

PRIVACY NOTICE

This Privacy Notice provides information regarding the processing of personal data submitted through the online table reservation platform (Sevenrooms) of Aleli Budapest (operator: Dorottya Étteremüzemeltető Zrt., registered office: 1026 Budapest, Pasaréti út 122-124., hereinafter: Data Controller).

Our aim is to ensure that you are fully informed about the purpose and conditions of data processing, the associated risks and safeguards, as well as your rights, prior to providing your personal data and giving your consent.

By using the restaurant's online reservation system and/or visiting the restaurant, you, as a visitor (hereinafter: Data Subject), acknowledge and accept the provisions of this Notice, confirm that you have read and understood the information contained herein, and consent to the processing of your personal data.

The purpose of this Privacy Notice is to inform Data Subjects about how the Data Controller uses the personal data obtained in the context of visiting the restaurant, which are processed on the basis of the Data Subject's consent or the Data Controller's legal obligations, and, in some cases, shared for specific processing purposes. Data processing is carried out exclusively based on personal data voluntarily provided by the Data Subjects and their prior consent, in connection with their visit to the restaurant.

By issuing this Privacy Notice, our companies aim to comply with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 — on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter: the Regulation, GDPR) — as well as with the provisions of Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information (hereinafter: Infotv.).

Our companies are committed to providing Data Subjects with all information related to the processing of personal data in a concise, transparent, intelligible and easily accessible form, using clear and plain language, and to facilitating the exercise of Data Subjects' rights.

The terms used in this Notice correspond to the definitions and interpretations set out in the Infotv. and the Regulation.

1. IDENTIFICATION OF PARTIES INVOLVED IN DATA PROCESSING AND THEIR RESPONSIBILITIES

Name	Role	Contact Information
Dorottya Étteremüzemeltető Zrt.	Data Controller	1026 Budapest, Pasaréti út 122–124., Hungary
BDPST Koncept Kft.	Data Processor – Event management, online and social media platforms management, and website administration	1026 Budapest, Pasaréti út 122–124., Hungary
SevenRooms Ltd.	Data Processor – Provider of the online reservation system	228 Park Ave South, PMB 33706, New York, NY 10003, USA
BDPST Hotel Management Zrt.	Data Processor – Sales promotions and newsletter distribution	1026 Budapest, Pasaréti út 122–124., Hungary
Stripe Inc.	Payment service provider for card transactions	354 Oyster Point Boulevard, South San Francisco, CA 94080, USA

Corient Accounting Kft.	Data Processor – Accounting and invoicing	1026 Budapest, Pasaréti út 122–124., Hungary
--------------------------------	---	--

In the course of operating the table reservation system, the Data Controller reserves the right to charge a cancellation fee to guests who cancel their reservation less than 24 hours prior to the reserved time or who fail to appear at the restaurant at the scheduled time without prior notice to the Data Controller.

The amount of the cancellation fee is HUF 15,000 per person, which will be charged to the payment card provided during the reservation process. The Data Controller does not process payment card data; such data is provided through Stripe, Inc.'s secure payment system, which uses the card information exclusively for the execution of the transaction. The Data Controller only receives a notification regarding the outcome of the transaction (e.g. successful charge).

The cancellation fee is applied solely under the conditions described above, based on predefined terms established by the Data Controller, which are clearly made available to and accepted by the guest during the reservation process.

Please note that personal data provided during the payment transaction—particularly payment card data—are transferred to Stripe, Inc., a data controller established in the United States of America (a third country outside the European Union). Stripe carries out such data transfers on the basis of the Standard Contractual Clauses (SCCs) approved by the European Commission, thereby ensuring an adequate level of protection for the personal data.

For the operation of the table reservation system, Dorottya Étteremüzemeltető Zrt. engages the services of SevenRooms, Inc. (228 Park Avenue South, PMB 33706, New York, NY 10003, USA) as a data processor. The processing of personal data is carried out under a data processing agreement, in accordance with the instructions of Dorottya Étteremüzemeltető Zrt. SevenRooms, Inc. is certified under the EU–U.S. Data Privacy Framework (EU–US DPF), thereby meeting the safeguards required by the GDPR for international data transfers to third countries.

Personal data are not used by SevenRooms for its own purposes; the service provider acts solely on behalf of the restaurant and in accordance with its instructions.

The data processors do not use the provided data for their own purposes; they process the data exclusively on behalf of the Data Controller.

By accepting this Privacy Notice during the online reservation process, the Data Subject explicitly consents to the Data Processor engaging additional sub-processors for the purpose of enhancing and personalizing the service experience, as follows.

SevenRooms Ltd., the Data Processor, is based in the United States, which constitutes a third country under the GDPR. However, SevenRooms Ltd. has incorporated the Standard Contractual Clauses (SCCs) approved by the European Commission into the data protection addendum to its standard terms and conditions. As a result, the transfer of personal data to SevenRooms Ltd. is deemed to provide appropriate safeguards even without prior authorization from a supervisory authority, and there are no legal obstacles to such data transfer.

