PRIVACY POLICY

For Website Visitors

The Data Controller pays special attention to ensuring that the processing of personal data within its system complies with the provisions of Regulation (EU) 2016/679 of the EUROPEAN PARLIAMENT AND OF THE COUNCIL ("Regulation") on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, as well as repealing Directive 95/46/EC (General Data Protection Regulation - GDPR).
In relation to data processing, the Data Controller hereby informs website visitors (hereinafter referred to as "User") about the personal data processed, the principles and practices followed in the processing of personal data, as well as the manner and possibilities for exercising User rights.
The User is entitled to partially or fully withdraw consent to data processing or request the deletion of their data via a written request addressed to the Data Controller in accordance with the procedure set out in this notice.

1. IDENTIFICATION OF THE DATA CONTROLLER

- The data is processed by Sportfive MPA Kft.
  - **Name:** Sportfive MPA Kft.
  - **Registered office:** 1091 Budapest, Üllői út 133-135.
  - **Company registration number:** 01-09-402227
  - **Tax number:** 32005781-2-43
  - **Email:** mvmdome@sportfive.com
  - **Website:** www.mvm-dome.hu, www.mvmdome.funcode.hu
- **Contact details of the Data Protection Officer:**

  - **Name:** Dr. Malich Adrienn
  - **Address:** 1091 Budapest, Üllői út 133-135.
  - **Email:** mvmdome@sportfive.com

2. DATA PROCESSING CASES

- Users can purchase tickets for cultural and sports events, as well as parking tickets, through the Website. These tickets can be purchased without registration (guest checkout). However, some tickets require Users to be redirected to the ticket sales platform of a Partner that has a contractual relationship with the Data

Controller. In such cases, the User purchases the ticket directly from the Partner via the Partner's website, and not from the Data Controller.

- For such purchases, the User provides personal data directly on the Partner's website, and the data processing is governed by the data processing policies available on the respective Partner's website. The Data Controller does not receive any personal data from the Partner but is notified about the ticket number sold, solely for the purpose of enabling the User's entry into MVM-DOME.

2.1. Registration on the Website

The email address provided during registration does not necessarily have to contain personal data. For example, it does not need to include the User's name. The User may choose an email address that does not reveal their identity.

Services available for purchase through the Website (e.g., concert tickets, parking tickets) do not require registration. However, Users have the option to register using the methods below.

If a User purchases a ticket sold by a Partner rather than directly by MVM DOME, they will be redirected from the Website to the Partner's page to complete the purchase. The Partner does not share User data with the Data Controller, and all personal data processing is subject to the Partner's data processing notice available on their website.

2.1.1. Registration Using an Email Address on the Website

Processed Data	Purpose of Data Processing
Name	User identification
Email	Contact and password retrieval
Password	Ensuring secure access

If a User places an order after registration, providing billing details is mandatory so that the Data Controller can fulfill its legal obligations specified in Section 2.6.

Purpose of Data Processing: Registration provides a convenience feature, allowing Users to avoid re-entering necessary purchase details for future transactions.

Duration of Data Processing: Personal data required for registration is processed from the time of registration until the User requests deletion. If the User does not request deletion, the Data Controller will delete their personal data from the system no later than 30 days after the termination of the Website.

Legal Basis for Data Processing: User's voluntary consent under Article 6(1)(a) of the Regulation.

Source of Data: Directly provided by the User.

Consequences of Not Providing Data: Users can still complete purchases as a guest without registration. Lack of registration does not result in any disadvantage for the User.

2.1.2. Login/Registration with Google Account

If the User has a Google account, they can log in by clicking the "Sign in with Google" button or register by clicking the "Register with Google" button to make purchases or use services on the Website.

Scope of Data Processed and Purpose of Data Processing:

When logging in with a Google account, the Data Controller processes the following data:

Processed Data	Purpose of Data Processing
User's unique identifier	User identification
Email	Communication and password delivery

The User is redirected to the external service provider's login page, where they can log in to the Data Controller's site using the credentials previously registered on the Google platform. The Data Controller does not have access to or store the entered password details.

Further purpose of data processing: Ensuring that the User can register/log in to the MVM Dome registration platform using their existing Google account details.

Legal basis for data processing: The User's voluntary consent based on Article 6(1) (a) of the Regulation.

