

Privacy Policy

Data Controller: Kúria Zrt.

Registered Address: 9737 Bük, Nagy Pál utca 7

Tax ID: 10426656-2-18

Phone: +36 20 511 8263

Email: info@bukfalva.hu

1. General Provisions

The Data Controller ensures that all personal data processing activities are conducted lawfully and purposefully. This Privacy Policy aims to provide guests booking accommodations and sharing personal data with the necessary information about how their data will be handled, from the booking process to the period following their stay.

The Data Controller abides by the regulations outlined in this policy, considering them mandatory for all personal data processing cases.

The data processing operations comply with relevant laws, specifically:

EU Regulation 2016/679 (GDPR): Protecting the rights of natural persons concerning personal data processing and the free movement of such data.

Hungarian Law on Information Self-Determination and Freedom of Information (2011 CXII).

Definitions of Terms Used in this Policy

Data Subject: Any identified or identifiable individual based on personal data.

Personal Data: Any information associated with the Data Subject that allows conclusions about the individual, including names, identifiers, or other unique characteristics.

Consent: The voluntary, explicit indication by the Data Subject, based on adequate information, expressing clear consent to process their data for specific or general purposes.

Data Controller: The natural or legal person who determines the purposes and methods of data processing.

Data Processing: Any operation or set of operations performed on data, such as collection, storage, alteration, use, disclosure, and destruction, regardless of the method or device used.

Data Transfer: Making data accessible to specific third parties.

Data Deletion: Irreversibly erasing data to prevent future recovery.

Data Processor: Any person or organization that processes data on behalf of the Data Controller under a contract.

Data Protection Incident: Unauthorized access, alteration, transmission, publication, deletion, or destruction of personal data, as well as accidental damage or loss.

2. Online Booking Data Processing

The Data Controller offers an online booking option for guests to facilitate a quick, convenient, and cost-free reservation process.

Purpose of Data Processing: To make the booking process easier and more efficient.

Legal Basis: The prior consent of the individual making the reservation.

Data Processed: Title, first name, last name, address (country, postal code, city, street, house number), phone number, email address, gender; for companies, company name, headquarters, tax ID, and bank card number.

Data Retention Period: Five years from the last day of stay according to the booking.

Use of Data Processor:

The company uses an IT service provider for the online booking system:

Provider: "A VENDÉGEM SZÁLLÁS SZOFTVER"

Contract Number: 2023/55218570

Consequences of Not Providing Data: Failure to provide the necessary data will result in the inability to complete the room reservation.

Additional Information: The Data Controller takes all necessary technical and organizational measures to prevent data protection incidents, such as damage or loss of personal data files or unauthorized access. In the event of an incident, the company keeps a record of the affected personal data, scope and number of affected individuals, date, circumstances, impact, and corrective actions taken, along with other required data as specified by applicable laws.

3. Inquiry Processing

The company provides an option for guests to request quotes electronically, offering information based on availability.

Purpose of Data Processing: To allow prospective guests to gather preliminary information about accommodation pricing.

Legal Basis: The prior consent of the individual making the inquiry.

Data Processed: Title, first name, last name, phone number, email address, number of guests, and gender.

Data Retention Period: Five years from the last day of the intended stay.

4. Cookie Management

To provide personalized service, the Data Controller places small data files, known as cookies, on the user's computer and retrieves them on future visits. If the browser returns a previously saved cookie, the service provider can link the current visit to previous ones for content solely within its own scope.

Purpose of Data Processing: To identify, track, and distinguish users; identify user sessions and store data provided during sessions; prevent data loss; and facilitate web analytics and personalized service.

Legal Basis: The consent of the user.

Data Processed: Identifier number, date, time, and the URL of the previously visited page.

Data Retention Period: A maximum of 90 days.

Additional Information: Users can delete cookies from their computers or disable cookies in their browsers. This can typically be done under the Tools/Settings menu in the browser's Privacy/History/Custom settings. Cookies are often labeled as "cookie," "süti," or "tracking" in these settings.

5. Website Server Logs

When visiting the website <http://www.bukfalva.eu>, the web server automatically logs user activity.

Purpose of Data Processing: During the website visit, the service provider records visitor data to monitor the operation of services and prevent misuse.

Legal Basis: GDPR Article 6(1)(f) – Legitimate interests of the company in ensuring the secure operation of the website.

Data Processed: Identifier number, date, time, and the URL of the visited page.

Data Retention Period: A maximum of 90 days.

Additional Information: The company does not attempt to identify users by linking logged data with other information. However, combined with data provided during registration, such as the visited page and timestamp, it may indirectly infer user actions.

External Service Providers and Data Processing Related to Logging: The portal's HTML code includes links to external servers. These servers can communicate directly with the user's device, and as such, providers may collect user data (e.g., IP address, browser and OS details, mouse movements, URL of visited pages, and visit timestamps). The IP address is a numeric sequence that uniquely identifies devices connecting to the internet.

6. Guest Registration Form Data Processing

Upon check-in, the apartment requires guests to fill out a registration form with their personal details. The Data Controller stores the information both digitally and in paper form.

