Effective from: July 1, 2025

I. The Data Controller (Service Provider)

Name of the Service Provider:	InterTicket Ltd.
Headquarters and postal address:	1139 Budapest, Váci út 99.
Registering authority:	Budapest Court as Court of Registration
Company registration number:	Cg. 01-09-736766
Tax number:	10384709-2-41
Email address:	interticket@interticket.hu
Website address:	www.jegy.hu
Customer service availability:	Through chat application, which can be accessed here
Customer service email address:	interticket@interticket.hu For online events (live streaming, video): online@interticket.hu
Complaint handling location and contact details:	1139 Budapest, Váci út 99. Balance Building Through chat application, which can be accessed here interticket@interticket.hu On working days between 10:00 - 16:00
Hosting service provider name:	T-Systems Datapark
Hosting service provider address:	1087 Budapest, Asztalos Sándor u. 13.
Data protection registration identifier:	NAIH-54216/2012.

Name of the Service Provider:	InterTicket Ltd.
Data Protection Officer email:	adatvedelmi.tisztviselo@interticket.hu

II. Data Protection Principles Applied by the Company

1. The Service Provider, as data controller, undertakes to ensure that all data processing related to its activities complies with the requirements set out in this policy and in the applicable national legislation, as well as in the legal acts of the European Union.

2. The Service Provider operates an online internet system primarily to facilitate the purchase of tickets and season passes for various theatrical, musical, sporting and other events, as well as related online product and service sales (purchase of vouchers, books, audio carriers, parking tickets, etc.). The Service Provider is not the operator of the website; under the contract between the two parties, it only provides the ticket sales service on the given website. The website operator or the event organizer is entitled to provide other services on their own website - beyond the ticket sales service detailed in this Data Protection Policy - to sell other products, or to sell tickets that do not come from the Service Provider's system. This Data Protection Policy naturally does not apply to these services and product sales, as this Data Protection Policy only sets out the data protection rules related to the ticket and other product or service sales activities provided by the Service Provider. In terms of ticket sales, the individual websites managed by the Service Provider may differ based on the decisions of the website operator. Information about the Service Provider's data processing is continuously available on the ticket sales pages of the website. The detailed Data Protection Policy regarding the Service Provider's data processing is also continuously available in the footer of the Jegy.hu website operated by the Service Provider.

3. The Service Provider is entitled to unilaterally modify this Data Protection Policy. In case of modification of the Data Protection Policy, the Service Provider informs the User of the changes by publishing them on the website and on the Jegy.hu page. By using the service after the modification takes effect, the User accepts the modified Data Protection Policy.

4. The Service Provider is committed to protecting the personal data of its customers and partners, and considers respecting its customers' right to informational self-determination as highly important. The Service Provider treats personal data confidentially and takes all security, technical and organizational measures that guarantee the security of the data. The Service Provider's data processing practices are contained in this Data Protection Policy.

5. The Service Provider's data protection principles are in accordance with the current legislation on data protection, particularly with 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 CXXXVI of 2007 - 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 requirements and certain restrictions of commercial advertising activities (Advertising Act).

6. The Service Provider uses personal data based on the legal basis in the GDPR and exclusively for specified purposes.

7. The Service Provider undertakes to make a clear, attention-grabbing and unambiguous statement before collecting, recording, or processing any Personal Data of its Users, informing them of 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 of the purpose of the Data Processing and who will process or handle the Personal Data.

8. In all cases where the Service Provider intends to use the provided Personal Data for a purpose other than the original purpose of data collection, it will inform the User of this and obtain their prior, express consent, or provide them with the opportunity to prohibit such use.

III. The legal basis, purpose and scope of data processing, the duration of data processing, and persons entitled to access personal data

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

a) The data subject has given consent to the processing of their 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 (performance of contract);

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 the case of data processing based on voluntary consent, data subjects may withdraw this consent at any stage of data processing.

3. Incapacitated and partially incapacitated minors may not use the services through the Service Provider's system.

4. In certain cases, the processing, storage, and transfer of a certain set of provided data is required by law, of which Users will be specifically notified.