Duration of data processing: The processing of personal data required for registration begins with the registration and lasts until the User requests its deletion. If the User does not request the deletion of their registration, the Data Controller will delete the User's personal data no later than 30 days after the Website ceases to exist.

Source of data: Directly collected from the User.

Consequence of not providing data: The User can place an order without using a Google account (as a guest), and the lack of registration does not result in any disadvantageous legal consequences for the User.

2.1.3. Login/Registration with Facebook Account

If the User has a Facebook account, they can register by clicking the "Register with Facebook" button or log in by clicking the "Sign in with Facebook" button. In this case, the User is redirected to the external service provider's login page, where they can log in to the Data Controller's site using the credentials previously registered on the Facebook platform. The Data Controller does not have access to or store the entered password details. Registration is not mandatory in this case either.

Scope of Data Processed and Purpose of Data Processing:

When logging in/registering with a Facebook account, the Data Controller receives the following data:

Processed Data	Purpose of Data Processing
User's name	User identification
User's unique identifier	User identification
Email	Communication and password delivery

Further purpose of data processing: Ensuring that the User can register/log in to the MVM Dome registration platform using their existing Facebook account details.

Legal basis for data processing: The User's voluntary consent based on Article 6(1) (a) of the Regulation.

Duration of data processing: The processing of personal data required for registration begins with the registration and lasts until the User requests its deletion. If the User does not request the deletion of their registration, the Data Controller will delete the User's personal data no later than 30 days after the Website ceases to exist.

Source of data: Directly collected from the User.

Consequence of not providing data: The User can place an order without using a Facebook account (as a guest), and the lack of registration does not result in any disadvantageous legal consequences for the User.

2.1.4. Deletion of Registration

The User can request the deletion of their registration by sending a deletion request to the Data Controller. Upon receiving the request, the Data Controller will promptly delete the User's account along with all personal data. However, the deletion does not affect the retention of invoices related to already placed orders or data required for fulfilling legal obligations of the Data Controller (e.g., retaining complaints for three years).

Once the registration is deleted, data restoration is no longer possible.

2.2. Guest Checkout

Scope of Data Processed and Purpose of Data Processing:

Processed Data	Purpose of Data Processing
Name	User identification
Address	Required for invoice issuance
Email	Communication, invoice delivery, and event-related information
Place and date of birth	User identification
Ticket/Pass type, purchase date, validity period	Linking the purchased ticket/pass to the User and ensuring its use at a specific event and time
Online food/drink order	See section 5 for details

Further purpose of data processing: Ensuring that the User can place an order for a product or service available on the Website without registration.

Legal basis for data processing: Performance of contract under Article 6(1)(b) of the Regulation.

Duration of data processing: Personal data provided during the order process will be processed for 5 years from the completion of the order.

Source of data: Directly collected from the User.

2.3. Request for Quotation

Scope of Data Processed and Purpose of Data Processing:

Processed Data	Purpose of Data Processing
Name	User identification
Email	Communication regarding the quotation request
Service specification	Subject of the quotation request

The legal basis for data processing is the User's voluntary consent under Article 6(1)(a) of the Regulation. If a contract is concluded between the Data Controller and the User as a result of the quotation request, the legal basis for data processing will be the performance of the contract under Article 6(1)(b) of the Regulation.

Duration of data processing: Personal data provided in the quotation request will be processed for 2 months from the submission of the request. If a contract is concluded, personal data will be processed for 5 years from the completion of the order.

Source of data: Directly collected from the User.

2.4. Parking Ticket Purchase

Scope of Data Processed and Purpose of Data Processing:

Processed Data	Purpose of Data Processing
Name	User identification, order fulfillment

Processed Data	Purpose of Data Processing
Email	Communication and email delivery of the purchased parking ticket
Parking ticket purchase date	Ensuring the use of the purchased parking ticket at the specified time
Address details (postal code, city, street, house number)	Required for invoicing

Parking tickets can be purchased without registration.

Legal basis for data processing: Performance of contract under Article 6(1)(b) of the Regulation.

Duration of data processing: Data related to parking ticket purchases will be processed as long as the User's registration remains active, as all parking ticket-related information remains accessible in the User's account. If the User requests the deletion of their registration, the provisions set out in section 2.1.4 shall apply.

