Valid from: July 1, 2025

I. The Data Controller (Service Provider)

Name of the Service Provider:	InterTicket Ltd.
Registered office and postal address:	1139 Budapest, Váci út 99.
Registration authority:	Metropolitan Court as Court of Registration
Company registration number:	Cg. 01-09-736766
Tax number:	10384709-2-41
E-mail address:	interticket@interticket.hu
Website address:	www.jegy.hu
Customer service contact:	Chat application from any page of Jegy.hu
Customer service email address:	interticket@interticket.hu For online events (live broadcast, video): online@interticket.hu
Complaint handling location and contacts:	1139 Budapest, Váci út 99. Balance Building Through Chat application from any page of Jegy.hu interticket@interticket.hu On weekdays 10.00 - 16.00
Hosting service provider name:	T-Systems Data Park
Hosting service provider address:	1087 Budapest, Asztalos Sándor u. 13.
Data protection registration	NAIH-54216/2012.

identifier:	
Data protection officer email:	adatvedelmi.tisztviselo@interticket.hu

II. Data protection policies applied by the Company

1. The Service Provider, as data controller, undertakes that all data processing related to its activities complies with the expectations set forth in this regulation and applicable national legislation, as well as European Union legal acts.
2. Information related to the Service Provider's data processing is continuously available in the footer of the opening page of the Jegy.hu website operated by the Service Provider.
3. The Service Provider is entitled to unilaterally modify the Data Processing Notice. In case of modification of the Data Processing Notice, the Service Provider notifies users of changes by publishing them on the Jegy.hu page. By using the service after the modification takes effect, the user accepts the modified Data Processing Notice.
4. The Service Provider is committed to protecting the personal data of its customers and partners, considering the respect for customers' right to informational self-determination particularly important. The Service Provider handles personal data confidentially and takes all security, technical and organizational measures that guarantee data security. The Service Provider's data processing practice is contained in this data processing notice.
5. The Service Provider's data processing principles are in accordance with applicable data protection legislation, particularly the following:

- 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 (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 (General Data Protection Regulation, GDPR);
- Act V of 2013 - on the Civil Code (Civil Code);
- Act C of 2000 - on accounting (Accounting Act);
- Act LIII of 2017 - on the prevention and combating of money laundering and terrorist financing (AML Act);
- Act CVIII of 2001 - on certain issues of electronic commerce services and information society services (E-commerce Act);
- Act XLVIII of 2008 - on the basic conditions and certain restrictions of commercial advertising activities (Advertising Act).

6. The Service Provider uses personal data based on the legal basis contained in the GDPR and exclusively for specific purposes.
7. The Service Provider undertakes to make a clear, attention-grabbing and unambiguous disclosure before collecting, recording, processing any Personal data of users, informing them about the method, purpose and principles of data collection. In case of mandatory data provision, the legislation ordering the Data processing must also be indicated. The data subject must be informed about the purpose of Data processing and who will process or handle the Personal data.
8. In all cases where the Company wishes to use the provided Personal data for purposes other than the original data collection purpose, it informs the user about this and obtains their prior express consent, or provides them with the opportunity to prohibit such use.

III. Legal basis, purpose and scope of processed data, duration of data processing, persons authorized to access personal data

1. The Service Provider's data processing is based on the following legal bases (GDPR Article 6 (1)):

a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes (voluntary consent);

b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract (contract performance);

c) processing is necessary for compliance with a legal obligation to which the controller is subject (legal obligation);

d) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party (legitimate interest).

2. In case of data processing based on voluntary consent, data subjects may withdraw their consent at any stage of data processing.
3. Persons with no or limited legal capacity may not use services through the Service Provider's system.
4. In certain cases, legislation makes the processing, storage, transmission of a certain scope of provided data mandatory, about which we inform users separately.
5. We draw the attention of those providing data to the Service Provider that if they do not provide their own personal data, it is the data provider's obligation to obtain consent from the data subject.
6. Personal data may only be processed for a specific purpose. Data processing must comply with the purpose of data processing at all stages, data collection and processing must be fair and lawful. Only personal data that is essential for achieving the data processing purpose and suitable for achieving the purpose may be processed. Personal data may only be processed to the extent and for the duration necessary to achieve the purpose. The Service Provider does not use personal data for purposes other than those specified.
7. **Online webshop service (purchase of admission tickets, vouchers, books, audio media, parking tickets, etc.) - purchase transaction, admission, notification (one-time purchase)**

Purpose of data processing: ensuring the provision of webshop service available on the website, handling orders and their fulfillment, documenting purchases and payments, fulfilling accounting obligations. The purpose of data processing is also to identify the user as a ticket buyer, fulfill the ordered service, send related notifications (technical notifications related to the performance, such as performance changes, cancellations, time changes, parking information, etc.), enable payment through payment service providers, maintain user records, distinguish users from each other, transfer admission data to the event organizer, fulfill the contract.

Legal basis for data processing: contract performance, GDPR Article 6 (1) point b).

Scope of processed data: first and last name, phone number (data required by payment service provider, but also enables our customer service or event organizer to immediately notify the ticket buyer in case of possible program, venue, or time changes), email address, password provided during prior registration, delivery address provided when requesting home delivery, transaction number, date and time, customer code, gift voucher number, culture voucher number.

The scope of processed data also includes - in case the admission ticket is issued in a specific name based on the event organizer's decision - the name of the rightful user of the admission ticket and any other personal data possibly required by the event organizer. Considering that the ticket buyer's identity may differ from the rightful user of the admission ticket, if the ticket buyer does not provide their own personal data, by providing the data they guarantee that they have authorization from the data subject to provide the data and make declarations regarding data processing, and that the data subject has previously become familiar with the data processing rules.

Data deletion deadline: 210 days following the last performance in the transaction, if the performance is held at a specific time. For events without dates, data deletion occurs 18 months after the transaction date. If a transaction includes a mix of dated and undated performances, transaction-related data is stored until the latest time according to the above calculation.

Possible consequences of failure to provide data: failure of the purchase transaction. Source of personal data: the data subject.

Recipients of personal data, categories of recipients: personal data is accessed by the Service Provider's customer service staff.

7.A. If a legal dispute arises regarding the purchase transaction during the data retention period indicated in point 7, the Service Provider retains the data within the limitation period (5 years), the legal basis for this is the Service Provider's legitimate interest, GDPR Article 6 (1) point f). Otherwise, the rules written in point 7 apply to this data processing as well.

If the ticket buyer needs to be refunded for tickets or other products due to possible ticket refunds or other reasons, and the buyer did not provide bank details during purchase or did not pay by bank card, it may become necessary to request the buyer's bank account number or other data required by the financial institution performing the refund. In these cases, the legal basis for data processing is the voluntary consent of the data subject (GDPR Article 6 (1) point a)). Otherwise, the rules written in point 7 apply to this data processing as well.