5. We draw the attention of those providing data to the Service Provider that if they provide personal data other than their own, it is the responsibility of the data provider to obtain the consent of 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, and the collection and processing of data must be fair and lawful. Only personal data that is essential for achieving the purpose of data processing, suitable for achieving the goal, can be processed. Personal data may only be processed to the extent and for the time 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 tickets, vouchers, books, audio carriers, parking tickets, etc.) - purchase transaction, admission, notification (one-time purchase)

Purpose of data processing: The purpose of data processing is to provide the webshop service available on the website, to process the order, to serve it, to document the purchase and payment, and to fulfill accounting obligations. The purpose of data processing is also to identify the User as a ticket buyer, as well as to fulfill the ordered service, to send related notifications (technical notifications related to the performance, such as changes to the performance, cancellation, time changes, parking information, etc.), to enable payment processing with the help of the payment provider, to register users, to distinguish them from each other, to transfer admission data to the event organizer, and to fulfill the contract.

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

Scope of processed data: first and last name, phone number (data required by the payment provider, but in case of a change in program, venue, or time, it also allows our customer service or the event organizer to immediately notify the ticket buyer), email address, password provided during pre-registration, delivery address if home delivery is requested, transaction number, date and time, customer code, gift voucher number, culture voucher number.

The scope of processed data also includes - in case the ticket is personalized based on the decision of the event organizer - the name of the legitimate user of the ticket and any other personal data possibly required by the event organizer. Considering that the ticket buyer may differ from the legitimate user of the 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 statements regarding data processing, and that the data subject has previously been familiarized with the data processing rules.

Deadline for data deletion: 210 days after the last performance featured in the transaction, in case the performance is held at a specified time. In case of an event without a date, the data will be deleted 18 months after the transaction date. If a transaction includes both performances with a date and without a date, we store the transaction-related data until the latest date calculated according to the above. If a legal dispute arises in connection with the purchase transaction, the Service Provider will retain the data for the duration of the dispute; the legal basis for this is the Service Provider's legitimate interest, GDPR Article 6(1)(f).

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

Source of personal data: the data subject.

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

7.A. If a legal dispute arises in connection with 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)(f). In all other respects, the rules set out in point 7 apply to this data processing as well.

If due to potential ticket refunds or for other reasons, the buyer's ticket or other product price needs to be refunded, and the buyer did not provide bank details during the 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 data subject's voluntary consent (GDPR Article 6(1)(a)). In all other respects, the rules set out in point 7 apply to this data processing as well.

7.B. For certain events, the event organizer may request additional data during ticket or season ticket sales. This may be due to special security checks at the 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 operations - based on a data processing agreement concluded with the event organizer - INTERTICKET Ltd. acts as a data processor. The information regarding the processing of these data is prepared by the event organizer as the data controller, the link of which is published on the website used for the purchase.

8. Online season ticket purchase/renewal (- service not available on all websites)

Purpose of data processing: providing the webshop service related to season ticket purchases, gift card/discount card purchases, processing orders, serving them, documenting purchases and payments, fulfilling accounting obligations. The purpose of data processing is also to identify the user, as well as to fulfill the ordered service, to send related notifications, to enable payment processing with the help of the payment provider, to register users, to distinguish them from each other, to keep records of the balance on the card, to keep records of purchases made with the card, to keep records of discounts and privileges associated with the card, to ensure rights associated with the season ticket (including renewal pre-rights if provided by the event organizer), to fulfill the contract. The purpose of data processing is also to provide information about the annual renewal opportunity of the season ticket (via email or postal mail), to send reminders about the next season ticket performance (via email or postal mail), in case of free season tickets, to send information twice a month about the performances and events at the venue (via email form) - to help the User make their choice.

