# PRIVACY POLICY

The Om Sai Kft. (hereinafter referred to as the "Data Controller") operates the website available under the domain name haveli.hu (hereinafter referred to as the "Website").

By starting to use the Website, the user (hereinafter referred to as the "User") accepts all the terms and conditions contained in this Data Privacy Policy (hereinafter referred to as the "Policy"). Therefore, please read this Policy carefully before starting to use the Website.

## I. Processing of Data Expressly Provided by Users

### I.1. Data of the Data Controller

Om Sai Limited Liability Company
Mailing address: 1063 Budapest, Szinyei Merse u. 1.
Company registration number: 01-09-195-642
Tax identification number: 25029358-2-42
Contact: haveli@haveli.hu, +36 1 426 4897

### I.2. Scope of Processed Data

When using the Website to place an order, the User needs to provide the following personal information:
Full name
Email address
Phone number
Delivery address (ZIP code, city, street name, house number)

The Data Controller declares that no card data required for payment transactions with bank cards or SZÉP cards are processed, collected, stored, or accessed in any way. These data are handled by the service provider offering the option of card payment.

Only individuals who have reached the age of 18 are authorized to provide data on the Website.

### I.3. Purpose and Duration of Data Processing

In connection with providing services available on the Website, the Data Controller uses the data for the following purposes:
- During the use of the Website (placing an order): The purpose of data processing is to ensure the provision of services available on the Website, manage the database related to the operation of the website, and transmit the data to the Data Controller for the purpose of fulfilling orders.

The Data Controller processes personal data until the purpose of data processing exists, i.e., until the order is fulfilled. Personal data is deleted simultaneously with the cessation of the purpose of data processing or upon the User's request, except for data that the Data Controller is required by legislation to retain for a specified period based on mandatory data processing as stipulated in the relevant legislation.

### I.4. Data Transmission

The Data Controller only transmits the User's data (name, email address) to the payment service provider for card payments or SZÉP card payments. The User's data is not transmitted to any other third party.

### I.5. Legal Basis for Processing Personal Data

Users can provide only their own personal data on the Website. If they provide personal data that does not belong to them, the data provider will delete the User's data.

I.6. Range of Authorized Persons for Access to Personal Data, Data Processing

The Data Controller, as well as the data processors used by them, are entitled to access personal data in accordance with applicable legal regulations.

Data processing is carried out by the Data Controller.

The Data Controller reserves the right to involve further data processors in data processing in the future, which will be notified to Users by amending this Policy.

In the absence of express legal provisions, the Data Controller shall only transfer data suitable for the identification of the User to third parties with the explicit consent of the respective User.

I.7. User's Rights

Upon request, the Data Controller provides information about the personal data it processes, their source, the purpose of data processing, the legal basis, the duration, the name and address of the data processor, and the activities related to data processing. In the case of data transfer, the legal basis and the recipient of the data transfer are also provided. Requests for information can be made to the Data Controller's contact details, with identity verification and providing a mailing address. The Data Controller will respond in writing within a maximum of 25 days from the receipt of the request.

The User has the right to request the correction of their personal data (specifying the correct data) at any time, using the Data Controller's contact details, with identity verification and providing a mailing address. The Data Controller will promptly correct the data in its records and inform the data subject in writing.

In addition to the above, the User can request the deletion or blocking of their data - in whole or in part - at any time, free of charge and without giving a reason, using the Data Controller's contact details, with identity verification and providing a mailing address. Upon receiving a deletion request, the Data Controller immediately terminates data processing and deletes the User from the records.

If the Data Controller does not fulfill the User's request for correction or deletion, within 25 days from the receipt of the request, it will inform the User in writing of the factual and legal reasons for rejecting the request. In case of rejection of the request for correction or deletion, the Data Controller will inform the User about the possibility of judicial remedies and the option to turn to the National Authority for Data Protection and Freedom of Information.

