we are also connected to Hungarian and European booking systems (booking.com, szallas.hu, SabeeApp), which operate according to their own data processing policies. If you have made your booking through an external on-line booking system, the source of the data is the operator of the on-line system. If you have any questions, please read carefully the privacy policies of these operators.

In the case of reservations made through the above mentioned booking systems, the data necessary for the reservation are transmitted to us by the booking systems.

Duration of data processing: 5 years from the date of service use (performance of the contract).

1. Data processing in relation to invoicing

The purpose of the processing: to issue invoices and to keep accounting records in accordance with the law, following the services provided.

Pursuant to Article 169 (1) to (2) of the Act, companies must keep accounting documents that directly and indirectly support the accounting.

Legal basis for processing.

Data processed: name, address.

Duration of data management: invoices issued must be kept for 8 years from the date of issue of the invoice, pursuant to Section 169 (2) of the Public Finance Act.

2. Camera surveillance system

Purpose of data processing: the purpose of data processing is the protection of persons and property in the hotel premises operated by Gyáli Városgazda Kft. The camera surveillance is indicated by a pictogram and warning text at the entrance of the hotel.

Legal basis for processing: article 6 (1) (f) GDPR (legitimate interest of the Data Controller).

Scope of data processed: camera images of the data subjects.

Duration of data processing: ... days from the date of recording of the camera recordings.

3. Sending out newsletters

Purpose of processing: to inform data subjects about our services, promotions and news. We only send newsletters if you give your express, voluntary consent, which can be withdrawn at any time.

Legal basis for processing: consent of the data subject pursuant to Article 6(1)(a) of the GDPR.

Scope of data processed: email addresses of recipients of electronic newsletters.

Duration of processing: until consent is withdrawn. We will only send our newsletter to the data subject for as long as he or she requests it. If the data subject no longer wishes to receive the newsletter, he or she can unsubscribe at any time by using the link at the bottom of the newsletter. Such withdrawal of consent shall not affect the lawful processing of the data prior to such withdrawal.

4. Frequent Guest Programme

Purpose of data processing: to provide a service of your choice to our returning guests and to increase trust in our hotel.

Legal basis for processing: consent of the data subject pursuant to Article 6(1)(a) of the GDPR.

Data processed: name, email address.

Duration of processing: until the consent is withdrawn, if there is no other legal basis for processing, or until the purpose of the processing ceases to exist at the latest. If the data subject does not wish to participate in our loyalty programme, he or she may withdraw his or her consent at any time.

5. Complaint handling

During the consumer complaint handling process, if you disagree with the handling of the complaint or if it is not possible to investigate the complaint immediately, Gyáli Városgazda Kft. shall immediately record the complaint and its position on the complaint.

Legal basis for processing.

Scope of the data processed: the content of the record, in particular: the name and address of the consumer, a detailed description of the consumer's complaint, the documents, records and other evidence presented by the consumer.

Duration of processing: 3 years as defined by law.

6. Data management of the website

For details, see the information on the placement of cookies on the website.

When the data subject visits our website, the data of your device (e.g. the device used) are automatically recorded. Such data include IP address, time and date of visit, type of browser used, type of operating system, and domain name and address of the Internet service provider. The data recorded is

automatically logged by the web server serving the website without any declaration or action by the data subject when the website is viewed. From this data, the system automatically generates statistical data. These data are no longer personal data, they are used for statistical purposes only.

Purpose of data processing:

Legal basis for processing:

Duration of processing: 30 days from the date of accessing the website.

Data collected for the purpose of data transmission:

Purpose of data processing: the purpose of data processing is to fulfil the mandatory transmission of data by the accommodation provider to the National Tourist Information Centre (NTAK).

Legal basis for the processing: Article 6(1)(c) GDPR (fulfilment of a legal obligation)

6.6.6.1 (legal obligation) pursuant to Government Decree No. 235/2019 (X. 15.) on the implementation of the Act on State Tasks for the Development of Tourist Areas and in order to fulfil a legal obligation as defined in Act CLVI of 2016 on State Tasks for the Development of Tourist Areas (Tourism Act).