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

Scope of processed data: first and last name, phone number (data required by the payment provider, but in case of a change in program, venue, or time, it also allows our customer service or the event organizer to immediately notify the ticket buyer), email address, password provided during pre-registration, delivery address if home delivery is requested, 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 referred to as season tickets) is personalized based on the decision of the event organizer - the name of the legitimate user of the season ticket and any other personal data possibly required by the event organizer. Considering that the season ticket buyer may differ from the legitimate 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 statements regarding data processing, and that the data subject has previously been familiarized with the data processing rules.

Deadline for data deletion: for season tickets, 36 months after the transaction date. For gift cards, discount cards, and Culture cards, if the card has an expiry date, 6 months from the expiry date; if the card does not have an expiry date, 18 months after the transaction. If a legal dispute arises in connection with the purchase transaction, the Service Provider will retain the data for the duration of the dispute; the legal basis for this is the Service Provider's legitimate interest, GDPR Article

6(1)(f).

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

Source of personal data: the data subject.

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

8.A. If during the data retention period indicated in point 8, a legal dispute arises in connection with the purchase transaction, 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)(f). In all other respects, the rules set out in point 8 apply to this data processing as well.

If due to potential season ticket/ticket refunds or for other reasons, the buyer's season ticket or other product price needs to be refunded, and the buyer did not provide bank details during the 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 data subject's voluntary consent (GDPR Article 6(1)(a)). In all other respects, the rules set out in point 8 apply to this data processing as well.

8.B. For certain events, the event organizer may request additional data during ticket or season ticket sales. This may be due to special security checks at the 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 operations - based on a data processing agreement concluded with the event organizer - INTERTICKET Ltd. acts as a data processor. The information regarding the processing of these data is prepared by the event organizer as the data controller, the link of which is published on the website used for the purchase.

9. Invoicing

Purpose of data processing: issuing accounting documents related to purchase transactions and storing them within the time limits specified by law.

Legal basis of data processing: compliance with a legal obligation, GDPR Article 6(1)(c).

Scope of processed data: first and last name, billing address provided for invoice issuance, transaction number, date and time, content of the document, tax number (if provided by the buyer), and email address for sending and possibly resending the invoice.

Deadline for data deletion: The duration of data processing: 8 years, or the period specified in the current tax and accounting legislation.

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

Source of personal data: the data subject.

Recipients of personal data, categories of recipients: the 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: Számlázz.hu, KBOSS.hu Ltd. (tax number: 13421739-2-13, company registration number: 13-09-101824, headquarters: 2000 Szentendre, Táltos u. 22/b).

10. Cookie Management

A cookie is an alphanumeric information package with variable content sent by the webserver, which is stored on the User's computer and is stored for a predetermined validity period. The use of cookies allows for querying certain user data and tracking internet usage. Cookies help track the data subject User's interests, internet usage habits, and website visit history to optimize the User's shopping experience. Since cookies function as a kind of label that allows the website to recognize returning visitors, their use can also store valid usernames and passwords on the given page. If the browser returns a previously saved cookie, the cookie manager service provider has the opportunity to connect the user's current visit with previous ones, but only in terms of its own content.

With the help of information sent by cookies, web browsers are more easily recognizable, making it possible for Users to receive relevant and "personalized" content. Cookies make browsing more convenient, including online data security needs and relevant advertisements. With the help of cookies, the Service Provider can also create anonymous statistics about the habits of site visitors, enabling us to better personalize the site's appearance and content.

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

-Temporary cookies - session cookies essential for using the site. Their use is essential for navigating the website, for the functionality of the website. Without accepting these, the website or parts of it may not appear, browsing becomes hindered, and adding tickets to the cart and bank payment cannot be properly implemented.

-Permanent cookies, which, depending on the web browser's settings, remain on the device for a longer period or until the User deletes them. Among these, we can talk about internal or external cookies. If the Service Provider's web server installs the cookie and the data is forwarded to its own database, we talk about an internal cookie. If the cookie is installed by the Service Provider's web server, but data is transferred to an external service provider, we talk about an external cookie. Such external cookies are also third-party cookies, which are placed in the User's browser by a third party. These are placed in the browser if the visited website uses the services provided by a third party. The purpose of permanent cookies is to ensure the highest possible functioning of the given page in order to increase the user experience.