7.B. For certain events, the event organizer requests provision of additional data beyond the above during ticket and season ticket sales. The reason may be, for example, the need for special security checks for the event venue (e.g., closed military facilities, guarded state facilities), special admission requirements, legal requirements (e.g., data needed for accommodation booking), or other reasons established by the event organizer. The controller of these data is not INTERTICKET Ltd., but the event organizer. In these data processing activities - based on a data processing agreement concluded with the event organizer - INTERTICKET Ltd. acts as a data processor. The information notice regarding the processing of these data is prepared by the event organizer as data controller, whose link we publish on the website used during purchase.

8. **Online season ticket, gift card, discount card, Culture card purchase/renewal**

Purpose of data processing: ensuring the webshop service available on the website related to season ticket purchase, gift card/discount card/culture card purchase, handling orders and their fulfillment, documenting purchases and payments, fulfilling accounting obligations. The purpose of data processing is also to identify the user, fulfill the ordered service, send related notifications, enable payment through payment service providers, maintain user records, distinguish users from each other, maintain card balance records, maintain records of purchases made with the card, maintain records of discounts and privileges related to the card, ensure rights related to the season ticket (including renewal privileges if provided by the event organizer), fulfill the contract. The purpose of data processing is also to inform about annual season ticket renewal possibilities (by email or postal mail), reminders about upcoming season performances (by email or postal mail), for flexible season tickets, information twice monthly about the venue's programs and events (by email) - to assist User selection.

Legal basis for data processing: contract performance, GDPR Article 6 (1) point b).

Scope of processed data: first and last name, phone number (data required by payment service provider, but also enables our customer service or event organizer to immediately notify the ticket buyer in case of possible program, venue, or time changes), email address, password provided during prior registration, delivery address provided when requesting home delivery, transaction number, date and time, customer code, gift voucher number, balance, culture voucher number,

balance. The scope of processed data also includes - in case the season ticket (gift card, discount card or Culture card - hereinafter collectively season ticket) is issued in a specific name based on the event organizer's decision - the name of the rightful user of the season ticket and any other personal data possibly required by the event organizer. Considering that the season ticket buyer's identity may differ from the rightful user of the season ticket, if the season ticket buyer does not provide their own personal data, by providing the data they guarantee that they have authorization from the data subject to provide the data and make declarations regarding data processing, and that the data subject has previously become familiar with the data processing rules.

Data deletion deadline: for season tickets, 36 months from the transaction date. For gift cards, discount cards, Culture cards, if the given card has an expiration date, 6 months from the expiration date, and if the given card has no expiration date, we delete the data 18 months after the transaction. If the purchased card is associated with a tax benefit (e.g., Culture card), the data retention period is prescribed by applicable legislation, the legal basis being GDPR Article 6 (1) point c).

Possible consequences of failure to provide data: failure of the purchase transaction.

Source of personal data: the data subject.

Recipients of personal data, categories of recipients: personal data is accessed by the Service Provider's customer service staff.

8.A. If a legal dispute arises regarding the purchase transaction during the data retention period indicated in point 8, the Service Provider retains the data within the limitation period (5 years), the legal basis for this is the Service Provider's legitimate interest, GDPR Article 6 (1) point f). Otherwise, the rules written in point 8 apply to this data processing as well. If the buyer needs to be refunded for season tickets/tickets or other products due to possible season ticket/ticket refunds or other reasons, and the buyer did not provide bank details during purchase or did not pay by bank card, it may become necessary to request the buyer's bank account number or other data required by the financial institution performing the refund. In these cases, the legal basis for data processing is the voluntary consent of the data subject (GDPR Article 6 (1) point a)). Otherwise, the rules written in point 8 apply to this data processing as well.

8.B. For certain events, the event organizer requests provision of additional data beyond the above during ticket and season ticket sales. The reason may be, for example, the need for special security checks for the event venue (e.g., closed military facilities, guarded state facilities), special admission requirements, legal requirements (e.g., data needed for accommodation booking), or other reasons established by the event organizer. The controller of these data is not INTERTICKET Ltd., but the event organizer. In these data processing activities - based on a data processing agreement concluded with the event organizer - INTERTICKET Ltd. acts as a data processor. The information notice regarding the processing of these data is prepared by the event organizer as data controller, whose link we publish on the website used during purchase.

9. Registration

Purpose of data processing: Through prior registration with password provision, it becomes possible for the User to provide their data only once rather than with each purchase. Certain services on the website are available exclusively to registered Users. Such services include blog and comment writing, the ability to rate comments, and the follow function (requesting notifications about creators, venues, programs). As a convenience service, in the account that opens as a personal menu item on the website, the user can edit their personal data, view and download their tickets, invoices, track their comments, previously viewed pages, ratings they gave, modify their follow services and newsletter subscriptions, and if they are a member of a loyalty program, view their point balance. Processing diverse personal data stored in the account necessarily also means

profiling.

Legal basis for data processing: voluntary consent of the data subject, GDPR Article 6 (1) point a).

Scope of processed data: email address, password and all personal data provided by the User during purchase or in the account: address, billing address, phone contact. Processed data may include products purchased by the User during orders, purchase dates, invoices, User comments and their ratings, comments rated by the User, performances, creators, venue ratings, creators, venues, programs marked for following by the User, pages viewed by them, newsletter subscriptions, and loyalty points.

Data deletion deadline: The Service Provider processes the provided data as long as the User does not prohibit such use of the data - by unsubscribing. If the User performs no activity and thus does not use any service provided by the Service Provider, the Service Provider deletes the registration 3 years after registration.

Possible consequences of failure to provide data: the user cannot use the website's convenience functions and services.

Source of personal data: the data subject.

Recipients of personal data, categories of recipients: personal data is accessed by the Service Provider's customer service staff.

10. **Notification service**

Purpose of data processing: Considering that ticket and season ticket purchases often occur weeks or months before the Event date, the Service Provider operates a notification service that alerts ticket buyers to upcoming events, and - if such data is available - can provide additional technical information about the Event (technical notifications related to the performance, performance changes, venue and time changes, parking information, suggested arrival time, dress code, dining options available at the venue, buffet opening hours, expected performance end time, etc.). The notification service is not available for all Events or all ticket purchases made on buyer pages.

Legal basis for data processing: contract performance, GDPR Article 6 (1) point b).

Scope of processed data: email, name.

Data deletion deadline: the Service Provider processes the data for the same period as the related ticket or season ticket purchase transaction data (see points III. 7-8 of this notice).

Source of personal data: the data subject.

Recipients of personal data, categories of recipients: personal data is accessed by the Service Provider's customer service staff.

11. **Invoicing**

Purpose of data processing: issuing accounting documents for purchase transactions and preserving them for the period specified in legislation.

Legal basis for data processing: fulfilling legal obligation, GDPR Article 6 (1) point c).

Scope of processed data: first and last name, billing address provided for invoice issuance, transaction number, date and time, document content, tax number in case of VAT invoice (if

provided by the buyer), and email address for sending the invoice and possible resending.

Data deletion deadline, data processing duration: 8 years, or the period specified in applicable tax and accounting legislation.

Possible consequences of failure to provide data: purchase failure.

Source of personal data: the data subject.

Recipients of personal data, categories of recipients: personal data is accessed by the Service Provider's customer service and marketing department staff.