2. CATEGORIES OF PERSONAL DATA PROCESSED, PURPOSES OF PROCESSING, AND LEGAL BASIS

Personal Data Processed	Purpose of Processing	Legal Basis of Processing
Name, email address, phone number	Communication and providing information related to table reservations	GDPR Article 6(1)(a): the Data Subject has given consent to the processing of their personal data for one or more specific purposes

	Sending notifications, newsletters, and updates about future events, promotions, and plans	GDPR Article 6(1)(a): the Data Subject has given consent to the processing of their personal data for one or more specific purposes
Image (video surveillance footage)	Operation of the restaurant's security camera system for safety, life and property protection purposes	GDPR Article 6(1)(f): processing is necessary for the purposes of the legitimate interests pursued by the Data Controller or by a third party
Name, address, and invoicing details	Issuing and managing invoices	GDPR Article 6(1)(c): processing is necessary for compliance with a legal obligation to which the Data Controller is subject, pursuant to Act C of 2000 on Accounting, Section 169

5. RIGHTS OF THE DATA SUBJECT

RIGHT TO TRANSPARENT INFORMATION

You have the right to be informed about the facts and circumstances of the data processing prior to its commencement. This Privacy Notice was created in part to fulfil this right.

RIGHT OF ACCESS

The Data Subject has the right to obtain confirmation from the Data Controller as to whether or not personal data concerning them are being processed, and, where that is the case, access to the following information:

- the personal data being processed and the categories of such data;
- the purposes of the processing;
- the recipients or categories of recipients to whom the personal data have been or will be disclosed;
- the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period.

RIGHT TO RECTIFICATION

The Data Subject has the right to request the rectification or completion of personal data that are inaccurate, incorrect, or incomplete. Before correcting inaccurate data, the Data Controller may verify the accuracy and authenticity of the data in question.

RIGHT TO WITHDRAW CONSENT

Where processing is based on consent, the Data Subject has the right to withdraw that consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.

RIGHT TO ERASURE (“RIGHT TO BE FORGOTTEN”)

The Data Subject has the right to request the erasure of personal data concerning them without undue delay, and the Data Controller is obliged to erase such data. This right does not apply where the processing is based on a legal obligation.

RIGHT TO RESTRICTION OF PROCESSING

The Data Subject has the right to obtain from the Data Controller restriction of processing where one of the following applies:

- the accuracy of the personal data is contested by the Data Subject, for a period enabling the Data Controller to verify the accuracy of the personal data;
- the processing is unlawful and the Data Subject opposes the erasure of the personal data and requests the restriction of their use instead;
- the Data Controller no longer needs 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;
- the Data Subject has objected to processing, pending the verification whether the legitimate grounds of the Data Controller override those of the Data Subject.

RIGHT TO DATA PORTABILITY

The Data Subject has the right to receive the personal data concerning them, which they have provided to the Data Controller, in a structured, commonly used and machine-readable format, and has the right to transmit those data to another controller without hindrance from the controller to which the personal data were originally provided.

This right applies where:

- the processing is based on the Data Subject's consent (including consent for the processing of special categories of personal data for one or more specific purposes) or on a contract pursuant to Article 6(1)(b) of the GDPR; and
- the processing is carried out by automated means.

RIGHT TO OBJECT

The Data Subject has the right to object, on grounds relating to their particular situation, at any time to the processing of personal data concerning them, where the processing is based on the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, or where the processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, including profiling based on those grounds.

The Data Controller shall no longer process the personal data unless it demonstrates 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.

6. REMEDIES AVAILABLE TO THE DATA SUBJECT

We encourage you to contact us first—we are committed to resolving any issues you may have.

If you are not satisfied with our response, or prefer not to contact us, you have the right to lodge a complaint with the data protection supervisory authority, or to seek a judicial remedy.

Supervisory authority in Hungary:

Hungarian National Authority for Data Protection and Freedom of Information

Mailing address: 1363 Budapest, Pf. 9.

Office address: 1055 Budapest, Falk Miksa utca 9–11.

Phone: +36 (1) 391-1400

Fax: +36 (1) 391-1410

Email: ugyfelszolgalat@naih.hu

Website: <https://naih.hu>

Right to bring proceedings before a court:

If you believe that your rights under the GDPR have been infringed, you are entitled to bring an action against the Data Controller before a court. You may choose to initiate the proceedings before the court of your place of residence or habitual residence.

7. DATA SECURITY MEASURES

We are committed to protecting personal data from loss, unlawful use, unauthorized disclosure, alteration, unavailability, or destruction, and we take all necessary measures to preserve the confidentiality of personal data, including the implementation of appropriate technical and organisational measures.

Organisational measures include physical access control at our premises, staff training, and secure storage of paper-based records in restricted areas. Technical measures include encryption related to access to our systems, password protection, and the use of antivirus software.

As part of the process through which you provide us with your personal data, such data may be transmitted over the internet. While we take all necessary precautions to protect the personal data you share with us, data transmission over the internet cannot be considered completely secure. Accordingly, you acknowledge and accept that we cannot assume full responsibility for the security of data transmitted via our website, and that such transmission is at your own risk. Once your personal data are received by our systems, we apply strict procedures and security features to prevent unauthorised access.

If we have provided you (or if you have chosen) a password that enables access to certain parts of our services, you are responsible for keeping this password confidential. We kindly ask you not to share this password with anyone.

Our websites and social media platforms may from time to time contain links to websites operated by third parties, including those of affiliated companies or partner networks. The processing of data on such websites is not governed by this Privacy Notice and falls outside the scope of our activities.

8. HANDLING AND REPORTING DATA BREACHES

A personal data breach refers to any event involving personal data that are processed, stored, transmitted, or otherwise handled by the Data Controller, which results in the unlawful processing of such data—particularly their unauthorised or accidental access, alteration, disclosure, erasure, loss, destruction, or accidental damage.

The designated data protection officer shall investigate any reported or observed data breach without delay and, within 24 hours of becoming aware of the incident, shall make a recommendation on how to remedy and manage the breach.

The Data Controller ensures that all data processing activities are conducted in full compliance with the applicable legal requirements.

Date of issue: 22 May 2025