During the visit to the website, the User can give their consent for permanent cookies to be stored on the User's computer and for the Service Provider to access them by clicking on the cookie warning button on the login page.

The User can set and prevent cookie-related activities using the browser program. Cookie management is usually available in the browsers' Tools/Settings menu under Privacy/History/Custom Settings, labeled as cookie, cookie, or tracking. However, we would like to point out again that without the use of cookies, the User may not be able to use all the services of the website, especially payment services. For more information about cookies, click on the link in the cookie warning bar that appears on the Jegy.hu page.

Purpose of data processing: conducting payment transactions with the payment provider, identifying users, distinguishing them from each other, identifying users' current sessions, storing data provided during those sessions, preventing data loss, identifying users, tracking them, and web analytics measurements.

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

Scope of processed data: identification number, date, time, and the previously visited page.

Duration of data processing: temporary cookies are stored until the user closes all browsers of that type. Permanent cookies are stored on the user's computer for 1 year or until the User deletes them.

Possible consequences of failing to provide data: inability to fully use the website's services, failure of payment transactions, inaccuracy of analytical measurements.

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

Recipients of personal data, categories of recipients: none.

This website uses Microsoft Clarity, a web analytics tool provided by Microsoft Ireland Operations Ltd. (One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, Ireland). Clarity allows for analyzing website traffic and user interactions. The information obtained helps us improve our website's usability and user experience. The data collection process is carried out through cookies.

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

Collected data is automatically deleted after 13 months. Fields containing sensitive information (such as forms, search fields) are blurred during data collection, and their content is not recorded.

In certain cases, data may also be transferred to the United States, which is a third country outside the European Union and the European Economic Area. Microsoft Corporation has the appropriate data protection certificates, so the data transfer complies with GDPR requirements.

Data processing is based on the user's consent, in accordance with GDPR Article 6(1)(a). The user is entitled to withdraw their consent at any time. Withdrawal of consent does not affect the legality of data processing operations performed prior to the withdrawal.

11. Statistical Data

The Service Provider may use the data for statistical purposes. The use of data in statistically aggregated form shall not contain the name of the data subject user or any other data suitable for their identification in any form.

12. Data Technically Recorded During the Operation of the System

The technically recorded data includes the data of the User's login computer that is generated during the use of the service and is logged by the data controller's system as an automatic result of technical processes (e.g., IP address, session ID). Due to the operation of the internet, these automatically recorded data are automatically logged by the system without a separate statement or action by the User - by using the internet. These data cannot be linked to other User personal data - except in cases where such connection is made mandatory by law. Only the Data Controller has access to the data. Log files that are automatically technically recorded during the operation of the system are stored in the system for a period justified from the point of view of ensuring the system's operation.

13. Recording of Phone Conversations

The Service Provider records incoming and outgoing phone calls to customer service.

Purpose of data processing: enforcement of the rights of customers and the data controller,

providing evidence for potential legal disputes, providing evidence for subsequent verification and supporting the irrecoverability of a claim, as well as subsequent proof of agreements, quality assurance, and fulfillment of legal obligations.

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

Scope of processed data: identification number, phone number, called number, date and time of the call, recording of the phone conversation, and other personal data provided during the conversation.

Deadline for data deletion: five years.

Possible consequences of failing to provide data: lack of telephone assistance.

Source of personal data: the data subject.

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

14. The Service Provider's Customer Correspondence (Email) and Chat Communication

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

Purpose of data processing: to provide customer service assistance and complaint handling for buyers and users.

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

Scope of processed data: The Service Provider processes the email and chat communication received by it 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 set out in this notice. During chat communication, providing an email address is mandatory because this allows the Service Provider to coordinate parallel complaint handling. Providing additional personal data (name, phone number, etc.) may become necessary during complaint handling for the substantive handling of the request.