Data processor: The technical conditions for invoicing are provided by the following company: Számlázz.hu, KBOSS.hu Ltd. (tax number: 13421739-2-13, company registration number: 13-09-101824, registered office: 2000 Szentendre, Táltos u. 22/b).

12. **Personalized offers, profiling**

Purpose of data processing: Profiling helps ensure that Users encounter relevant, personalized offers in website and newsletter recommendations. Profiling helps the data processor compile the most suitable offerings for customers.

Legal basis for data processing: voluntary consent of the data subject, GDPR Article 6 (1) point a).

Scope of processed data: email, name, address, information related to website usage (visit time, duration, viewed pages, clicks on pages, search usage), cart usage (order identifier, products, their product categories, values), purchases (transaction time, value, product, its category, discount used, payment method), technical information (IP address, cookie identifier, browser type, device type, Google, Facebook, Hotjar, Findgore, Prefixbox identifiers, source page), newsletter and notification message usage data (email opening time, device, clicked links, purchase data), data related to blog system usage (comments, ratings, clicked links).

No automated decision-making occurs in connection with profiling.

Profiling logic: the recommendation system offers a list of programs presumed most suitable for the buyer for display on the website and in messages sent by the Service Provider.

Data deletion deadline: The Service Provider processes the provided data as long as the User does not prohibit such use of the data - by unsubscribing.

If the User performs no activity and thus does not use any service provided by the Service Provider, the Service Provider deletes the registration 3 years after subscribing to profiling.

Possible consequences of failure to provide data: offers not relevant to the User appear on the website and in newsletters, the User cannot use convenience services tied to registration.

Source of personal data: the data subject.

Recipients of personal data, categories of recipients: personal data is accessed by the Service Provider's customer service and marketing department staff.

13. **Electronic newsletters and other electronic mailings containing advertising**

Purpose of data processing: Sending email newsletters and other electronic mailings containing advertising to interested parties. If the User subscribes to the newsletter, the Service Provider may

send newsletters at its own discretion frequency. If the User requests that the Service Provider display additional offers in the ticket delivery email and emails sent as notification service, the Service Provider also displays offers for the User in these documents. In case of registration and/or profiling consent, the Service Provider strives where possible to offer relevant events of interest to the User based on residence, previous purchases, and other data provided or collected during registration and profiling.

Legal basis for data processing: voluntary consent of the data subject, GDPR Article 6 (1) point a).

Scope of processed data: name, email address, postal code, as well as data provided or collected during registration/profiling.

Data deletion deadline: The Service Provider processes the provided data as long as the User does not prohibit such use of the data - by unsubscribing. The newsletter and additional electronic mailings and advertising contained therein can be cancelled by clicking the "Unsubscribe" link at the bottom of the newsletter/electronic mailing. Personal data deletion occurs within 10 working days of receiving the request. If the User performs no activity and thus does not use any service provided by the Service Provider, the Service Provider deletes the registration 3 years after newsletter subscription.

Possible consequences of failure to provide data: the User does not receive notifications about programs.

Source of personal data: the data subject.

Recipients of personal data, categories of recipients: personal data is accessed by the Service Provider's customer service and marketing department staff.

14. **Participation in the Service Provider's loyalty program**

Purpose of data processing: ensuring participation in the loyalty program announced by the Service Provider for regular buyers of the Jegy.hu website.

Legal basis for data processing: voluntary consent of the data subject, GDPR Article 6 (1) point a).

Scope of processed data: name, email address, postal code, phone number, as well as data collected during profiling.

Data deletion deadline: The Service Provider processes the provided data as long as the User does not prohibit such use of the data - by unsubscribing. If the User performs no activity and thus does not use any service provided by the Service Provider, the Service Provider deletes the registration 3 years after registration in the loyalty program.

Possible consequences of failure to provide data: the User cannot participate in the loyalty program announced by the Service Provider.

Source of personal data: the data subject.

Recipients of personal data, categories of recipients: personal data is accessed by the Service Provider's customer service staff.

15. **Cookie handling**

A cookie is a variable-content, alphanumeric information package sent by the web server, which is recorded on the User's computer and stored for a predetermined validity period. Cookie usage

provides the opportunity to query certain visitor data and track internet usage. Cookies help track the affected User's interests, internet usage habits, website visit history, so that the User's shopping experience is optimal. Since cookies function as a kind of tag with which the website can recognize returning visitors, their use can also store the username and password valid on the given site. If the browser sends back a previously saved cookie, the service provider handling the cookie has the opportunity to connect the user's current visit with previous ones, but exclusively regarding its own content.

Information sent by cookies helps internet browsers be more easily recognized, so Users can receive relevant and "personalized" content. Cookies make browsing more convenient, including online data security needs and relevant advertising. Using cookies, the Service Provider can also prepare anonymous statistics about site visitor habits, allowing even better personalization of the site's appearance and content.

The Service Provider's website uses two types of cookies:

- Temporary cookies - session (session-id) cookies essential for site use. Their use is essential for navigation on the website and for website functions to work. Without accepting these, the website or its parts do not appear, browsing becomes hindered, adding tickets to cart and bank payment cannot be properly implemented.
- Permanent cookies, which remain on the device for longer periods depending on web browser settings, or until the User deletes them. Within these, we can speak of internal or external cookies. If the Service Provider's web server installs the cookie and the data is transmitted to its own database, we speak of internal cookies. If the cookie is installed by the Service Provider's web server but data transmission occurs to an external service provider, we speak of external cookies. Such external cookies include third-party cookies placed in the User's browser by third parties (Google Analytics, Facebook Pixel). These are placed in the browser if the visited website uses services provided by third parties. The purpose of permanent cookies is to ensure the highest quality operation of the given site to increase user experience.

When visiting the website, the User can give consent for permanent cookies to be stored on the User's computer and for the Service Provider to access them using the button on the cookie warning found on the login page.

The User can set up and prevent cookie-related activities using the browser program. Cookie management is generally possible in browsers under the Tools/Settings menu under Privacy/History/Custom settings menu, with names like cookie, süti or tracking. However, we again draw your attention that in the latter case, without using cookies, the User may not be able to use all website services, particularly payment services. You can read additional information about cookies by clicking the link in the cookie warning bar appearing on the Jegy.hu page.

Purpose of data processing: conducting payment transactions with payment service providers, identifying users, distinguishing them from each other, identifying users' current sessions, storing data provided during them, preventing data loss, identifying users, tracking, web analytics measurements. Legal basis for data processing: voluntary consent of the data subject, GDPR Article 6 (1) point a). Scope of processed data: identifier, date, time, and previously visited page. Data processing duration: temporary cookies are stored until all browsers of the given type are closed by the user. Permanent cookies are stored on the user's computer for 1 year or until the User deletes them. Possible consequences of failure to provide data: incomplete use of website services, payment transaction failures, analytical measurement inaccuracies. Source of personal data: data automatically generated by the IT system. Recipients of personal data, categories of recipients: none

This website uses the Microsoft Clarity web analytics tool provided by Microsoft Ireland Operations

Ltd. (One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, Ireland). Clarity provides opportunity to analyze website traffic and user interactions. The information obtained helps improve our website's usability and user experience. The data collection process is implemented using cookies.