I.8. Handling and Reporting of Data Breaches

A data breach is considered to be any event that results in the unlawful processing or processing of personal data managed, transmitted, stored, or processed by the Data Controller, particularly involving unauthorized or accidental access, alteration, disclosure, deletion, loss, or destruction, as well as accidental destruction and damage of personal data.

The Data Controller shall, without undue delay, but no later than 72 hours after becoming aware of the data breach, report the data breach to the National Authority for Data Protection and Freedom of Information, except if the Data Controller can prove that the data breach is unlikely to result in a risk to the rights and freedoms of natural persons. If the report cannot be made within 72 hours, the reasons for the delay must be indicated, and the required information can be provided in stages without undue delay. The report to the National Authority for Data Protection and Freedom of Information includes at least the following information:
- The nature of the data breach, the number and category of data subjects and personal data;
- The name and contact details of the Data Controller;
- The likely consequences of the data breach;
- Measures taken or planned to address, remedy, or mitigate the data breach.

The Data Controller shall inform the data subjects about the data breach within 72 hours of becoming aware of the data breach through the Data Controller's website. The notification must include at least the information specified in this section.

The Data Controller keeps a record of data breaches for the purpose of monitoring the measures taken in connection with data breaches and informing the data subjects. The record includes the following information:
- The scope of personal data of the data subjects;
- The number of data subjects;
- The date of the data breach;
- Circumstances and consequences of the data breach;
- Measures taken to remedy the data breach.

The data recorded in the register is kept for 1 year from the detection of the data breach.

I.9. Card Payment

I acknowledge that the following personal data(name, email address) stored by the Data Controller in the user database of the Website will be transferred to OTP Mobil Ltd as data processor can be found in the SimplePay Data Processing Information Notice, available at the following link: https://simplepay.hu/adatkezelesi-tajekoztatok

I.10. SZÉP Card Payment

In the case of MBH (MKB) SZÉP card:
MBH and MKBSZÉP card transactions are jointly provided by MBH Pension Fund, and online payments are facilitated by Jasmine Financial Services Ltd., serving as "financial service providers" according to Act 2013:CCXXXVII.
The web payment interface does not request or handle any personal data (name, email address).
The card numbers pass through the web payment system for the necessary duration of transactions, but they are not stored or archived in a long-term database.
The communication of web payments is secured by the Microsec e-Szignó certificate.

II. Other Information Collected in Connection with Website Use - Cookies

II.1. What Information Do We Collect in Connection with Website Use?

If the User does not explicitly provide personal information about themselves as described in Part I on the Website, the Data Controller does not collect or process any personal data about the User in a way that would allow them to be personally identified.

By visiting the Website and pressing the "Accept" button, every User consents to the Data Controller recording the data and information described in Part II of this Policy and placing the necessary cookies for recording.

Such data includes the data of the User's logging computer generated during the use of the Website and automatically recorded by the Data Controller's system as a result of technical processes. The data that is automatically recorded is logged when the User visits or exits the Website, without any separate statement or action by the User.

This data is not linked to other personal user data, and the User cannot be identified based on this data. Only the Data Controller and the data processors they engage have access to this data. This data can be collected using various technologies, including cookies, web beacons, and log files.

These data include the following information:

Cookies: Cookies are short text files sent by the website to the User's computer's hard drive and contain information about the User. Log files: The web browser automatically transmits certain other data to the website, such as the User's computer's IP address (e.g., 222.110.20.20), the type of operating system and browser program used by the User, the domain name from which the User visited the website, and the subpages visited by the User within the website, the

content viewed on the website.

Similar to other internet service providers, the Data Controller analyzes this data to determine which areas of the Website are more popular than others. Furthermore, like other major service providers, the Data Controller uses this data to tailor the website experience to the user's needs.

II.3. How Do We Use This Information?

The data collected through the aforementioned technologies cannot be used to identify the User, and the Data Controller does not associate this data with any other data that may be suitable for identification.

The primary purpose of using this data is to enable the Data Controller to operate the Website properly. This includes tracking visitation data on the Website and identifying potential misuse of the Website. The data specified in this notice is also used to tailor the user's personal preferences (e.g., most frequently viewed content on the Website).