The accommodation service provider shall transmit the data pursuant to Section 9/H (1) of the Tourism Act to the hosting provider in electronic form and encrypted per accommodation unit using the accommodation management software, with the assistance of the data transmission module.

Duration of data processing: for the period specified by law.

V. OBLIGATION TO PROVIDE INFORMATION

The Data Controller shall take appropriate measures to provide the data subject with all the information relating to the processing of personal data in a concise, transparent, intelligible and easily accessible form, in clear and plain language.

The Data Controller shall fulfil its obligation to provide information by drawing up and publishing this Policy and by drawing up information notices for each category of data subject and by displaying information notices.

Forms of information:

- **Privacy Policy: this Policy, which is available on the website of the Data Controller (www.a22hotel.hu).**
- Data Processing Notice.

VI. DATA TRANSMISSION

Data recorded for the purpose of data transmission:

Purpose of data processing: the purpose of data processing is the mandatory transmission of data by the accommodation provider to the National Tourist Information Centre (NTAK).

The processing is based on Article 6(1)(c) of the GDPR (fulfilment of a legal obligation). is based on the implementation of the Government Decree 235/2019 (X. 15.) on the implementation of the Act on State Tasks for the Development of Tourist Areas and the legal obligation set out in Act CLVI of 2016 on State Tasks for the Development of Tourist Areas (Tourism Act). In addition to the above, personal data may be disclosed to third parties only with the prior written consent of the data subject. This does not apply to any mandatory data transfers, which may only take place in exceptional cases. The Data Controller informs the data subjects that it uses data processors to process and store

the data processed in the employer's human resources system. The Data Controller shall inform the data subjects of the identity of the processors.

The Data Controller expects its contracted data processing partners to comply with the provisions of the Infotv., the GDPR and the applicable data protection legislation to the maximum extent possible, but at least to the extent guaranteed by this Policy, when processing personal data for third parties. The Data Controller shall seek the specific consent of the data subjects in all cases where the transfer is to a country outside the EEA. Both the information and the consent must include the exact identity of the data processor (name and address or company name and registered office), the scope of the data transferred, the exact physical location of the storage and processing of the data.

For the purposes of monitoring the lawfulness of the transfer and informing the data subjects, the Controller shall keep a record of the transfers of data involving a higher risk and involving a larger volume of data, including the date of the transfer of the personal data processed, the legal basis and the recipient of the transfer, the scope of the personal data transferred and other information specified in the legislation providing for the processing.

VII. DATA DELETION

The personal data shall be erased if the purpose of the processing has ceased and there are no longer any reasonable grounds for keeping the personal data or if the data subject has given a reason for not keeping the personal data in accordance with Article 17. Article 17(1), namely in the following cases: where the purpose of the processing has ceased to exist; where the data subject has withdrawn his or her consent to the processing and there is no other legal ground for the processing; or where the data subject objects to the processing of his or her personal data on the basis of a legitimate interest pursued by the controller or a third party and there are no compelling legitimate grounds which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims or where the data subject objects to processing for direct marketing purposes; or where the personal data have been unlawfully processed; or where the personal data must be erased in order to comply with a legal obligation under Union or Member State law to which the controller is subject; or where the collection of personal data is based on a ground referred to in Article 8. Article 8(1) of the GDPR.

VIII. DATA SECURITY

The Data Controller, as well as the data processor within its scope of activities, implements appropriate technical and organizational measures, taking into account the position of science and technology and the costs of implementation, as well as the nature, scope, circumstances, and purposes of data processing, and considering the variable likelihood and severity of risks to the rights and freedoms of natural persons. This is done to ensure a level of data security that corresponds to the level of risk.

Data must be protected by appropriate measures, especially against unauthorized access, alteration, transmission, disclosure, deletion, or destruction, as well as against accidental destruction and damage, and against becoming inaccessible due to changes in the applied technology.

When determining and implementing measures to ensure the security of data, the Data Controller and the data processor must take into account the current state of technology. Among several possible data processing solutions, the one that ensures a higher level of protection of personal data should be chosen, unless it would impose disproportionate difficulties on the Data Controller.