The system records and processes the following data: IP address, location data, session identifier, user interactions, clicks, scrolling, mouse movements, unique user identifier, visit date and time.

Automatic deletion of collected data occurs after 13 months. Fields containing sensitive information (such as forms, search fields) are blurred during data collection, their content is not recorded.

In certain cases, data may also be transmitted to the United States, which qualifies as a third country outside the European Union and European Economic Area. Microsoft Corporation has appropriate data protection certifications, so data transmission complies with GDPR requirements.

Data processing is based on user consent, in accordance with GDPR Article 6 (1) paragraph a). The user is entitled to withdraw consent at any time. Withdrawing consent does not affect the lawfulness of processing operations performed before withdrawal.

16. Location determination

If the User uses the service from a mobile device (e.g., smartphone), for using location-requiring functions, the program may request permission to use location data when downloading the application (e.g., when using the "nearby" function).

Purpose of data processing: With user permission, the application can offer personalized searches that take into account where the user is at the given moment. Location data is not recorded in the Data Controller's system, it only enables use of certain functions available during the given transaction (more precise search, "nearby" function, etc.).

Legal basis for data processing: voluntary consent of the data subject, GDPR Article 6 (1) point a).

Scope of processed data: the user's geographical position at a given time, IP address.

Data processing duration: 3 days

Possible consequences of failure to provide data: incomplete use of mobile device services.

Source of personal data: data automatically generated by the IT system.

Recipients of personal data, categories of recipients: none

17. Statistical data

The data controller may use data for statistical purposes. Statistical use of data in aggregated form may not contain the affected user's name or other identifying data in any form.

18. Data technically recorded during system operation

Technically recorded data is data from the User's logging computer that is generated during service use and which the data controller's system logs as an automatic result of technical processes (e.g., IP address, session ID). Due to internet operation, automatically recorded data is logged by the system automatically - through internet use - without separate declaration or action by the User. The internet does not function without these automatic server-client communications. These data cannot be connected with other User personal data - except in cases required by law. Only the Data

Controller accesses the data. Log files automatically technically recorded during system operation are stored in the system for the duration justified for ensuring system operation.

19. Recording telephone conversations

The Service Provider records incoming and outgoing telephone conversations to customer service.

Purpose of data processing: enforcing customer and data controller rights, providing evidence for deciding possible legal disputes, subsequent verifiability and providing evidence supporting possible claim uncollectibility, as well as subsequent proof of agreements, quality assurance, fulfilling legal obligations.

Legal basis for data processing: voluntary consent of the data subject.

Scope of processed data: identifier, calling number, called number, call date, time, telephone conversation audio recording, as well as other personal data provided during the conversation.

Data deletion deadline: five years.

Possible consequences of failure to provide data: no telephone assistance provided.

Source of personal data: the data subject.

Recipients of personal data, categories of recipients: personal data is accessed by the Service Provider's customer service staff.

20. Service Provider customer correspondence (email) and chat communication

Chat communication is not available on all pages, the applicable data processing rules are only applied if chat communication is used on the given page.

Purpose of data processing: providing customer service assistance and complaint handling available to buyers and users.

Legal basis for data processing: voluntary consent of the data subject, GDPR Article 6 (1) point a).

Scope of processed data: The Service Provider processes incoming emails and chat communications together with the data subject's email address, any additional personal data possibly provided by the data subject, as well as date and time data according to the rules contained in this notice. During chat communication, providing an email address is mandatory because this ensures the Service Provider coordinates parallel complaint handling. Providing additional personal data (name, phone number, etc.) may become necessary during complaint handling for substantive handling of the request.

Data deletion deadline: The Service Provider processes the provided data until the User has them deleted - with a specific request to the Service Provider's customer service. If the data subject does not declare otherwise, the Service Provider deletes the data three years after closing the complaint. If legislation prescribes mandatory retention periods for documents created during complaint handling, the Service Provider preserves the relevant documents until the end of document retention deadlines prescribed in applicable legislation.

Possible consequences of failure to provide data: the data subject cannot use the Service Provider's customer service.

Source of personal data: the data subject.

Recipients of personal data, categories of recipients: personal data is accessed by the Service Provider's customer service staff.

The Service Provider does not transfer personal data to third parties.

21. Web analytics measurements

Google Analytics as an external service provider helps independently measure the website's traffic and other web analytics data. Detailed information about handling measurement data can be found at the following link: http://www.google.com/analytics . The Service Provider uses Google Analytics data exclusively for statistical purposes, to optimize site operation.

Source of personal data: data automatically generated by the IT system.

Recipients of personal data, categories of recipients: none

22. Other data processing

We provide information about data processing not listed in this notice when collecting data. We inform our customers that courts, prosecutors, investigative authorities, misdemeanor authorities, administrative authorities, the National Data Protection and Freedom of Information Authority, the Hungarian National Bank, or other bodies based on legal authorization may contact the Service Provider for providing information, communicating data, transferring data, or making documents available. The Service Provider provides personal data to authorities - if the authority has indicated the precise purpose and scope of data - only to the extent absolutely necessary to achieve the purpose of the request.

23. The Data Controller does not verify personal data provided to it. Only the person providing the data is responsible for the adequacy of provided data. When providing any user's email address, they also assume responsibility that only they use services from the provided email address. Due to this responsibility assumption, all responsibility related to logins from a given email address falls exclusively on the user who registered that email address. If the user provides data that is not their own personal data, they are obligated to obtain consent from the data subject.
24. Those authorized to access personal data are employees in employment or commission relationships with the Service Provider, courier service employees participating in product delivery (if delivery was requested by the buyer), as well as Data Processors.

III/A. Special data processing related to certain prominent sporting events (special information regarding prominent sporting events is communicated in italicized text for easier overview)

1. According to the agreement between Interticket Ltd. and MLSZ, Interticket Ltd. is authorized to sell tickets for Hungarian national team matches based on MLSZ's mandate. The ticket sales process and essential elements of data processing were jointly determined by MLSZ and Interticket, the ticket sales process is implemented with MLSZ cooperation, since MLSZ is the match organizer, thus MLSZ and Interticket Ltd. act as joint data controllers during ticket sales.
2. Presentation of special data processing cases related to certain prominent sporting events and scope of processed data

Ticket sales are implemented according to the following data processing process:

a) Ticket purchase online or at box office with club card or by providing personal data

b) Check in Sports Police Registry (hereinafter: SRNY) in case of personalized ticket sales

c) Fan Club membership verification, discount validation

d) Ticket issuance

e) Ticket exchange

f) Forwarding ticket barcode to Puskás Aréna entry system

g) Providing report data to MLSZ

3. Ticket purchase [data processing according to points a)-d)]

Data processing process, purpose and data controller identity

Buyers can purchase tickets both at box office and online for Hungarian national team matches held at Puskás Aréna.

Tickets can be purchased in person at InterTicket's national ticket office network. Ticket office contacts can be found on the Jegy.hu website.

Box office ticket purchase If the buyer wants to buy tickets at the box office and sales occur in specific names, they must provide three mandatory data items (name, birth date and place), which must be entered into Interticket Ltd.'s ticket sales system and optionally mother's maiden name data can be recorded.