Source of data: Directly collected from the User.

Consequence of not providing data: The User cannot purchase a parking ticket without providing personal data.

1.1. Számla kiállítása a megrendelésről

Kezelt adatok köre, adatkezelés célja:

Személyes adat	Adatkezelés célja
Név (vezetéknév, keresztnév)	felhasználó azonosítása, számla kötelező tartalmi eleme.
Cím adatok (irányítószám, város, utca, házszám)	számla kötelező tartalmi eleme.
Cégek esetén adószám	számla kötelező tartalmi eleme.

Adatkezelés célja**:** számlázási kötelezettség teljesítése és számviteli alapelveknek való megfelelés, könyvelés előkészítése, nyilvántartása.

Adatkezelés jogalapja**:** a Rendelet 6. cikk (1) bekezdés c) pontja értelmében jogi kötelezettség teljesítése. (Áfa tv. / 2007. évi CXXVII. törvény az általános forgalmi adóról)

Adatkezelés időtartama: a számla megőrzésére 8 évig kerül sor.

A személyes adatok címzettjeinek kategóriái: adóhatóság, szükség esetén és megkeresés esetén egyéb hatóságok, bíróságok.

Adatok forrása: közvetlenül a Felhasználótól felvett.

Adatkezelés elmaradásának következménye: Adatkezelő a hatályos magyar jogszabályokban meghatározott jogi kötelezettségét nem tudja teljesíteni.

2.5. Invoice Issuance for Orders

Scope of Data Processed and Purpose of Data Processing:

Personal Data	Purpose of Data Processing
Name (first and last)	User identification, mandatory invoice element
Address (postal code, city, street, house number)	Mandatory invoice element
Tax number (for companies)	Mandatory invoice element

Purpose of data processing: Fulfillment of invoicing obligations, compliance with accounting principles, preparation and record-keeping of bookkeeping.

Legal basis for data processing: Compliance with a legal obligation under Article 6(1)(c) of the Regulation. (VAT Act / Act CXXVII of 2007 on Value Added Tax)

Duration of data processing: The invoice will be retained for 8 years.

Recipients of personal data: Tax authorities, and if necessary, other authorities or courts upon request.

Source of data: Directly collected from the User.

Consequence of not providing data: The Data Controller will be unable to fulfill its legal obligations under Hungarian law.

2.6. Data Processing Related to Invoice Sending

Scope of Data Processed and Purpose of Data Processing:

Personal Data	Purpose of Data Processing
Name (first and last)	User identification
Email address	Sending the invoice to the User

Duration of data processing: The Data Controller uses the **szamlazz.hu** system for issuing and sending invoices. Through this system, invoices are sent, and the system retains the User's email address for **8+1 years** as specified in the **szamlazz.hu** data protection notice.

Legal basis for data processing: Compliance with a legal obligation under Article 6(1)(c) of the Regulation. (Act C of 2000 on Accounting)

Source of data: Directly collected from the User.

Consequence of not providing data: The Data Controller will be unable to fulfill its obligation to provide the invoice to the User.

2.7. Customer Correspondence, Contact, and Inquiry Handling

Scope of Data Processed and Purpose of Data Processing (depending on the communication platform):

Personal Data	Purpose of Data Processing
Name (first and last)	User identification
Email address	Contact and communication regarding the inquiry
Phone number	Contact regarding the inquiry
Other (optional) data provided by the User	Additional information that may be necessary for responding to the inquiry (optional)

Further purpose of data processing: If the User has any questions regarding the Website or the services of the Data Controller, they can contact the Data Controller via the contact form on the Website or other available communication channels. The purpose is to enable communication between the Data Controller and the User regarding the inquiry.

Duration of data processing: The Data Controller retains incoming emails and postal letters, including the sender's name, email address, and any other personal

data provided in the message, until the User's inquiry or concern has been resolved or answered.

Legal basis for data processing: The User's voluntary consent under Article 6(1)(a) of the Regulation.

Source of data: Directly collected from the User.

Potential consequences of not providing data: The User will not be able to communicate with the Data Controller via customer correspondence.