IX. THE RIGHTS OF THOSE CONCERNED AND THEIR ENFORCEMENT

IX.1. The rights of the individuals concerned

The data subject, based on Article 13 of the GDPR, has the right to request information about the processing of their personal data. According to Article 15, they have the right to access personal data and the information listed in the referenced article. Under Article 16, the data subject can request the correction of their personal data, and according to Article 17, they can request the deletion of their data or, in accordance with Article 18, restriction of processing. Additionally, as per the provisions of Article 21, they have the right to object to the processing of their personal data. In cases specified in Article 20, the data subject also has the right to data portability. These rights are not absolute, and their fulfillment is possible only under the conditions specified in the relevant legal provisions.

IX.2. Right to information

Upon the data subject's request, the Data Controller provides information about the data subject's processed data, as well as data processed by a data processor appointed by the Data Controller. This information includes details about the source of the data, the purpose and legal basis of processing, the duration of processing, the name and address of the data processor, and their related activities. In cases of data transmission, the legal basis and recipient of the data transfer are also disclosed.

The Data Controller does not deny the fulfillment of the data subject's request for exercising their rights, except if it can prove that identifying the data subject is impossible. The provision of information and taking necessary actions must be provided free of charge if the requesting party has not submitted a request for information regarding the same data category to the Data Controller in the current calendar year.

If the data subject's request is clearly unfounded or, particularly due to its repetitive nature, excessive, the Data Controller may charge a reasonable fee or refuse to take action based on the request, considering the administrative costs associated with providing the requested information or taking the requested action. If costs were already paid, they should be refunded if the data was unlawfully processed or if the information request led to a correction.

In case of denial of information, the Data Controller informs the data subject in writing about the applicable legal provisions justifying the refusal. In such instances, the Data Controller also informs the data subject about the possibility of seeking judicial remedies and contacting the National Authority for Data Protection and Freedom of Information (located at Falk Miksa u. 9-11, 1055 Budapest, Hungary; mailing address: 1530 Budapest, Pf.: 5.; email: ugyfelszolgalat@naih.hu, hereinafter referred to as the Authority). If you are not a Hungarian citizen, you may also contact the data protection authority in your own Member State.

IX.3. Right to access

The data subject is entitled to receive feedback from the Data Controller regarding whether the processing of their personal data is ongoing. If such processing is underway, the data subject has the right to access the personal data and information about the purpose of processing, the categories of processed data, and the recipients to whom the personal data has been disclosed.

The data subject is entitled to access information about the planned duration of storing personal data or the criteria for determining this duration. Additionally, they have the right to request the correction, deletion, restriction of processing, or to submit a complaint to the supervisory authority.

If personal data is transmitted to a third country or international organization, the data subject has the right to be informed about the guarantees related to the transfer.

The Data Controller provides the data subject with a copy of the personal data undergoing processing. For additional copies requested by the data subject, the Data Controller may charge a reasonable fee based on administrative costs. If the data subject has submitted the request electronically, the information should be provided in a widely used electronic format unless otherwise requested by the data subject.

IX. 4. Right to Rectification

The data subject is entitled to request the Data Controller to rectify without undue delay any inaccurate personal data concerning them. Taking into account the purpose of the data processing, the data subject has the right to request the completion of incomplete personal data, including by means of providing a supplementary statement.

IX. 5. Right to Erasure (Right to be Forgotten)

The data subject is entitled to request the Data Controller to erase without undue delay the personal data concerning them. In such cases, the Data Controller is obligated to delete the personal data related to the data subject if one of the following reasons applies:

- (i) the personal data is no longer needed for the purposes for which it was collected or otherwise processed;
- (ii) the data subject withdraws their consent on which the processing is based, and there is no other legal ground for the processing;
- (iii) the data subject objects to the processing, and there are no overriding legitimate grounds for the processing;
- (iv) the personal data has been unlawfully processed;
- (v) erasure is required to fulfill a legal obligation to which the Data Controller is subject.

