Effective from 10 Dec 2020

I. Data Controller (Service Provider)

Service Provider's Name:	INTERTICKET Ltd.
Seat and Postal Address:	1139 Budapest, Váci út 99.
Registration Authority:	Metropolitan Court acting as Registry Court
Company Registration Number:	Cg. 01-09-736766
Tax number:	10384709-2-41
E-mail address:	interticket@interticket.hu
Website:	www.jegy.hu
Customer Service availability	Please send your message using the Chat function
Customer Service e-mail address:	interticket@interticket.hu in case of live streaming (video): online @interticket.hu
Location and Contact for Complaints:	1139 Budapest, Váci út 99. Balance Building Please send your message using the Chat function interticket@interticket.hu Weekdays between 10.00 and 16.00
Name of Data Storage Provider:	T-Systems Adatpark
Address of Data Storage Provider:	1087 Budapest, Asztalos Sándor u. 13.
Data Protection Identifier:	NAIH-54216/2012.
Data Protection Officer's e-mail address:	adatvedelmi.tisztviselo@interticket.hu

II. Privacy policy employed by the Company

1. As a data controller, the Service Provider undertakes that all data processing related to its activities complies with the requirements specified in these regulations and in national legislation and the legislation of the European Union.

2. Information regarding management of data by Service Provider is continuously available in the footer of the starting page of the Jegy.hu website operated by the Service Provider.

3. Service Provider reserves the right to modify the Prospectus on Data Management unilaterally. In the event of modification, Service Provider shall notify the User by publishing the changes on the jegy.hu website. User accepts the revised Prospectus on Data Management by using the service after the modification takes effect.

4. In order to protect the personal information of its customers and partners, Service Provider considers it important to respect its clients` right to information self-determination. Service Provider shall treat the personal data in a confidential manner and shall apply all security, technical and organizational measures that guarantee the security of data. Service Provider's data management

practices are contained in this Prospectus on Data Management.

5. Service Provider's principles on privacy are in line with the current data protection legislation, thus especially with the following:

- Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information (hereinafter referred to as Privacy Act);

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (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 2000 on the Prevention and Combating of Money Laundering and Terrorist Financing (PCMLTF);

- Act CVIII of 2001 on Certain Aspects of Electronic Commerce and Information Society Services (E-Commerce Act);

- Act XLVIII of 2008 on the Basic Requirements and Certain Restrictions of Commercial Advertising Activities (Business Advertising Act).

6. Service Provider shall only use personal information based on the legal basis included in the GDPR and solely for the specified purpose.

7. Service Provider is committed that before collecting, recording or handling any personal data of its customers it will publish clear, soliciting Customers' attention and unambiguous statements which inform Customers of the ways their data is recorded, their purpose and principles. If providing personal data is compulsory by law, the relevant rules and regulations must also be indicated. Those involved must also be informed of the purposes of data processing and by whom the personal data will be handled and processed.

8. If the Company intends to use the personal data provided for purposes other than it was originally provided for, the Company must inform the customer and obtain their express, prior consent and make it possible for the customer to prohibit such use.

III. The legal basis and purpose of data processing, the scope of the processed data, length of data processing, entities entitled to learn personal data

1. Service Provider`s data processing is based on the following legal rights (Paragraph 1 of Section 6 of the GDPR):

a) the individual has given their consent to the processing of their personal data for one or more specific purpose (voluntary consent);

b) data processing is necessary for the fulfilment of such a contract where the affected person is one of the parties or if it necessary to carry out steps required by the affected person before the contract is entered into (fulfilment of the contract);

c) data processing is necessary to fulfil the legal obligation for the data controller (legal obligation);

d) data processing is necessary to validate legitimate interest of data controller or a third party (legitimate interest).

2. In case of data processing based on voluntary consent the affected person may withdraw their consent at any time during data processing.

3. Individuals with particular disabilities and children with limited ability may not use services via Service Provider`s system.

4. In some cases processing, storage and forwarding are made mandatory by law of which we will notify users separately.

5. Please note that if data provider is not providing their own personal data, it is their responsibility to obtain the consent of the person concerned.

6. Personal data may only be handled for a specific purpose. The purpose of data management must be met, data entry and management must be fair and legitimate at all stages of data processing. Only personal data that is essential for achieving the purpose of data processing can be handled to achieve this goal. Personal data can only be handled to the extent and for the duration required to achieve the goal. Service Provider will not use personal data for purposes other than those indicated.