2.8. Complaint Handling

Scope of Data Processed and Purpose of Data Processing (depending on the communication platform):

Personal Data	Purpose of Data Processing
Name (first and last)	User identification
Email address	Contact and communication regarding the complaint
Phone number	Contact regarding the complaint
Other (optional) data provided by the User	Additional data provided by the User in the complaint, which may be necessary for investigation

Purpose of data processing: If the Data Controller handles the User's complaint related to the provided service, personal data will also be processed during the administration. The purpose of data processing is to handle complaints in accordance with legal requirements and to enable communication between the Data Controller and the User regarding the complaint.

Duration of data processing: According to the Consumer Protection Act (Act CLV of 1997), the Data Controller is required to retain complaints for **3 years**.

Legal basis for data processing: Compliance with a legal obligation under Article 6(1)(c) of the Regulation, as required by the Consumer Protection Act and the Civil Code.

Source of data: Directly collected from the User.

Potential consequences of not providing data: The complaint cannot be handled, as personal data is necessary for the Data Controller to contact the User and address the issue.

2.9. Newsletter Subscription

Scope of Data Processed: First name, last name, email address.

Purpose of data processing: Recording and identifying the User in the newsletter database. Upon subscription, the Data Controller sends personalized **direct marketing** newsletters to the User based on their subscribed services and purchases. Unless otherwise stated, objected to, or unsubscribed, the Data Controller uses the provided personal data to send **service-related updates, promotions, offers, and notifications**.

Duration of data processing: The Data Controller processes these data **until the User unsubscribes** by clicking the unsubscribe link in the newsletter or by requesting removal via email or postal mail. After unsubscribing, the User will no longer receive newsletters or promotional offers. The User may unsubscribe **at any time, without restriction, justification, or cost**.

Legal basis for data processing: The User's **voluntary consent** under Article 6(1)(a) of the Regulation.

Source of data: Directly collected from the User.

Potential consequences of not providing data: The User will not receive newsletters from the Data Controller and will not be informed about promotions, discounts, or offers.

2.10. Direct Marketing and Commercial Communication

Scope of Data Processed: First name, last name, email address, and services used.

Purpose of data processing: The Data Controller **sends direct marketing content** to the User via direct contact. Personal data is used to send **notifications, offers, or feedback requests** regarding services similar to those previously used by the User. The Data Controller only sends **e-DM (electronic direct marketing) messages** when

there is a relevant relationship between the User and the Data Controller, such as the User being an existing customer.

Right to object: The User may object **at any time** to direct marketing communications, and in such cases, the Data Controller **will cease using** the User's data for this purpose.

Legal basis for data processing: Legitimate interest of the Data Controller under Article 6(1)(f) of the Regulation.

Duration of data processing: The Data Controller will continue processing the User's data for direct marketing **until the User objects**.

Source of data: Directly collected from the User.

Potential consequences of not providing data: If the User unsubscribes or objects, they will no longer receive direct marketing communications.

Legitimate Interest Assessment – Direct Marketing Based on Legitimate Interest

The Data Controller conducted a **legitimate interest assessment**, which is available upon request. The conclusion is that the Data Controller's **legitimate interest does not disproportionately infringe upon** the rights of the individuals concerned. The processing of personal data is **necessary** for marketing communications, promotional offers, and notifications. No alternative data processing methods exist that would require fewer personal data.

Since marketing messages are only sent to **customers** who have previously engaged with the Data Controller, they can **reasonably expect** such communications. According to **Recital 47 of the GDPR**, the processing of personal data for **direct marketing purposes may be considered a legitimate interest**.

3. ACCESS TO DATA, DATA SECURITY MEASURES, AND DATA TRANSFER

3.1. Access to Data and Data Transfer

3.1.1. Data Transfer to Authorities

The personal data is accessible to the Data Controller and the employees of the Data Processor of the Data Controller in order to perform their duties.

The Data Controller transfers the personal data it manages to other entities or state authorities only in a manner and for purposes defined by law.

The Data Controller informs the User that courts, prosecutors, investigative authorities, administrative authorities, the National Authority for Data Protection and Freedom of Information, and other bodies authorized by law may request information, data disclosure, or documents from the Data Controller.

The Data Controller will only provide personal data to the authorities if they specify the exact purpose and scope of the data requested, and only to the extent strictly necessary for achieving the purpose of the request.