Purchase may also occur for another person, in which case data processing does not differ from when someone buys tickets in their own name.

Ticket purchase is generally not tied to identity verification. However, MLSZ as organizer may decide to require that during ticket purchase the buyer present their Club card, Football card (hereinafter together: fan card) or identity document. Club cards issued by club teams can also be used for ticket purchase purposes at MLSZ-organized matches.

Data provided in connection with ticket purchase is processed by Interticket Ltd., who conducts commission sales on MLSZ's behalf. MLSZ's role in data processing is limited to prescribing personalized ticket sales and, due to compliance with entry and security requirements, processing provided data as detailed separately below.

Interticket Ltd. issues invoices to buyers for purchases, processing the buyer's name and address for this.

The purpose of data processing related to personalized ticket and season ticket sales is implementing ticket sales compliant with stadium security requirements according to Sports Act Section 72/B.

Based on the referenced legislation, data may be used for criminal or misdemeanor proceedings initiated due to crimes or misdemeanors committed at the sports event venue or during approach to or departure from the sports event venue, as well as for exclusion from participation in sports events.

Data processing related to ticket sales is mandatory when using entry systems based on Sports Act Section 72 (3) and (4), however fan card use is only mandatory if MLSZ makes it mandatory for the given match.

Before ticket purchase, Interticket Ltd. verifies Fan Club membership discounts and validates discounts in case of personalized ticket sales.

In case of mandatory identity verification:

- for purchase, the buyer must present their fan card or identity document (in case of purchase in another person's name, that person's club card or identity document is needed for whom the ticket will be issued),
- with the fan card number (barcode), the name, birth place and date data needed for ticket purchase (also mother's maiden name data if provided when obtaining the card) can be filled in using the fan card register,
- failing this, the cashier records data needed for ticket purchase in the system based on the provided identity document or fan card data.

If fan card possession and presentation is not a condition for ticket purchase, the cashier records data needed for ticket purchase based on information provided by the buyer and issues tickets based on this, but may request club card or identity document presentation to verify data.

However, it should be considered that in case of personalized ticket sales, identity verification also occurs during entry and if the data on the ticket does not match the data on the identity document, the buyer cannot be admitted to the match.

The IT system behind ticket purchase examines whether the given person is banned, excluded or barred based on provided buyer data (i.e., queries the Sports Police Registry - SRNY).

If there is a match based on previously provided personal data, the buyer may provide their mother's maiden name even if they did not provide this initially. The system then performs another check. This option is not available to the buyer if they purchase with a Club card or Football card.

No person who appears in SRNY for the given match and/or venue cannot purchase tickets for the match, nor can tickets be purchased for such persons.

In case of positive response (banned/excluded or barred status), the buyer's or ticket beneficiary's personal data is not stored in the ticket system, but the affected person's data is accessible in the SRNY log, which can be traced back to the fact that even the purchase attempt qualifies as a misdemeanor.

If the buyer or ticket beneficiary does not appear in SRNY, the buyer's personal data necessary for ticket purchase (name, birth place and date, optionally mother's maiden name) is stored in the central ticket sales IT system database.

During personalized ticket sales, name and birth date data also appear on the ticket.

Online ticket purchase Data needed for ticket purchase:

- in case of personalized ticket sales: name, birth place and date, one optional data: buyer's mother's maiden name, as well as
- in case of fan card-linked ticket sales, the card number and PIN code.

During online purchase, ticket purchase occurs in the web system operated by Interticket Ltd. The scope of processed personal data and the ticket purchase process match the process occurring at the box office.

If ticket sales for a given match do not occur in specific names and online purchase occurs, Interticket Ltd. only processes the ticket buyer's data provided during registration.

If data is provided with a club card, the card number and associated secret PIN code must be entered into the system, and the IT system fills in the buyer's personal data necessary for purchase based on the provided data.

If payment occurred by bank card, the buyer provides the data required by the relevant bank themselves on the payment service provider's own interface, Interticket Ltd. does not access card data and performs no data processing operations in this regard.

Data processing duration Interticket Ltd. processes data provided during registration in the online ticket sales system until registration deletion or consent withdrawal.

Data processed for ticket sales purposes is deleted from the ticket sales system 60 days after the match - unless the competent authority instructs MLSZ as organizer to retain data for an additional maximum of 30 days - personal data is deleted according to legal requirements.

Interticket Ltd. preserves invoices for 8 years as accounting documents.

Legal basis for data processing The legal basis for data processing is legal obligation according to Regulation Article 6 (1) paragraph c), since based on Sports Act Section 72 (1), the organizer may use a security entry and control system suitable for individual identification of participants (hereinafter: entry system), and for football sports, in case of prominent security risk sports events and increased security risk sports events - if the National Police Headquarters ordered the obligation to use an entry system, or the organizer decides independently - an entry system is used.

Based on paragraph (2) of the same section, when using an entry system, the organizer or person conducting ticket sales on the organizer's mandate may only sell personalized admission tickets or season tickets.

Based on paragraph (4) of the same section, the organizer or person conducting ticket sales on the organizer's mandate is entitled to establish the viewer's identity based on identity documents suitable for identity verification when selling admission tickets, season tickets, and during entry.

Based on paragraph (5) of the same section, when using an entry system, the organizer or person conducting ticket sales on the organizer's mandate may compare the viewer's identity with SRNY data when selling admission tickets or season tickets.

In case of registration performed on the online interface, the legal basis for data processing is the buyer's voluntarily given consent according to Regulation Article 6 (1) paragraph a).

Invoice issuance and preservation is a legal obligation according to Regulation Article 6 (1) paragraph c), invoice issuance is prescribed by Act CXXVI of 2007 on general sales tax Section 159 (1), preservation is prescribed by Act C of 2000 on accounting Section 169 (2).

The legal basis according to Regulation Article 6 (1) paragraph b) for contract performance also generally appears behind data processing related to ticket purchase, since Interticket Ltd. cannot sell tickets to the buyer without processing data provided for ticket purchase.

4. *Ticket exchange*

Data processing process, purpose and data controller identity If the buyer purchased a personalized ticket and wants to transfer it to another person, this is possible through ticket exchange.

Ticket exchange is performed by Interticket Ltd. at the buyer's request.

Regarding ticket exchange, the data processing operations described for ticket purchase must also be performed for the new ticket owner, with the difference that Interticket Ltd. does not provide an invoice to the new ticket owner.

Data processing duration The rules written for ticket purchase apply to storing the new ticket buyer's data.

Legal basis for data processing The legal basis for data processing regarding ticket exchange is contract performance with the previous ticket owner according to Regulation Article 6 (1) paragraph b), which includes the possibility of ticket exchange. For the new ticket owner, the legal basis for data processing matches what is written for ticket purchase.

5. Forwarding ticket barcode to Puskás Aréna entry system

Data processing process, purpose and data controller identity

Interticket Ltd. is obligated to forward the ticket barcode given during ticket purchase to the Puskás Aréna entry system. The barcode alone does not contain personal data, but together with other data, Interticket Ltd. and MLSZ can identify who purchased the ticket belonging to the barcode (in case of personalized ticket sales).