7. Online web shop services (purchase of tickets, vouchers, books, audio recording, parking tickets, etc.) – purchase transaction, entry, notification (one-off purchase)

Purpose of data processing: to ensure the provision of a web shop service on the web site, the order, to fulfil the order, to document the purchase and payment and to fulfil the accounting obligation. Further purpose of data processing is to identify the user as a ticket buyer, as well as to deliver the ordered service and to send notifications (technical notifications related to the performance, such as changes to the performance, cancellation, change of times, parking information etc.), to carry out payment through payment service provider, to register users, differentiate between users, to transfer access data to the event organizer, and to fulfil the contract

Grounds for data processing: fulfilment of a contract, subsection b) Paragraph 1 of Section 6 of the GDPR.

Scope of processed data: surname and first name, phone number (optional if customer provides for receiving notifications, email address, password given at pre-registration, delivery address provided for home delivery, the number, date and time of the transaction, customer code, number of the gift card or culture voucher. In case of issuing and renaming name-specific/registered tickets, in addition to the listed data - place of birth, date of birth and possibly other personal data required by the event organizer as a condition for issuing the original name-specific/registered ticket (typically for special sport events, name-specific tickets are used by the organizers, according to the decisions of international sport federations).

Deadline to erase data: 210 days after the last performance in the transaction, supposed that the performance has a specific date. In case of performance without specific date, deadline to erase data is 18 months after the date of transaction. If in the same transaction there are tickets purchased for performances with and without specific date, the later date would be taken into consideration.If a dispute arises in connection with the purchase transaction, Service Provide shall maintain the data for the duration of the dispute; the legal basis of which is legitimate interest of Service Provider, subsection f) of Paragraph 1 of Section 6 of the GDPR.

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

8. Online purchase/renewal of season tickets, gift cards, discount cards, Culture Cards

Purpose of data processing: to ensure the provision of a web shop service on the web site, the order, to fulfil the order, to document the purchase and payment and to fulfil the accounting obligation. Further purpose of data processing is to identify the user as a ticket buyer, as well as to deliver the ordered service and to send notifications (technical notifications related to the performance, such as changes to the performance, cancellation, change of times, parking information etc.), to carry out payment through payment service provider, to register users, differentiate between users, to register the balance on the card, to register purchases made with the card, to register discounts and privileges connected to the card, to provide the rights in connection with the season ticket (including rights for renewal if provided by event organizer), to fulfil the contract. Further purpose of data processing is to provide information on the annual renewal of the season ticket (via email or post), reminder regarding the next performance for the season ticket (via email or post), in case of free season tickets twice monthly notification regarding the events of the venue (via email) to facilitate the choice of User.

Grounds for data processing: fulfilment of a contract, subsection b) Paragraph 1 of Section 6 of the GDPR.

Scope of processed data: surname and first name, phone number (optional if customer provides for receiving notifications, email address, password given at pre-registration, delivery address provided for home delivery, the number, date and time of the transaction, customer code, number and balance of the gift card, number and balance of culture card.

Deadline to erase data: 24 months following the date of the transaction for season tickets. In case of gift cards, discount cards, Culture Cards, deadline to erase data is 6 months following the expiration date, or – if the given card has no expiration date – 18 months following the date of transaction. If a dispute arises in connection with the purchase transaction, Service Provide shall maintain the data for the duration of the dispute; the legal basis of which is legitimate interest of Service Provider, subsection f) of Paragraph 1 of Section 6 of the GDPR. If tax benefits are connected to the purchased card (for instance Culture Card) the data retention period shall be specified in the effective regulations; grounds: subsection c) Paragraph 1 of Section 6 of the GDPR.

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

9. Registration

Purpose of data processing: By choosing a password during the pre-registration process it will be possible for the user to provide their details only once and not at each purchase. Some services are only available to registered users on the web site. Such services include blogging and comment writing, comment rating, and the following functionality (to be notified about artists, venues and events). As a convenience functionality, in a personal menu, User may edit their personal information, view and download their tickets and invoices, follow their comments, already visited pages, reviews, modify following and newsletter subscriptions and if they are part of the membership system, view the balance of their points. Managing multiple personal data stored in the account obviously means profiling as well.

Grounds for data processing: voluntary consent of the affected person, subsection a) Paragraph 1 of Section 6 of the GDPR.

Scope of processed data: email address, password and those personal data that User has provided during purchase or in their account: address, billing address, phone number. Processed data may furthermore be products purchased by User during their orders, date and invoice of the purchases, Comments made by User and their rating, comments, performances, artists, venues rated by the User, artists, venues and performances marked by User to be followed, pages viewed by User,

newsletter subscriptions and balance of membership points collected.