Deadline for data deletion: The Service Provider processes the provided data until the User - with an individual request to the Service Provider's customer service - requests its deletion. If the data subject does not state otherwise, the Service Provider deletes the data three years after the complaint is closed. If legislation prescribes a mandatory retention period for documents created during complaint handling, the Service Provider shall keep the relevant documents until the end of the document retention period prescribed by the current legislation.

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

Source of personal data: the data subject.

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

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

15. Web Analytics Measurements

Google Analytics, as an external service provider, helps with the independent measurement of website traffic and other web analytics data. For information about the handling of measurement data, please visit: http://www.google.com/analytics. The Service Provider uses Google Analytics data exclusively for statistical purposes, to optimize the operation of the site.

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

Recipients of personal data, categories of recipients: none.

16. Other Data Processing

We provide information about data processing not listed in this notice at the time the data is collected. We inform our customers that courts, prosecutors, investigative authorities, regulatory authorities, administrative authorities, the National Authority for Data Protection and Freedom of Information, and other bodies authorized by law may contact the Service Provider to provide information, communicate data, transfer data, or make documents available. The Service Provider provides personal data to authorities - if the authority has specified the exact purpose and scope of data - only to the extent and to the degree that is essential for the realization of the purpose of the request.

17. The Data Controller does not verify the personal data provided to it. The person providing the data is solely responsible for the accuracy of the provided data. When providing an email address, any user also assumes responsibility that they are the only one using the service from the provided email address. Due to this responsibility, all liability related to logins from a given email address is exclusively borne by the user who registered that email address. If the User provides personal data other than their own, it is their responsibility to obtain the consent of the data subject.

18. Those entitled to access personal data are the Service Provider's employees or individuals in a contractual relationship with the Service Provider, employees of the courier service involved in product delivery (if the buyer requested delivery), and Data Processors.

IV. Data Transfer, Designation of Data Processors

1. By using the service, the User agrees that the Service Provider may transfer the data to the following partners. The legal basis for data transfer: performance of the contract, GDPR Article 6(1)(b).

-To the organizer of the given event, so that the event organizer can directly and immediately inform about the cancellation of the event, changes in time, or any important circumstances affecting the viewer, and in case of cancellation, can directly handle the refund or exchange of tickets, admit the buyer to the event, and fulfill the contract (proper execution of the performance). With the data transfer, the organizer of the given event becomes an independent data controller with respect to the transferred data. Data transfer may also take place in such a way that the Service Provider allows appropriate access to its ticket management IT system ("Tickets system") to the event organizer.

-To the service provider providing the technical conditions for invoicing, as Data Processor, which is: Számlázz.hu, KBOSS.hu Ltd. (tax number: 13421739-2-13, company registration number: 13-09-101824, headquarters: 2000 Szentendre, Táltos u. 22/b).

-Tasks related to sending emails to Users, and if the data subject has given permission for profiling, tasks related to this, are performed as data processor by Wanadis Commercial and Service Provider Ltd. (1118 Budapest, Rétköz u. 7.), or Emarsys eMarketing Systems AG (Marzstrasse 1, 1150 Vienna, Austria) based on a contract with the data controller.

-For all transactions where the product/service fee can be paid via online banking service, the Service Provider transfers the data to the financial institutions involved in the purchase process, which handle the payment. The transfer of the listed data is required by the financial institution for processing the payment; the scope of requested data varies by financial institution. The Service Provider does not access personal data provided on the financial institution's own data request pages. The following financial institutions may appear as payment providers on the website; the table also includes the data that the given financial institution requires to be transferred. (Not all payment financial institutions appear on the website at a given time.) The data required by financial institutions may change, especially with regard to the introduction of so-called strong customer authentication - with different deadlines by bank.

Payment Provider Name	**Transferred Data**
OTP	transaction amount, name, address, IP number
SimplePay Ltd. / SIMPLE	email address, phone number
CIB	transaction amount
K&H	transaction amount, currency
Barion	name, email address

-SimplePay Ltd.. / SIMPLE / SimplePay Privacy Policy can be viewed at the following link: https://simplepay.hu/adatkezelesi-tajekoztatok/

-Barion Payment Zrt. is an institution supervised by the National Bank of Hungary, its license number: H-EN-I-1064/2013.