Forwarding the barcode is essential, since without this the entry system does not recognize valid tickets.

Data processing duration The barcode loses its personal data quality when Interticket Ltd. and MLSZ delete the known personal data connected to it. The rules written for ticket purchase apply to deletion.

Legal basis for data processing The legal basis for data processing is contract performance between Interticket Ltd. and the buyer according to Regulation Article 6 (1) paragraph b), since entry to the match cannot be ensured without data transfer when using an entry system.

6. Providing report data to MLSZ

In this data processing framework, Interticket Ltd. transfers personal data to MLSZ as organizer of Hungarian national team matches according to applicable legislation. In this case, MLSZ acts as data controller. In the data processing framework, MLSZ receives data provided for ticket purchase in the ticket sales system provided by Interticket Ltd., supplemented with precise seating data. The purpose of data processing is for MLSZ as match organizer to be able to perform entry and safe organization tasks prescribed by the sports law. Additionally, MLSZ data processing is prescribed by UEFA Safety and Security Regulations points 16.01, 16.02 and 16.03, which prescribe that MLSZ must have ticket holders' personal data. Based on personal data linked to seating, MLSZ can identify ticket holders, provide information about them to arriving medical personnel in case of medical emergencies, and data processing is also necessary for filing complaints or taking measures in case of misdemeanors and crimes or violation of field regulations.

7. *Special rules for wheelchair ticket buyers and their companions*

Data processing process, purpose

In certain stadiums, for certain matches or events, it is possible to watch matches from places specifically designed for wheelchair or mobility-impaired visitors, and occasionally, in limited numbers, it is possible to reserve parking spaces designed for mobility-impaired persons. These places can only be used by proving eligibility, eligibility verification occurs during the online ticket purchase process and during entry. Ticket and parking space requests must be submitted to

Interticket Ltd. on a form designed for this purpose. By submitting the online form, the mobility-impaired ticket buyer expressly consents to processing the data detailed below, including that the data controller - to ensure special wheelchair places and parking spaces - also processes health condition data. The following data must be provided on the online form: email address to which tickets are requested to be delivered, name, birth place and date, mother's maiden name data, both for the wheelchair or mobility-impaired buyer and their companion (if appropriate places are designed for companions at the given event), and beyond these, the wheelchair buyer's mobility impairment certificate number.

The data controller identity and data processing duration match what is described for online ticket purchase.

The legal basis for data processing is the affected person's express consent, which they provide by filling out and submitting the online form to the data controller as described above (GDPR Article 6 (1) point a).

For prominent sporting events, if the User requests wheelchair tickets and accompanying companion tickets, and if they have observations requiring investigation regarding data reconciliation, they must fill out a Google Form. The Service Provider deletes data received on the Form on the sixtieth day following the Match. Click here for Google Privacy Policy and General Terms and Conditions.

III/B. Special rules for online events

1. Personal buyer account

Online events can be live and/or recorded theatrical or other performances, events, etc., for viewing which - at the time or period indicated during ticket purchase - the Buyer acquires authorization through ticket purchase.

Purpose of data processing: Creating a personal buyer account is necessary for viewing online events. Creating the personal buyer account requires an accessible, valid email address, and providing name and password. After providing data, the Service Provider's system sends a message to the indicated email address requesting its confirmation. Authorizations for viewing individual content are tied to the personal buyer account. Creating the personal buyer account is not the same as registration - optionally offered, non-mandatory - for non-online events detailed in point III/9 of this Data Processing Notice. For technical reasons, accordingly, buyers registered according to point III/9 also need to create a personal buyer account if they want to view online events. Registration and the personal buyer account are therefore not connected, their use is independent of each other.

Legal basis for data processing: contract performance GDPR Article 6 (1) point b).

Scope of processed data: email address, name, password. Data deletion deadline: The Service Provider processes the provided data as long as the User does not request deletion of the personal buyer account. If the User performs no activity and thus does not use services provided by the Service Provider, the Service Provider deletes the account 3 years after the last user activity.

Possible consequences of failure to provide data: the User cannot view online events.

Source of personal data: the data subject. Recipients of personal data, categories of recipients: personal data is accessed by the Service Provider's customer service staff.

2. IP address

Purpose of data processing: The Service Provider provides its service related to online events - if different information is not found in the given performance description - free from territorial restrictions. However, territorial restrictions may be possible for some performances due to copyright, performance rights limitations, or other reasons. In these cases, the Service Provider draws Buyers' attention to these restrictions in the event description before purchase. In case of territorial restrictions, the Service Provider is entitled to verify the Buyer's IP address, to check compliance with territorial restrictions, and to refuse access if the viewing location would conflict with territorial restrictions.

Legal basis for data processing: contract performance GDPR Article 6 (1) point b).

Scope of processed data: IP address.

Data deletion deadline: Until the end of online event viewability.

Possible consequences of failure to provide data: the User cannot view online events whose viewability is territorially restricted.

Source of personal data: the data subject (through machine communication).

Recipients of personal data, categories of recipients: personal data is accessed by the Service Provider's customer service staff.

IV. Data transfer, naming Data Processors

1. By using the service, the User consents to the Service Provider transferring data to the following partners. Legal basis for data transfer: contract performance, GDPR Article 6 (1) point b).

1.1. In case of data processing indicated in points III. 7.-8, to the given event organizer for the purpose that the event organizer can provide direct and immediate information about event cancellation, time changes or any important circumstances affecting the viewer, or - in case of performance cancellation - directly handle ticket refunds or exchanges, admit the buyer to the event, and fulfill the contract (proper conduct of the performance). With data transfer, the given event organizer becomes an independent data controller regarding the transferred data. Data transfer may also occur by the Service Provider granting appropriate access to the event organizer to the IT system serving ticket management ("Tickets system"). Scope of processed data: data indicated in points III. 7-8.

1.2. In case of point III. 11, to the service provider providing technical conditions for invoicing, as Data Processor, which is the following: Számlázz.hu, KBOSS.hu Ltd. (tax number: 13421739-2-13, company registration number: 13-09-101824, registered office: 2000 Szentendre, Táltos u. 22/b). Scope of processed data: data indicated in point III. 11.

1.3. Sending emails to Users, and if the affected person gave permission for profiling, tasks related to this are also performed by Wanadis Commercial and Service Ltd. (1118 Budapest, Rétköz u. 7.), or Emarsys eMarketing Systems AG (Marzstrasse 1, 1150 Vienna, Austria) as data processor, based on a contract concluded with the data controller.

1.4. For all transactions where the product/service value can be paid through online banking service, the Service Provider transfers data to financial institutions participating in the purchase process and handling payment. The indicated data transfer is required by the financial institution to conduct payment, the scope of required data varies by financial institution. The Service Provider does not learn personal data provided on the financial institution's own data input pages. The following financial institutions may appear as payment service providers on the website, the table

also contains data whose transfer is required by the given financial institution. (Not all payment financial institutions appear on the website at a given time.) Data required by financial institutions may change, particularly considering the introduction of so-called strong customer authentication - at different deadlines by bank.