3.1.2. Data Transfer to Payment Service Providers

If the User chooses to pay by bank card, they will be redirected from the Website to the SimplePay payment system operated by OTP Mobil Kft. The Data Controller transfers the following data to OTP Mobil Kft. as the data processor: the payable amount.

OTP Mobil Kft. does not transfer to the Data Controller any personal data necessary for the bank card payment that the User provides during the payment process. The Data Controller only receives information about whether the payment transaction was successful or not. OTP Mobil Kft. acts as a data processor only for the data provided by the Data Controller. Regarding the data entered on the payment page, OTP Mobil Kft. acts as a data controller, as the Data Controller does not receive any of these data in any form.

Purpose of Data Transfer: Conducting bank card payments, informing the User via email about the success or failure of the transaction, and fraud monitoring (a fraud detection system supporting the control of electronic banking transactions) for the protection of the User.

Legal Basis for Data Transfer: Based on Article 6(1)(a) of the Regulation, the User's voluntary consent, as online payment is only possible if the User voluntarily provides their data.

The detailed data processing policy of the SimplePay payment system can be found at the following link: https://simple.hu/adatkezelesi-tajekoztato

3.1.3. Data Transfer for Invoice Issuance

Data transfer occurs during invoice issuance using the billing program (szamlazz.hu) operated by KBOSS.hu Kft. When the Data Controller issues an invoice for a purchase, the invoice is automatically sent electronically (via email) from the szamlazz.hu system.

Data Provided in the Billing System: Name, address, and tax number (for companies).

Purpose of Data Transfer: Issuing an invoice.

Legal Basis for Data Transfer: Based on Article 6(1)(c) of the Regulation, fulfillment of a legal obligation.

3.2. Data Security Measures

The Data Controller takes all necessary measures to ensure data security and protects the data at an adequate level, particularly against unauthorized access, alteration, transfer, disclosure, deletion, or destruction, as well as accidental destruction or damage. The Data Controller ensures data security through appropriate technical and organizational measures.

The IT system of the Website is hosted on the servers of the Data Processor (WIX.com Ltd.).

When processing personal data, the Data Controller selects and operates the IT tools used in the provision of the service in a way that ensures that the processed data:

- is accessible to those authorized (availability);
- is authentic and authenticated (data authenticity);
- remains unchanged (data integrity);
- is protected against unauthorized access (data confidentiality).

During data processing, the Data Controller ensures:

- **Confidentiality:** Protects information so that only authorized persons can access it;

- **Integrity:** Ensures the accuracy and completeness of information and processing methods;
- **Availability:** Ensures that authorized users can access the required information when needed and that the necessary tools are available.

4. DATA PROCESSING

In the course of its activities, the Data Controller may engage data processors in certain cases. Data processors record, manage, and process the personal data transferred to them by the Data Controller in accordance with the Regulation and provide a declaration to the Data Controller regarding this. The data processor is only authorized to execute the instructions and decisions of the Data Controller.

The Data Controller transfers the necessary data based on data processing agreements, following the specified procedures. The Data Controller's data processors have operational locations in Hungary.

Name of Data Processor	Data Processor's Information	Activity of Data Processor
Kboss Kft.	Address: 1031 Budapest, Záhony utca 7/D. Email: info@szamlazz.hu Tel: +36-30-35-44-789 Web: www.szamlazz.hu	Operator of the Szamlazz.hu invoicing program
Showtrade Kft.	Address: 2310 Szigetszentmiklós, Dózsa György köz 3.	Software operation services, ticket sales platform
NU Web System Ltd.	Enterprise House, Lloyd Street North, Manchester, Science Park, Manchester, M15 6SE, United Kingdom	Software operation services
Amazon Web Services EMEA SARL	38 Avenue John F. Kennedy, L-1855, Luxembourg	Database management services
OTP Mobil Kft.	Address: 1143 Budapest, Hungária krt. 17-19. Email: informacio@otpbank.hu Web: https://otpmobil.hu/	Operator of the SimplePay payment system
Google Tag Manager (Googleplex)	1600 Amphitheatre Parkway, Mountain View, CA 94043, USA	Website tracking system
T-Soft	4032 Debrecen, Poroszlay út 6.	ERP system

Name of Data Processor	Data Processor's Information	Activity of Data Processor
Mérnökiroda Kft.		
Adroit Group Kft.	2000 Szentendre, Kőzúzó utca 2. a. ép.	IT development services, data entry
Data Talks AB	Kungsbroplan 3A, 112 27 Stockholm, Sweden	Database management services

5. USER RIGHTS

5.1. Right to Information and Access to Personal Data

The User may request information in writing from the Data Controller through the contact details provided above regarding:

- Which personal data are processed,
- On what legal basis,
- For what purpose,
- From what source,
- For how long.