-If the User purchases with a specific discount-providing tool, the Data Controller forwards the buyer data required by the company or financial institution providing the discount. For information about the related data processing rules, the User can directly request information from the company providing it. The Data Controller processes the identifiers and other data of such tools automatically only to the extent that the provider company requires it - for executing the purchase and providing the discounts. The following companies and financial institutions may appear on the website; the table also includes the data that the given company or financial institution requires to be transferred. (Not all payment providers or companies appear on the website at a given time.)

Payment Provider Name	**Transferred Data**
OTP SZÉP card	transaction amount, name, address, email address, IP number
Sponsorem	transaction amount, card number, currency

Payment Provider Name	Transferred Data
Supershop	transaction amount, card number, name, date of birth, email address
MKB SZÉP	card transaction amount
Cafe T-rend	transaction amount, card number

-For major sporting events, if the User requests a wheelchair ticket or accompanying escort ticket, or initiates name change on the ticket, they need to fill out a Google Form. The data received through the Form is deleted by the Service Provider on the third day after the Match. For Google's Privacy Policy and Terms of Service, click here.

2. The Service Provider, as Data Controller, is entitled and obliged to transfer all personal data in its possession that it has properly stored to the competent authorities if it is obliged to do so by law or by a final authority order. The Data Controller cannot be held responsible for such data transfer and the consequences arising from it.

3. The Service Provider performs data transfers not indicated above only with the prior and informed consent of the User.

V. Method of Storing Personal Data, Security of Data Processing

1. The Service Provider's computer systems and other data storage locations are located at its headquarters and at its data processors.

2. In choosing and operating the IT tools used for processing personal data during service provision, the Service Provider ensures that the processed data:

a) is accessible to those authorized (availability);

b) its authenticity and authentication are ensured (authenticity of data processing);

c) its integrity can be verified (data integrity);

d) is protected against unauthorized access (confidentiality of data).

3. The Service Provider protects the data with appropriate measures, particularly against unauthorized access, alteration, transmission, disclosure, deletion or destruction, as well as against accidental destruction, damage, and inaccessibility due to changes in the technology used.

4. To protect electronically managed data sets in its various records, the Service Provider ensures through appropriate technical solutions that the stored data - except where permitted by law - cannot be directly linked and associated with the data subject.

5. Taking into account the state of the art, the Service Provider takes technical, organizational, and structural measures to protect the security of data processing that provide a level of protection appropriate to the risks associated with data processing.

6. During data processing, the Service Provider maintains:

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

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

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

7. The IT system and network of the Service Provider and its partners are equally protected against computer-aided fraud, espionage, sabotage, vandalism, fire and flood, as well as computer viruses, computer break-ins, and other attacks. The operator ensures security through server-level and application-level protection procedures.

8. During the automated processing of personal data, the Service Provider takes additional measures to ensure:

a) prevention of unauthorized data entry;

b) prevention of the use of automated data processing systems by unauthorized persons using data transmission equipment;

c) the ability to check and establish to which bodies personal data has been or may be transmitted using data transmission equipment;

d) the ability to check and establish which personal data has been entered into automated data processing systems and when and by whom;

e) the recoverability of installed systems in case of malfunction; and

f) that a report is generated on errors occurring during automated processing.

9. In determining and applying measures to ensure data security, the Service Provider takes into account the state of technological development. Among several possible data processing solutions, it must choose the one that provides a higher level of protection for personal data, unless it would represent a disproportionate difficulty.

10. The Service Provider takes technical, organizational, and structural measures to protect the security of data processing that provide a level of protection appropriate to the risks associated with data processing.