Purpose of Data Processing: For contact during the guest's stay, for post-departure contact, to distinguish guests, assist in the declaration of tourism tax, and fulfill the Data Controller's legal obligations.

Legal Basis:

Guest consent – GDPR Article 6(1)(a).

Legal obligation of the Data Controller – GDPR Article 6(1)(c).

Data Processed: First and last name, birth name, email address, phone number, place and date of birth, gender, nationality, address, license plate number, room number, check-in and check-out dates, accompanying guests' information, newsletter subscription, and payment method.

For foreign nationals: Passport or identification document data, visa or residence permit number, and entry date and location.

Accommodation address, start and expected/actual end date of stay.

Data Retention Period: Data are stored until the end of the first year after they become known to the Data Controller, for purposes specified in Act CLVI of 2016. For accounting compliance under Act C of 2000, data are retained for eight years from the end of the reporting year.

Consequences of Not Providing Data: The individual will not be able to check in to the accommodation.

Additional Information: The company undertakes all necessary technical and organizational measures to prevent data protection incidents (e.g., damage or loss of files containing personal data or unauthorized access). In case of an incident, the Data Controller logs details about affected data, the scope of affected individuals, date, impact, and measures taken to resolve the incident.

7. Telephone Booking Data Processing

The apartment accepts room bookings via telephone, after which it requests a written confirmation from guests. The Data Controller records telephone bookings in the apartment management software along with the booker's data.

Purpose of Data Processing: To record the room reservation.

Legal Basis:

Guest consent – GDPR Article 6(1)(a).

Necessary for the performance of a contract or steps taken at the request of the data subject before entering a contract – GDPR Article 6(1)(b).

Data Processed: Name, phone number, and email address.

Data Retention Period: Data are retained for eight years following the end of the reporting year for accounting compliance per Act C of 2000.

Consequences of Not Providing Data: Failure to provide data means the reservation cannot be completed.

Additional Information: The company takes necessary steps to prevent data protection incidents and maintains records of any incident's impact, affected data, and corrective actions.

8. Payment Data Processing

Guests can pay for services by cash or bank transfer.

Purpose of Data Processing: To issue an invoice for the services provided.

Legal Basis:

Guest consent – GDPR Article 6(1)(a).

Necessary for the performance of a contract in which the data subject is a party, or to take steps at the data subject's request prior to entering a contract – GDPR Article 6(1)(b).

Necessary for compliance with the Data Controller's legal obligations – GDPR Article 6(1)(c).

Data Processed: Name, address, list of services, total amount, payment method, invoice date, payment completion date, and transaction identifiers for card payments.

Data Retention Period: Data are retained for eight years following the end of the reporting year, as required for compliance with Act C of 2000 on accounting.

Use of Data Processor:

Data Processor: The Data Controller's bank.

9. Group Booking and Corporate Event Data Processing

The apartment also facilitates group bookings and event reservations, which may involve storing personal data of participants and organizers.

Purpose of Data Processing: To organize accommodation for groups, facilitate event planning, and identify guests.

Legal Basis: Prior consent of the individual organizing the group booking or event.

Data Processed: For companies, name, tax ID, and headquarters; for the booking contact, name, phone number, email; participant names, birth information, vehicle license plates, and list of services ordered as specified in the confirmation and offer.

Data Retention Period: Five years from the last day of the group's stay.

Data Storage: Data is recorded and stored on the apartment's internal server.

10. Job Applicant Data Processing

If an individual applies for a job position advertised by the company, their personal data is processed according to GDPR, Hungary's Information Self-Determination Law, and the Labor Code.

Purpose of Data Processing: To facilitate the selection process for employment.

Data Processed: Personal identification data, contact information, employment-related data, including salary expectations, education, skills, work experience, language proficiency, and other relevant details provided by the applicant.

Legal Basis:

Intention to form an employment contract – GDPR Article 6(1)(b).

Legitimate interest of the Data Controller – GDPR Article 6(1)(f).

Applicant's consent – GDPR Article 6(1)(a).

Description of Legitimate Interest:

The company's interest in recruiting the best candidate for an open position. This includes conducting interviews and assessing professional skills.

In case of potential legal disputes, the company retains data to demonstrate the fairness and legality of the recruitment process.

Data Sources: Data provided directly by the applicant.

Data Recipients: Only HR personnel, the applicant's prospective supervisor, and executive management have access to the data during evaluation.

Data Retention Period:

If hired, data is retained according to the data processing rules for employment.

If not hired, the data is retained for further consideration only if the applicant provides explicit consent, for up to one year.

For possible legal claims, data is retained until six months after the statutory limitation period ends.

No Automated Decision-Making: The company does not use automated decision-making or profiling with regard to job applications.

11. Other Data Processing

For data processing cases not listed in this policy, information is provided at the time of data collection. The company informs guests and interested parties that certain authorities and public bodies may request data under legal requirements. In such cases, the company provides only the necessary information specified by law.

When communication or data collection occurs on third-party platforms (e.g., Booking.com, online payment services), the third party acts as an independent data controller and processes data in line with its own privacy policies.