Deadline to erase data: Data provided will be handled by Service Provider until such time as User prohibits use for this purpose by unsubscribing.

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

10. Notification service

The Notification Service allows the ticket buyer, in addition to technical information about the event (technical alerts related to the performance, such as changes to the performance, cancellation, change of times, parking information etc.), to use notification services such as pre-performance reminder, rating following the performance, as well as automated announcements (alerts for leaving the basket, ticket available to buy again, etc.).

Grounds for data processing: voluntary consent of the affected person, subsection a) Paragraph 1 of Section 6 of the GDPR.

Scope of processed data: email address, name, optional phone number if user would like to receive the notifications via text message, Facebook Messenger ID if user would like to receive the notifications via Messenger chatbot.

Deadline to erase data: Data provided will be handled by Service Provider until such time as User prohibits use for this purpose by unsubscribing.

Possible consequences of failure to provide data: User cannot use the convenience functions of the website, not notified of changes.

11. Billing

Purpose of data processing: to issue invoice related to the purchase transaction and to retain such for the duration specified in the relevant laws.

Grounds for data processing: to meet legal obligation, subsection c) Paragraph 1 of Section 6 of the GDPR.

Scope of processed data: first and family name, billing address provided for billing, number, date and time of the transaction, contents of invoice, tax number in case of VAT receipt (if provided by customer).

Deadline to erase data, period of data processing: 8 years or as specified in the currently effective legislation on taxation and accounting.

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

12. Personalized offers, profiling

Purpose of data processing: Profiling helps User to see relevant and personalized offers on the website and in the newsletters` recommendations. Profiling helps data processor to create the most appropriate offers for the customers.

Grounds for data processing: voluntary consent of the affected person, subsection a) Paragraph 1 of Section 6 of the GDPR.

Scope of processed data: email address, name, address, information relating to the use of the website (time of the visit, duration, pages viewed, clicks on the page, search engine usage), basket usage (order identifier, products, product categories, values), purchases (transaction date, value, product, its category, discounts used, method of payment), technical information (IP address, cookie ID, browser type, device type, Google, Facebook, Hotjar, Findgore, Prefixbox identifiers, source page), newsletter and notification message usage information (time of opening the email, its tool, click-through links, purchase data), blog-related data (comments, ratings, click-through links).

The logic of profiling: the offer system offers a list of events to be displayed on the website and in the messages sent by Service Provider that are likely to be the most relevant to the customer.

Deadline to erase data: Data provided will be handled by Service Provider until such time as User prohibits use for this purpose by unsubscribing.

Possible consequences of failure to provide data: offers not relevant to the user are displayed on the website and the newsletters, User cannot use the convenience functions of the website.

13. Electronic newsletter

Purpose of data processing: Sending email newsletters containing advertisements to interested users. If user subscribes to the newsletter, Service Provider can send newsletters at a frequency at its own discretion. Service Provider shall endeavour to offer events relevant to the reader of the newsletter based on user`s place of residence, previous purchases and other data collected through profiling.

Grounds for data processing: voluntary consent of the affected person, subsection a) Paragraph 1 of Section 6 of the GDPR.

Scope of processed data: name, email address, post code, phone number and data collected through profiling.

Deadline to erase data: Data provided will be handled by Service Provider until such time as User prohibits use for this purpose by unsubscribing. To unsubscribe from the newsletter, click the Unsubscribe link at the bottom of the newsletter. The personal data will be deleted within 10 working days of receiving this request.

Possible consequences of failure to provide data: User is not notified of the events.

14. Participation in Service Provider`s loyalty program

Purpose of data processing: to provide participation in the loyalty program offered by Service Provider available to regular users of the Jegy.hu website.

Grounds for data processing: voluntary consent of the affected person, subsection a) Paragraph 1 of Section 6 of the GDPR.

Scope of processed data: name, email address, post code, phone number and data collected through profiling.

Deadline to erase data: Data provided will be handled by Service Provider until such time as User prohibits use for this purpose by unsubscribing.

Possible consequences of failure to provide data: User cannot take part in the loyalty program offered by Service Provider.

15. Cookie management («Cookie»)

Cookies are variable content alphanumeric information packets sent by the web server that is stored on the user's computer and stored for a predetermined validity period. The use of cookies allows to query some data of the website`s visitor and track their internet usage. Cookies help to keep track of user`s interests, internet usage patterns and the website visit history in order to ensure that the user's shopping experience is optimal. Since cookies are used as a kind of tag that allows a web page to recognize a visitor returning to the page, by using them valid username and password for that site can also be stored. If the browser sends back a previously stored cookie, service provider processing the cookie has the ability to link the current visit of the user to previous ones but only to relating to their own content.