11. Electronic messages transmitted over the internet, regardless of protocol (email, web, ftp, etc.), are vulnerable to network threats that can lead to unfair activity or disclosure, modification of information. To protect against such threats, the Service Provider takes all reasonably expected precautions. It monitors the systems to record any security deviations and provide evidence for any security event. System monitoring also allows for checking the effectiveness of the precautions applied. However, the Internet is, as is known to Users, not 100% secure. The Service Provider is not liable for any potential damages caused by unavoidable attacks despite the greatest expected care.

VI. Rights of Data Subjects

1. The data subject may request information about the processing of their personal data, and may also request the rectification of their personal data, or - except for mandatory data processing - its deletion, withdrawal, may exercise their right to data portability and objection in the manner indicated when the data was collected, or at the Service Provider's contact details given in Section I

of this Data Protection Policy.

Changes in personal data or requests for the deletion of personal data may be communicated via the registered email address or by postal mail through a private document with full probative force containing a written statement. In addition, some personal data may be modified by changes made on the page containing the personal profile.

2. Right to information: The Service Provider takes appropriate measures to provide the data subjects with all information referred to in Articles 13 and 14 of the GDPR and all communications under Articles 15 to 22 and 34 in a concise, transparent, intelligible and easily accessible form, using clear and plain language. The right to information may be exercised in writing through the contact details given in Section I of this Data Protection Policy. Upon request, after verifying their identity, the data subject may also be given information orally.

3. The data subject's right of access: The data subject has the right to obtain from the controller confirmation as to whether or not personal data concerning them are being processed, and, where that is the case, access to the personal data and the following information:

-the purposes of the processing;

-the categories of personal data concerned;

-the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organizations;

-the planned period for which the personal data will be stored;

-the right to rectification, erasure or restriction of processing and the right to object;

-the right to lodge a complaint with a supervisory authority;

-information about the data sources;

-the fact of automated decision-making, including profiling, as well as meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

The Data Controller considers a request for information sent by email to be authentic only if it is sent from the User's registered email address - unless the data subject identifies themselves in another credible way. Requests for information should be sent by email to interticket@interticket.hu.

4. In the case of transfers of personal data to a third country or to an international organization, the data subject shall have the right to be informed of the appropriate safeguards relating to the transfer.

5. The Service Provider shall provide a copy of the personal data undergoing processing to the data subject. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. If the data subject makes the request by electronic means, the information shall be provided by the Service Provider in electronic form. The controller shall provide the information within a maximum of one month from the submission of the request.

6. Right to rectification: The data subject may request the rectification of inaccurate personal data concerning them and the completion of incomplete data processed by the Service Provider.

If the personal data does not correspond to reality, and the correct personal data is available to the data controller, the personal data shall be rectified by the data controller.

7. Right to erasure: The data subject shall have the right to obtain from the Service Provider the erasure of personal data concerning them without undue delay where one of the following grounds applies:

-the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

-the data subject withdraws consent on which the processing is based, and there is no other legal ground for the processing;

-the data subject objects to the processing and there are no overriding legitimate grounds for the processing;

-the personal data have been unlawfully processed;

-the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;

-the personal data have been collected in relation to the offer of information society services.

After fulfilling a request for the deletion or modification of personal data, the previous (deleted) data can no longer be restored.

8. Erasure of data cannot be initiated if the processing is necessary for one of the following reasons: to fulfill a legal obligation under Union or Member State law applicable to the data controller, or for the presentation, enforcement, or defense of the Service Provider's legal claims.

9. Right to restriction of processing: At the request of the data subject, the Service Provider restricts processing if one of the following conditions is met:

-the data subject contests the accuracy of the personal data, in which case the restriction applies for a period enabling the controller to verify the accuracy of the personal data;

-the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;

-the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defense of legal claims; or

-the data subject has objected to processing; in this case, the restriction applies for the period during which it is verified whether the legitimate grounds of the controller override those of the data subject.

10. Where processing has been restricted, such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defense of legal claims or for the protection of the rights of another natural or legal person. The Service Provider shall inform the data subject before the restriction of processing is lifted.