The Data Controller must also inform the User about when, to whom, and on what legal basis access was granted to their personal data or to whom the data were transferred.

The Data Controller provides the requested information in a widely used electronic format unless the User specifically requests it in writing in a paper format. The Data Controller does not provide verbal information via telephone.

The first copy of the personal data (which can be collected in person at customer service) is provided free of charge. For any additional copies requested, the Data Controller may charge a reasonable fee based on administrative costs. If the User requests the data electronically, the Data Controller provides them via email in a widely used electronic format.

Following the provided information, if the User disagrees with the data processing or the accuracy of the processed data, they may request the correction,

supplementation, deletion, restriction of processing, or object to the processing of their personal data as specified in Section IV. The User may also initiate the procedures described in Section IV.

5.2. Right to Rectification and Supplementation of Processed Personal Data

Upon the User's written request, the Data Controller will correct any inaccurate personal data without undue delay or supplement incomplete data with the content specified by the User.

The Data Controller informs any recipients to whom the personal data have been disclosed about the correction or supplementation unless this is impossible or requires disproportionate effort. The User may request information about these recipients in writing.

5.3. Right to Restriction of Data Processing

The User may request the restriction of data processing in writing if:

- The User disputes the accuracy of the personal data. In this case, the restriction applies for a period allowing the Data Controller to verify the accuracy of the personal data.
- The data processing is unlawful, and the User opposes the deletion of the data, requesting instead the restriction of their use.
- The Data Controller no longer needs the personal data for processing purposes, but the User requires them for the establishment, exercise, or defense of legal claims.
- The User has objected to data processing. In this case, the restriction applies until it is determined whether the Data Controller's legitimate reasons override those of the User.

During the restriction period, personal data, except for storage, may only be processed with the User's consent, for the establishment, exercise, or defense of legal claims, for the protection of another natural or legal person's rights, or for important public interest reasons of the European Union or a member state.

The Data Controller informs the User who requested the restriction before lifting the restriction on data processing.

5. USER RIGHTS

5.1. Right to Information and Access to Personal Data

The User may request information from the Data Controller in writing through the provided contact details. The Data Controller shall inform the User about:

- What personal data is being processed,
- The legal basis for processing,
- The purpose of data processing,
- The source of the data,
- The duration of data processing,

Additionally, the Data Controller shall inform the User about who, when, on what legal basis, and which personal data has been made accessible or transferred.

The Data Controller provides the requested information in a widely used electronic format unless the User requests it in writing on paper. The Data Controller does not provide verbal information over the phone.

The first copy of the personal data (in person at customer service) is provided free of charge. The Data Controller may charge a reasonable fee based on administrative costs for any additional copies requested. If the User requests the copy electronically, the Data Controller shall provide the information via email in a widely used electronic format.

After receiving the information, if the User disagrees with the data processing or the accuracy of the processed data, they may request correction, supplementation, deletion, restriction of processing, or object to the processing under Section IV. They may also initiate the procedures set out in Section IV.

5.2. Right to Rectification and Completion of Processed Personal Data

Upon written request, the Data Controller shall correct any inaccurate personal data specified by the User without undue delay and shall complete incomplete data with the content provided by the User.

The Data Controller shall inform all recipients to whom the personal data has been disclosed about the rectification or completion, except where this proves impossible or requires disproportionate effort. Upon written request, the Data Controller shall inform the User about these recipients.

5.3. Right to Restrict Data Processing

The User may request the restriction of data processing from the Data Controller in writing if:

- The User disputes the accuracy of the personal data, in which case the restriction applies for a period enabling the Data Controller to verify the accuracy of the data,
- The data processing is unlawful, and the User opposes the deletion of the data and requests the restriction of their use instead,
- The Data Controller no longer needs the personal data for processing purposes, but the User requires them for the establishment, exercise, or defense of legal claims,
- The User objects to processing: in this case, the restriction applies until it is determined whether the Data Controller's legitimate grounds override those of the User.