Payment service provider name	Transferred data (scope of processed data)
OTP	transaction amount, name, address, IP number
SimplePay Zrt. / SIMPLE	email address, phone number
CIB	transaction amount
K&H	transaction amount, currency
Barion	name, email address

- SimplePay Ltd. / SIMPLE / SimplePay Data Processing Notice can be viewed at the following link: https://simplepay.hu/adatkezelesi-tajekoztatok/
- Barion Payment Ltd. is an institution under the supervision of the Hungarian National Bank, license number: H-EN-I-1064/2013.

1.5. If the User purchases with some special discount-providing tool, the Data Controller forwards buyer data required by the company to the company or financial institution providing the discount. The User can request information about applicable data processing rules directly from the providing company. The Data Controller processes identifiers and other data of such tools automatically only to the extent that the providing company requires this - for conducting the purchase or providing discounts. The following companies and financial institutions may appear on the website, the table also contains data whose transfer is required by the given company or financial institution. (Not all payment service providers or companies appear on the website at a given time.)

Payment service provider name	Transferred data (scope of processed data)
OTP SZÉP card	transaction amount, name, address, email address, IP number
Sponsorem	transaction amount, card number, currency
Supershop	transaction amount, card number, name, birth date,

	email address
MKB SZÉP card	transaction amount
Cafe T-rend	transaction amount, card number

1.6. In case of point III/A, if personalized tickets/season tickets are issued for the given match/matches, and if the ticket/season ticket owner can request printing the ticket/season ticket on plastic card, InterTicket Ltd. forwards ticket/season ticket data and ticket/season ticket owner data (name, birth place and date, delivery address, and additional delivery data provided by the ticket buyer) to the contractor performing printing and delivery:

Company name: **Szűcs Network Hungary Ltd.**

Registered office address: 4400 Nyíregyháza, Rákóczi u. 98.

Company registration number: 15-09-073764

Tax number: 14617623-2-15

2. The Service Provider, as Data Controller, is authorized and obligated to transfer to competent authorities all available and regularly stored personal data, which data transfer is required by law or final administrative obligation. The Data Controller cannot be held responsible for such data transfer and consequences arising from it.
3. The Service Provider performs data transfer not indicated above exclusively with the User's prior and informed consent.

V. Method of storing personal data, data processing security

1. The Service Provider's computer systems and other data storage locations are found at its registered office and at its data processors.
2. The Service Provider selects and operates IT tools used for processing personal data during service provision so that processed data is:

a) accessible to those authorized (availability);

b) its authenticity and authentication is ensured (data processing authenticity);

c) its unchangeability is verifiable (data integrity);

d) protected against unauthorized access (data confidentiality).

3. The Service Provider protects data with appropriate measures especially against unauthorized access, modification, transmission, disclosure, deletion or destruction, as well as accidental destruction, damage, and inaccessibility resulting from changes in applied technology.
4. The Service Provider ensures with appropriate technical solutions for protecting electronically processed datasets in its various registers that stored data - except when permitted by law - cannot be directly connected and assigned to the data subject.
5. The Service Provider, considering the current state of technology, ensures data processing security protection with technical, organizational and administrative measures that provide a protection level appropriate to risks associated with data processing.
6. During data processing, the Service Provider maintains:

a) confidentiality: protects information so that only those authorized can access it;

b) integrity: protects the accuracy and completeness of information and processing methods;

c) availability: ensures that when authorized users need it, they can actually access desired information and related tools are available.

7. The Service Provider's and its partners' IT system and network are both protected against computer-supported fraud, espionage, sabotage, vandalism, fire and flood, as well as computer viruses, computer break-ins and other attacks. The operator ensures security with server-level and application-level protection procedures.
8. During automated processing of personal data, the Service Provider ensures with additional measures:

a) preventing unauthorized data entry;

b) preventing unauthorized use of automatic data processing systems by unauthorized persons using data transmission equipment;

c) verifiability and establishment of which bodies personal data was or can be transmitted to using data transmission equipment;

d) verifiability and establishment of which personal data was entered into automatic data processing systems when and by whom;

e) restorability of installed systems in case of operational failure; and

f) that reports are made about errors occurring during automated processing.

9. When determining and applying measures serving data security, the Service Provider considers the current state of technology. Among multiple possible data processing solutions, the one providing higher level protection for personal data must be chosen, except if this would mean disproportionate difficulty.
10. The Service Provider ensures data processing security protection with technical, organizational and administrative measures that provide a protection level appropriate to risks associated with data processing.
11. Electronic messages transmitted on the internet are vulnerable to network threats regardless of protocol (email, web, ftp, etc.), which can lead to dishonest activity or information disclosure or modification. To protect against such threats, the Service Provider takes all reasonable precautions. Systems are monitored to record all security deviations and provide evidence in case of any security events. System monitoring additionally enables checking the effectiveness of applied precautions. However, the Internet is notoriously - thus known to Users - not 100% secure. The Service Provider bears no responsibility for possible damages caused by unavoidable attacks occurring despite maximum expected care.

VI. Rights of data subjects

1. The data subject can request information about processing their personal data, and can request correction of their personal data, and - except for mandatory data processing - deletion, withdrawal, exercise their data portability and objection rights in the manner indicated during data collection, or at the Service Provider's contacts written in point I of this Data Processing Notice.

Changes in personal data or requests for personal data deletion can be communicated in a written

declaration with full probative value sent to the registered email address or by post. Additionally, certain personal data modifications can also be made by modifying the page containing the personal profile.

2. **Right to information**

The Service Provider takes appropriate measures to provide data subjects with information about personal data processing in concise, transparent, understandable and easily accessible form, clearly and comprehensibly worded. The right to information can be exercised in writing through the contacts written in point I of this Data Processing Notice. Information can also be given orally to the data subject upon request - after verifying their identity.

3. **Right of access**

The data subject is entitled to request information from the Service Provider through the contacts indicated in point I about whether processing of their personal data is ongoing, and if such data processing is ongoing, is entitled to know:

- what personal data; on what legal basis; for what data processing purpose; for how long the Service Provider processes; furthermore,
- when, based on what legislation, to which personal data it provided access or to whom it transmitted the personal data;
- what sources the personal data comes from;
- whether it applies automated decision-making, including profiling, and its logic.

The Service Provider provides a copy of personal data subject to data processing to the data subject upon their request free of charge for the first time, and may subsequently charge a reasonable fee based on administrative costs. To meet data security requirements and protect the data subject's rights, the Service Provider must verify the identity of the data subject and the person wishing to exercise access rights, for which information, access to data, or issuing copies thereof is tied to identifying the data subject's person.

Requests for information sent by email - except if the data subject identifies themselves credibly in another way - are only considered authentic by the Data Controller if sent from the User's registered email address. Requests for information must be sent by email to interticket@interticket.hu .

4. In case of transferring personal data to third countries or international organizations, the data subject is entitled to receive information about appropriate safeguards for the transfer.
5. Upon the data subject's request, the Service Provider provides information electronically. The data controller provides information within maximum one month from submitting the request.
6. **Right to rectification**

The data subject can request through the contacts indicated in point I that the Service Provider modify some personal data. If the data subject can credibly prove the accuracy of corrected data, the Service Provider fulfills the request within maximum one month and notifies the data subject at the contact they provided.