12. Storage and Security of Personal Data

The Data Controller's IT systems and other data storage locations are located at the company's premises and on servers leased by data processors. The Data Controller ensures that all IT tools used for processing data during service delivery are operated in a way that safeguards:

Authorized Access: Data is accessible only to those authorized to access it.

Authenticity and Verification: Data integrity and authenticity are maintained.

Data Inalterability: Measures ensure that data remains unchanged unless necessary.

Protection from Unauthorized Access: Data is protected by individual passwords.

The Data Controller is particularly diligent in ensuring data security. It has implemented the necessary technical and organizational measures to fulfill GDPR requirements, preventing unauthorized access, alteration, transmission, publication, deletion, or destruction. Additionally, it protects against accidental destruction, damage, and technological changes that might impact accessibility.

Both the company and its partners have systems that are safeguarded against computer fraud, viruses, breaches, and denial-of-service attacks. Security is managed with server-level and application-level defenses, and daily data backups are implemented to prevent data loss. In case of an incident, the Data Controller responds immediately to minimize risks and mitigate damages, following its incident management protocol.

13. Data Subject Rights and Remedies

Data subjects have the following rights regarding their personal data and may seek redress if necessary:

Right to Information: Individuals have the right to request detailed information on the processing of their personal data. The company takes appropriate measures to provide clear, accessible, and comprehensive information on personal data processing as required by GDPR Articles 13, 14, and 15–22.

Right to Access: Individuals have the right to confirm whether their personal data is being processed and, if so, to access this data.

Right to Rectification: Any individual may request the correction of inaccurate or incomplete personal data held by the Data Controller.

Right to Erasure (Right to Be Forgotten): Individuals may request the deletion of their personal data if:

The data is no longer necessary for the purposes it was collected or processed for.

Consent is withdrawn, and there is no other legal basis for processing.

The individual objects to the processing and no overriding legitimate grounds exist.

The data was processed unlawfully.

EU or national law requires the deletion of data.

The data was collected in relation to services offered by the information society.

However, deletion requests may not be accepted if the data is necessary for:

Exercising the right to freedom of expression and information.

Compliance with legal obligations of the Data Controller.

Public health, archival, scientific, or statistical purposes.

Establishing, exercising, or defending legal claims.

Right to Restriction of Processing: The individual may request processing restriction under certain conditions, for example, if:

Data accuracy is disputed, for the duration of verification.

Processing is unlawful, but deletion is opposed.

The data is no longer necessary for processing but required for legal claims.

There is a pending decision on the individual's objection to processing.

Restricted data may only be processed under specific circumstances, and individuals will be informed in advance of any change in processing restrictions.

Right to Data Portability: Individuals have the right to receive their personal data in a structured, commonly used, machine-readable format and to transfer this data to another controller. The company can provide data in Word or Excel format upon request.

Right to Object: Individuals may object to data processing for direct marketing purposes, including profiling, at any time. Upon objection, personal data will not be processed for such purposes.

Right to Withdraw Consent: Individuals have the right to withdraw their consent at any time. Withdrawal does not affect the lawfulness of data processing based on consent prior to withdrawal.

Procedural Rules: The Data Controller informs the individual of actions taken in response to a request within 30 days, extendable by two months if necessary, depending on the complexity and number of requests. Electronic responses are provided if the request was submitted electronically unless otherwise requested.

If the Data Controller does not act upon a request, it will inform the individual within one month, explaining the reason and advising on possible remedies with the supervisory authority or through judicial redress.

If data rectification, erasure, or restriction occurs, the Data Controller informs all data recipients unless doing so is impossible or disproportionately difficult. Upon request, the Data Controller will provide details of these recipients to the data subject.

Redress Options:

Individuals may contact the Data Controller directly regarding data processing issues.

Supervisory Authority: Complaints may be submitted to Hungary's National Authority for Data Protection and Freedom of Information (NAIH).

Contact: 1055 Budapest, Falk Miksa utca 9-11.,

Postal Address: 1363 Budapest, Pf.: 9.

Phone: +36-1-391-1400

Email: ugyfelszolgalat@naih.hu

If data processing issues arise, individuals may also pursue civil claims, with cases handled by Hungarian district courts. Cases can be initiated at the court of the individual's residence, with court listings available at <http://birosag.hu/torvenyszekek>.

14. External Service Providers and Data Processors

The Data Controller entrusts certain data processing and technical tasks to external partners. These service providers act under a contractual agreement with the Data Controller and process personal data in compliance with applicable data protection laws.

Web Developer

László Vörös ev.

Address: 6726 Szeged, Izabella 37.

Phone: +36 70/267-2068

Email: info@honlap-profi.hu

Tax number: 66739683-1-26

Activities: Website operation, maintenance, and development.

Purpose of Data Processing: Ensuring the secure operation of the website, troubleshooting technical issues, and enhancing functionality.

The Data Controller ensures that the web developer has access only to the personal data required to perform their tasks and uses the data exclusively for the specified purposes.

Date: Budapest, December 17, 2024