IX. 6. Right to Restriction of Processing

The data subject has the right to request the Data Controller to restrict the processing if one of the following conditions is met:

- (i) the data subject contests the accuracy of the personal data, in which case the restriction applies for a period allowing the Data Controller to verify the accuracy of the personal data;
- (ii) the processing is unlawful, and the data subject opposes the erasure of the data, instead requesting the restriction of their use;
- (iii) the Data Controller no longer needs the personal data for the purposes of processing, but the data subject requires them for the establishment, exercise, or defense of legal claims; or
- (iv) the data subject has objected to the processing; in this case, the restriction applies for the time it takes to determine whether the legitimate grounds of the Data Controller override those of the data subject.

IX. 7. Right to Data Portability

The data subject has the right to receive their personal data provided to the Data Controller in a structured, commonly used, and machine-readable format. They are also entitled to transmit these data to another data controller without hindrance from the Data Controller, where the legal basis for processing is the data subject's consent or the processing is necessary for the performance of a contract with the data subject, and the processing is carried out by automated means.

IX. 8. Right to Object

The data subject has the right to object to the processing of their personal data in the following cases:

- a) if the processing or transmission of personal data is necessary for the fulfillment of a legal obligation binding on the Data Controller or for the legitimate interests pursued by the Data Controller, the data transferor, or a third party, except in the case of mandatory data processing;
- b) if the use or transmission of personal data is carried out for direct marketing, public opinion research, or scientific research purposes; and
- c) in other cases defined by law.

The Data Controller shall examine the objection as soon as possible but no later than within 1 month of the submission of the request, make a decision regarding its validity, and inform the applicant in writing of the decision. If the Data Controller establishes the validity of the data subject's objection, they shall cease the data processing, including further data collection and transmission, and lock the data. The Data Controller shall also notify those to whom the relevant personal data was previously transmitted and who are obliged to take action to enforce the right of objection.

If the data subject disagrees with the decision of the Data Controller or if the Data Controller fails to meet the aforementioned 1-month deadline, the data subject may appeal to the court within 30 days from the communication of the decision or the last day of the deadline.

In this case, the Data Controller cannot continue processing personal data unless the Data Controller proves that there are compelling legitimate reasons for the processing that override the interests, rights, and freedoms of the data subject or are related to the submission, enforcement, or defense of legal claims.

If the data subject objects to the processing of personal data for direct marketing purposes, the personal data cannot be further processed for this purpose.

The right to object must be explicitly brought to the attention of the data subject during the first contact with them, and the relevant information must be presented clearly and separated from any other information.

If personal data is processed for scientific or historical research purposes or statistical purposes, the data subject has the right to object to the processing of their personal data for reasons related to their particular situation unless the processing is carried out for the performance of a task carried out in the public interest.

IX. 9. Data breach

The Data Controller has developed a data breach policy for cases of personal data-related infringements, which outlines the possibility of reporting data breaches and designates individuals responsible for addressing data breaches, as well as the applicable deadlines.

IX. 10. Right to Lodge a Complaint with a Court

In case of a violation of their rights, the data subject has the right to bring the matter to court. The court shall expedite the proceedings. The Data Controller is obligated to prove that the data processing complies with the legal requirements. The jurisdiction of the court is determined by the relevant law. The lawsuit can be filed before the court of the data subject's domicile or residence, based on the choice of the data subject. If the court grants the request, the Data Controller may be obliged to provide information, correct the data, restrict the processing, delete personal data, annul decisions made by automated processing, and consider the data subject's right to object. The court may order the publication of its judgment, including the identification data of the Data Controller, if the interests of data protection and the rights protected by this law of a larger number of data subjects so require.

IX. 11. Right to Compensation

The Data Controller is obligated to compensate any damage caused to others by the illegal processing of the data of the data subject or the violation of data security requirements. If the Data Controller violates the data subject's right to personal privacy through the illegal processing of the data or the breach of data security requirements, the data subject may claim damages from the Data Controller.

The Data Controller is also responsible for damages caused by the data processor to the data subject. The Data Controller is exempt from liability if it proves that the damage was caused by an unavoidable external factor beyond the scope of data processing. Compensation for damage and claims for damages cannot be demanded to the extent that the harm or violation of the right to personal privacy resulting in the damage was due to intentional or grossly negligent conduct by the data subject.

2023. november ...

.....
Gyáli-Városgazda Kft.
Zsigovits Gábor Executive