7. **Right to erasure**

The data subject - if data processing is based on their consent - is entitled to request that the Service Provider delete personal data concerning the data subject without undue delay, and the data controller is obligated to delete personal data concerning the data subject without undue delay, if no other legal basis exists for processing the data.

After fulfilling requests for personal data deletion or modification, previous (deleted) data can no longer be restored.

8. Data deletion cannot be initiated if data processing is necessary based on any of the following reasons: fulfilling obligations under Union or Member State law applicable to the data controller that prescribes personal data processing, or necessary for the Service Provider's legal claims presentation, enforcement, or defense.
9. **Right to restriction (limitation of data processing)**

The data subject can request through the contacts indicated in point I that the Service Provider restrict processing their personal data (by clearly marking the restricted nature of data processing and ensuring separate processing from other data) if:

- they contest the accuracy of their personal data (in this case, the Authority restricts data processing for the period needed to verify personal data accuracy);
- data processing is unlawful and the data subject opposes data deletion, requesting instead restriction of their use;
- the data controller no longer needs personal data for data processing purposes, but the data subject requires them for presenting, enforcing or defending legal claims; or
- the data subject objected to data processing (in this case, restriction applies for the period until it is established whether the data controller's legitimate reasons take precedence over the data subject's legitimate reasons).

10. If data processing is subject to restriction, personal data can only be processed - except for storage - with the data subject's consent, or for presenting, enforcing or defending legal claims, or for protecting other natural or legal persons' rights. The Service Provider informs the data subject in advance about lifting data processing restrictions.
11. **Right to data portability**

The data subject is entitled through the contacts indicated in point I to receive personal data concerning them that they provided to the Service Provider in a structured, commonly used, machine-readable format, and is entitled to transmit this data to another data controller without hindrance from the Authority regarding automated data processing operations.

12. **Right to object**

The data subject can object to data processing through the contacts indicated in point I if in their view the Service Provider would not process their personal data appropriately in connection with the purpose indicated in the applicable data processing notice for the given procedure. In this case, the Service Provider must prove that processing personal data is justified by compelling legitimate reasons that take precedence over the data subject's interests, rights and freedoms, or that relate to presenting, enforcing or defending legal claims.

If personal data processing occurs for direct marketing purposes, the data subject is entitled to object at any time to processing personal data concerning them for such purposes, including profiling insofar as it relates to direct marketing. In case of objection to processing personal data for direct marketing purposes, the data cannot be processed for such purposes.

13. **Automated decision-making in individual cases, including profiling**

The data subject is entitled not to be subject to decisions based solely on automated data processing - including profiling - that would have legal effects concerning them or similarly significantly affect them. The above entitlement does not apply if data processing:

- is necessary for concluding or performing a contract between the data subject and data

controller;
- is permitted by applicable Union or Member State law that also establishes appropriate measures to protect the data subject's rights, freedoms and legitimate interests; or
- is based on the data subject's express consent.

14. Right of withdrawal

The data subject is entitled to withdraw their consent at any time. Withdrawing consent does not affect the lawfulness of data processing based on consent before withdrawal.

15. Procedural rules

The Service Provider informs the data subject without undue delay, but in any case within one month of receiving the request, about measures taken following requests under GDPR Articles 15-22. If necessary, considering the request's complexity and number of requests, this deadline can be extended by an additional two months. The Service Provider informs the data subject about extending the deadline with reasons for delay within one month of receiving the request. If the data subject submitted the request electronically, information is provided electronically, unless the data subject requests otherwise.

16. If the Service Provider does not take measures following the data subject's request, it informs the data subject without delay, but at latest within one month of receiving the request, about reasons for not taking measures, and that the data subject can file a complaint with a supervisory authority and exercise judicial remedy rights.
17. The Service Provider provides requested information and data free of charge. If the data subject's request is clearly unfounded or - especially due to its repetitive nature - excessive, the Service Provider may charge a reasonable fee considering administrative costs of providing requested information or data or taking requested measures, or may refuse to act on the request.
18. The Service Provider informs all recipients about any rectification, erasure or data processing restriction it performed, except if this proves impossible or requires disproportionately great effort. The Service Provider informs the data subject about these recipients upon request.
19. The Service Provider makes available to the data subject a copy of personal data subject to data processing. The Service Provider may charge reasonable fees based on administrative costs for additional copies requested by the data subject. If the data subject submitted the request electronically, information is made available in electronic format, unless the data subject requests otherwise.

20. Compensation and satisfaction

Anyone who suffered material or non-material damage as a result of violating the data protection regulation is entitled to compensation from the data controller or data processor for the damage suffered. The data processor is only liable for damages caused by data processing if it failed to comply with obligations specifically imposed on data processors under the law, or if it disregarded or acted contrary to the data controller's lawful instructions. If multiple data controllers or multiple data processors or both the data controller and data processor are involved in the same data processing and are liable for damages caused by data processing, each data controller or data processor bears joint and several liability for the entire damage. The data controller or data processor is exempt from liability if they prove that they bear no responsibility in any way for the event causing the damage.

VII. Legal enforcement opportunities:

1. Contact the Data Protection Officer with your questions and observations at the contacts detailed in point I of this Data Processing Notice.

2. Right to turn to court: In case of violation of their rights, the data subject can turn to court against the data controller. The court handles the case out of turn.
3. Data protection authority procedure: Complaints can be made to the National Data Protection and Freedom of Information

Authority: Name: National Data Protection and Freedom of Information Authority

Registered office: 1055 Budapest, Falk Miksa utca 9-11.

Mailing address: 1363 Budapest, P.O. Box: 9.

Phone: +36 (1) 391-1400

Fax: +36 (1) 391-1410

Email: ugyfelszolgalat@naih.hu

Website: http://www.naih.hu

ANNEX

Definitions used in this Data Processing Notice

1. personal data: any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
2. processing: any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
3. restriction of processing: the marking of stored personal data with the aim of limiting their processing in the future;
4. profiling: any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;
5. controller: the legal person which, alone or jointly with others, determines the purposes and means of the processing of personal data;
6. processor: a legal person which processes personal data on behalf of the controller;
7. recipient: a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not;
8. third party: a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;
9. the data subject's consent: any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;
10. processing: performing technical tasks related to data processing operations, regardless of the method and tool used to perform the operations, and the place of application, provided that the technical task is performed on the data;
11. data deletion: making data unrecognizable in such a way that their restoration is no longer

possible;

12. EEA State: a Member State of the European Union and another State Party to the Agreement on the European Economic Area, furthermore the state whose nationals enjoy the same status as nationals of a State Party to the Agreement on the European Economic Area based on an international agreement concluded between the European Union and its Member States, and a State not Party to the Agreement on the European Economic Area;
13. data subject: any identified natural person, or natural person who can be identified - directly or indirectly - based on personal data;
14. user: the natural person who registers on the Service Provider's website or purchases without registration;
15. third country: any state that is not an EEA State;
16. disclosure: making personal data accessible to anyone.