In addition to the above, the Data Controller may use this information to analyze usage trends, improve and develop the Website's features, and obtain comprehensive traffic data regarding the complete use of the Website.

The Data Controller may use the information obtained in this way to compile and analyze usage statistics related to the Website and may disclose non-identifying statistical data (e.g., visitors, most viewed content) to third parties, or make it public in an aggregated, anonymous form.

II.4. Option to Disable Cookies

If you do not want the Data Controller to collect information about you related to the use of the Website as described above, you can partially or completely disable the use of cookies in your internet browser settings or otherwise modify the cookie message settings.

However, in this case, you accept that certain services displayed on the Website will not be available or may not be available in the same way as they would be with cookies enabled, and the User experience on the Website cannot be provided to the same extent by the Data Controller.

However, in such cases, you accept that certain services displayed on the Website will not be available or may not be available in the same way as they would be with cookies enabled, and the User experience on the Website cannot be provided to the same extent by the Data Controller.

II.5. Cookies Placed by Third Parties

The Website may contain information, especially advertisements, originating from third parties or advertising providers unrelated to the Data Controller. These third parties may also place cookies, web beacons on the User's computer, or use similar technologies to collect data in order to send targeted advertising messages to the User in connection with their own services. In such cases, the data protection requirements determined by these third parties shall apply, and the Data Controller assumes no responsibility for such data processing.

III. Data Security

The Data Controller undertakes to ensure the security of data, takes technical and organizational measures, and establishes procedural rules to ensure that the data collected, stored, or processed are protected and to prevent their destruction, unauthorized use, and unauthorized alteration. The Data Controller also undertakes to instruct all third parties to whom data is transmitted or disclosed based on User consent to comply with data security requirements.

The Data Controller ensures that unauthorized persons cannot access, disclose, transmit, modify, or delete the processed data. Only the Data Controller and their employees and data processors they engage can access this data. The Data Controller ensures that the data is not accidentally damaged or destroyed. The above commitment is also imposed by the Data Controller on the employees involved in data processing.

The User acknowledges and accepts that when providing personal data on the Website – despite the Data Controller having modern security measures to prevent unauthorized access to data or their decryption – data protection on the Internet cannot be guaranteed in full. The Data Controller is not responsible for any data acquisition or unauthorized access of any kind or any damage to the User due to unauthorized access or data disclosure. Furthermore, the User may disclose their personal data to third parties who may use them for unlawful purposes.

Under no circumstances does the Data Controller collect special data, i.e., data that relate to racial or ethnic origin, political opinion or affiliation, religious or philosophical beliefs, membership in interest representation organizations, health, pathological addiction, sexual life, or criminal record.

In terms of data security, it is important that when using the Internet on public computers, you should always delete data stored on the Website after use (Cart menu Delete button). If you visit our site from your own computer, it may remain stored for a certain period depending on the application. In this case as well, be cautious that strangers cannot access your computer and perform transactions (orders, etc.) on your behalf.

IV. Enforcement of Rights

The Data Controller does everything in its power to ensure that the handling of personal data complies with the applicable laws. If you feel that we have not met these requirements, please contact us at one of the Data Controller's contact details.

If you feel that your right to data protection has been violated in accordance with applicable laws, you may seek legal redress with the competent authorities: the National Authority for Data Protection and Freedom of Information (address: 1125 Budapest, Szilágyi Erzsébet fasor 22/C.) or the court.

The National Media and Infocommunications Authority is responsible for electronic advertisements, and detailed regulations can be found in Act CXII of 2011 on the Right to Information Self-Determination and Freedom of Information and Act CVIII of 2001 on Certain Issues of Electronic Commerce Services and Information Society Services.

V. Other Provisions

This Notice is governed by Hungarian law, especially the provisions of Act CXII of 2011 on the Right to Information Self-Determination and Freedom of Information.

The Data Controller reserves the right to unilaterally amend this Notice at any time with prior notice to data subjects.

2023.10.19