During the restriction period, the Data Controller may only process the personal data with the User's consent, for the establishment, exercise, or defense of legal claims, to protect the rights of another person, or for important public interest reasons of the Union or a Member State. The Data Controller shall inform the User in advance before lifting the restriction.

5.4. Right to Erasure (Right to Be Forgotten)

The Data Controller shall delete the User's personal data without undue delay upon request if any of the following grounds apply:

i. The personal data is no longer necessary for the purposes for which it was collected or otherwise processed,
ii. The User withdraws their consent, and there is no other legal basis for processing,
iii. The User objects to processing based on their specific situation, and there are no overriding legitimate grounds for processing,
iv. The User objects to the processing of their personal data for direct marketing purposes, including profiling related to direct marketing,
v. The personal data has been unlawfully processed,
vi. The personal data was collected in connection with offering information society services directly to children.

The right to erasure does not apply if processing is necessary:
i. For exercising the right to freedom of expression and information,
ii. For public health interests,
iii. For archival purposes in the public interest, scientific or historical research purposes, or statistical purposes, where erasure would render processing impossible or seriously impair it,
iv. For the establishment, exercise, or defense of legal claims.

5.5. Right to Data Portability

If data processing is necessary for contract performance or is based on the User's voluntary consent, the User has the right to receive the data they provided to the Data Controller in a machine-readable format. If technically feasible, they may also request that the Data Controller transmit the data to another controller. This right is limited to data provided by the User and does not apply to other data (e.g., statistics).

The User may:

- Receive their personal data in a structured, widely used, machine-readable format,
- Transmit the data to another data controller,
- Request direct transmission to another data controller if technically feasible.

The Data Controller processes portability requests only in writing via email or postal mail. To fulfill the request, the Data Controller must verify the identity of the User. This right applies only to data provided by the User.

Exercising the right to data portability does not automatically result in data deletion from the Data Controller's systems. The User must separately request data deletion if desired.

5.6. Right to Object to Personal Data Processing

The User may object to the processing of their personal data by submitting a statement to the Data Controller if processing is based on:

- Article 6(1)(e) GDPR (public interest),
- Article 6(1)(f) GDPR (legitimate interests).

If the User exercises the right to object, the Data Controller may no longer process the personal data unless it can demonstrate compelling legitimate grounds that override the interests, rights, and freedoms of the User or are necessary for the establishment, exercise, or defense of legal claims. The Data Controller decides whether such grounds exist and informs the User of its position.

The User may submit an objection in writing (via email or postal mail) or, in the case of newsletters, by clicking the unsubscribe link in the email.

5.7. Exercising Rights of a Deceased User

Within five years after the death of the User, their rights (access, rectification, deletion, restriction, portability, objection) may be exercised by a person designated in an official declaration made by the deceased User. This designation must be recorded in an authentic public document or a private document with full probative value.

If the deceased User has made multiple such declarations to the Data Controller, the latest declaration shall prevail.

If no such declaration was made, the deceased User’s closest relative under the Civil Code (Ptk.) may exercise these rights within five years after the User's death. If multiple close relatives wish to exercise these rights, the first relative to do so shall have priority.

Close relatives include:

- Spouse,
- Direct ascendants and descendants,
- Adopted, step, and foster children,
- Adoptive, step, and foster parents,
- Siblings.

The close relative must provide:

- Proof of the User’s death (death certificate or court ruling),
- Proof of their identity and, if necessary, their relationship to the deceased (official documents).

The designated representative or closest relative shall have the same rights and obligations as the deceased under the Data Protection Act (Infotv.) and GDPR.

Upon written request, the Data Controller shall inform the close relative of any measures taken, except where the deceased explicitly prohibited such disclosure in their declaration.

5.8. Deadline for Fulfilling Requests

The Data Controller shall, without undue delay and no later than within one month from receipt of the request, inform the User of the measures taken. If necessary—taking into account the complexity of the request and the number of requests—this deadline may be extended by a further two months. In such cases, the Data Controller shall inform the User within one month of receipt of the request, providing the reasons for the delay and informing the User of their right to lodge a complaint with the supervisory authority and to seek judicial remedy.