11. Right to data portability: The data subject shall have the right to receive the personal data concerning them, which they have provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller.

12. Right to object: The data subject shall have the right to object, on grounds relating to their particular situation, at any time to processing of personal data concerning them which is based on the legitimate interests pursued by the controller or by a third party, including profiling based on those provisions. In case of objection, the controller shall no longer process the personal data unless it demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defense of legal claims. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning them for such marketing, which includes profiling to the extent that it is related to such direct marketing. If the data subject objects to the processing of personal data for direct marketing purposes, the data shall no longer be processed for such purposes.

13. Automated individual decision-making, including profiling : The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or similarly significantly affects them. This right does not apply if the processing:

-is necessary for entering into, or performance of, a contract between the data subject and the data controller;

-is authorized by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or

-is based on the data subject's explicit consent.

14. Right to withdraw consent: The data subject shall have the right to withdraw their consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.

15. Procedural rules: The Service Provider shall, without undue delay, but in any event within one month of receipt of the request, inform the data subject of the action taken on a request under Articles 15 to 22 of the GDPR. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The Service Provider shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where the data subject makes the request by electronic means, the information shall be provided by electronic means unless otherwise requested by the data subject.

16. If the Service Provider does not take action on the request of the data subject, it shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy.

17. The Service Provider shall provide the requested information and communication free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the Service Provider may either charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested, or refuse to act on the request.

18. The Service Provider shall communicate any rectification, erasure of personal data or restriction of processing to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The Service Provider shall inform the data subject about those recipients if the data subject requests it.

19. The Service Provider shall provide a copy of the personal data undergoing processing to the data subject. For any further copies requested by the data subject, the Service Provider may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, the information shall be provided in electronic form, unless otherwise requested by the data subject.

20. Compensation and damages: Any person who has suffered material or non-material damage as a result of an infringement of the data protection regulation shall have the right to receive compensation from the controller or processor for the damage suffered. A processor shall be liable for the damage caused by processing only where it has not complied with obligations specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller. Where more than one controller or processor, or both a controller and a processor, are involved in the same processing and are responsible for any damage caused by processing, each controller or processor shall be held liable for the entire damage. The controller or processor shall be exempt from liability if it proves that it is not in any way responsible for the event giving rise to the damage.

VII. Legal Remedies:

1. For your questions or comments, please contact the Data Protection Officer at the contact details provided in Section I of this Data Protection Policy.

2. Right to judicial remedy: In case of infringement of their rights, the data subject may take legal action against the data controller. The court shall handle the case as a priority.

3. Data protection authority proceedings: Complaints can be filed with the National Authority for Data Protection and Freedom of Information:

Name: National Authority for Data Protection and Freedom of Information

Headquarters: 1125 Budapest, Szilágyi Erzsébet fasor 22/C.

Postal address: 1530 Budapest, Pf.: 5.

Phone: 06.1.391.1400

Fax: 06.1.391.1410

Email: ugyfelszolgalat@naih.hu

Website: http://www.naih.hu

APPENDIX

Definitions used in this Data Protection Policy

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, organization,

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 analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, 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 authorized to process personal data;

9. consent of the data subject: any freely given, specific, informed and unambiguous indication of the data subject's wishes by which they, by a statement or by a clear affirmative action, signify agreement to the processing of personal data relating to them;

10. data processing: the performance of technical tasks related to data processing operations, regardless of the method and means used to perform the operations and the place of application, provided that the technical tasks are performed on the data;

11. data erasure: making the data unrecognizable in a way that their restoration is no longer possible;

12. EEA State: a Member State of the European Union and a State party to the Agreement on the European Economic Area, as well as a State whose citizens enjoy the same status as citizens of States party to the Agreement on the European Economic Area based on an international agreement 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 natural person identified or identifiable - directly or indirectly - on the basis of specific personal data;

14. user: a natural person who registers on the Service Provider's website or makes purchases without registration;

15. third country: any State that is not an EEA State;

16. disclosure: making personal data available to anyone;