If the User's request is clearly unfounded or excessive (particularly due to its repetitive nature), the Data Controller may charge a reasonable fee for fulfilling the request or refuse to act on the request. The burden of demonstrating the unfounded or excessive nature of the request lies with the Data Controller.

If the User submitted the request electronically, the Data Controller shall provide the information electronically unless the User requests otherwise.

The Data Controller shall inform all recipients to whom the personal data was disclosed of any corrections, deletions, or restrictions on processing, unless this proves impossible or involves disproportionate effort. Upon request, the Data Controller shall inform the User about these recipients.

5.9. Compensation and Damages

Any person who has suffered material or non-material damage as a result of a breach of the Regulation is entitled to receive compensation from the Data Controller or the data processor for the damage suffered. The data processor is only liable for damages caused by processing if it did not comply with obligations under applicable laws that specifically bind data processors, or if it disregarded or acted contrary to the lawful instructions of the Data Controller.

The Data Controller and the data processor are exempt from liability if they can prove that they are in no way responsible for the event causing the damage.

6. LEGAL REMEDIES

The User can exercise their rights by submitting a written request via email or postal mail.

The User cannot exercise their rights if the Data Controller demonstrates that it cannot identify the User. If the User's request is clearly unfounded or excessive (particularly due to its repetitive nature), the Data Controller may charge a reasonable fee for fulfilling the request or refuse to act on it. The burden of proving this lies with the Data Controller. If the Data Controller has doubts about the identity of the natural person making the request, it may request additional information necessary to confirm the identity of the requestor.

Under the Info Act, the Regulation, and the Civil Code, the User may:

- Contact the National Authority for Data Protection and Freedom of Information (1055 Budapest, Falk Miksa Street 9-11; www.naih.hu); or
- Enforce their rights before a court. The lawsuit may be filed at the tribunal of the User's place of residence (for a list of tribunals and their contact information, see: http://birosag.hu/torvenyszekek).

7. HANDLING OF DATA PROTECTION INCIDENTS

A data protection incident is a security breach that results in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data that has been transmitted, stored, or otherwise processed. The Data Controller keeps records of data protection incidents for the purpose of monitoring measures taken, informing the supervisory authority, and notifying Users. These records include the categories of personal data affected, the scope and number of data subjects involved, the time of the incident, its circumstances, its effects, and the measures taken to mitigate it.

In the event of a data protection incident, unless it poses no risk to the rights and freedoms of natural persons, the Data Controller shall notify the User and the supervisory authority without undue delay, and no later than within 72 hours.

8. SECURITY BACKUPS MANAGEMENT

In the scope of its IT security responsibilities, the Data Controller ensures measures that allow for the restoration of data sets, including regular security backups and the separate, secure handling of these backups.

To prevent the loss of electronically stored data, the Data Processor creates security backups of its personal data database regularly, at intervals depending on the system's configuration.

Procedure for deleting security backups: Individual deletions are traceable in an anonymized registry, and automatic deletions are carried out based on system settings.

Access to security backups: Access to security backups is restricted to authorized personnel only. Data is accessible exclusively after proper identification (at least username and password).

9. OTHER PROVISIONS

The Data Controller reserves the right to unilaterally amend this Data Processing Notice after providing prior notice through the website used by the Users. The modifications become effective on the date specified in the notice unless the User objects.

If the User provides third-party data for the purpose of newsletter subscription or any other service, or causes damage in any way during website usage, the Data Controller is entitled to seek compensation from the User.

The Data Controller does not verify the personal data provided. Responsibility for the accuracy of the data provided rests solely with the person who submitted it. By submitting personal data, the User accepts responsibility for ensuring that the data is accurate, pertains to themselves, and that they use services based only on their personal data.

10. LEGAL BASIS FOR DATA PROCESSING

- **Act CXII of 2011** on the right to informational self-determination and freedom of information ("Info Act");

- **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 Directive 95/46/EC ("GDPR");
- **Act XLVIII of 2008** on the basic requirements and certain restrictions of commercial advertising activities;
- **Act V of 2013** on the Civil Code ("Civil Code").

Effective date of this Data Processing Notice: February 10, 2025.