The information sent by the cookies makes it easier to recognize web browsers therefore users can receive relevant and "personalized" content. Cookies make browsing more convenient, including online data security needs and relevant advertising. With the help of cookies, Service Provider can also create anonymous statistics on page viewers' habits, so can better customize the look and content of the page.

Service Provider's website uses two types of cookies:

- Temporary Cookies – session use (session–id) cookies necessary for the use of the website. Their use is essential for navigating on and for the functioning of the website. Without them, the site or parts of it will not be displayed, browsing becomes obstructed, placing tickets in the basket or bank payment cannot be properly implemented.

- Permanent cookies that will remain on the device, depending on the settings of the web browser, for a long time or until they are deleted by the user. Within these there are internal and external cookies. Internal cookies are created if Service Provider's server installs the cookie and the data is forwarded to its own database. If the cookie is installed by the Service Provider's server, but the data is forwarded to an external service provider, external cookie is used. Third party cookies placed by a third party in the user's browser (Google Analytics, Facebook Pixel) are external cookies. These are put in the browser if the visited website uses services provided by a third party. The purpose of permanent cookies is to ensure that the site operates at the highest level in order to increase user experience.

When visiting the website User can give their consent to storing permanent cookies stored on their computer that can be accessed by Service Provider by clicking on the cookie alert button on the sign in page.

User can configure and prevent cookie related activities by using the browser program. Use To manage cookies, user can usually use the Cookies or Cookie tracing option in Privacy/History/Custom Settings menu under Tools/Settings menu of their browser. Please note however that without the use of cookies it is possible that User will not be able to every service provided by the website, thus especially the payment options. For further information on cookies please click on the link provided on the cookie alertbanner on Jegy.hu website.

Purpose of data processing: carrying out payment transactions with the payment service provider, identifying and distinguishing users, identifying user's current session, storing data created during the session, preventing data loss, identifying and tracking users, web analytics.

Grounds for data processing: voluntary consent of the affected person, subsection a) Paragraph 1 of Section 6 of the GDPR.

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

Period of data processing: temporary cookies are stored until all websites of the same type are closed. Permanent cookies are stored on user`s computer for a year or until user deletes them.

Possible consequences of failure to provide data: unavailability of certain services of the website, unsuccessful payment transactions, inaccuracies in analytics.

16. Location

If user uses the service from a mobile device (e.g. smartphone), when the application is downloaded the program may ask for permission to use the location as data (egg. when using the "near" feature) for features that require location.

Purpose of data processing: If consent is given by user, the application can provide such personalized searches that takes into account where the user is currently located. The location as data is not stored in data processor`s system it is only facilitating the use of certain functions during a given transaction (more exact search, the "near" feature).

Grounds for data processing: voluntary consent of the affected person, subsection a) Paragraph 1 of Section 6 of the GDPR.

Scope of processed data: the geographical location of user at a certain time, IP address.

Scope of data processing: 3 days

Possible consequences of failure to provide data: inability to use all services of the mobile device

17. Statistics

Data controller can use the data for statistical purposes. The use of data in a statistically aggregated form cannot contain the name or any other identifiable information of the user in any form.

18. Data technically recorded during the operation of the system

Technically recorded data are data from the user's computer that has logged in that are generated when the service is being used and which are logged by the data management system of data controller as automatic results of technical processes (egg. IP address, session ID). Due to way the Internet works, the automatically recorded data will automatically be logged by the system, using the Internet, without a separate declaration or action from the User. The Internet does not work without this automatic server-client communication. Such data cannot be liked to other personal data of the User – with the exception of personal data for compliance with a legal obligation. This data can only be accessed by the data controller. Logs technically, automatically recorded during the operation of the system will be stored in the system for a reasonable period of time necessary for the operation of the system.

19. Recording phone calls

Service provider records incoming and outgoing phone calls of its customer services.

Purpose of data processing: to enforce the rights of customers and data controller, to provide evidence for possible disputes, to provide evidence to support subsequent verification and the possible un-collectability of a claim, and subsequent proof for agreements, quality assurance, compliance with legal obligations.

Grounds for data processing: voluntary consent of the person concerned.

Scope of processed data: identification number, caller`s phone number, called number, data and time of the call, audio recording of the call as well as other personal information provided during the call.

Deadline to erase data: 5 years.

Possible consequences of failure to provide data: inability to access help via phone.

20. Service Provider`s correspondence with customers (email)

If you would like to contact our company you can get in contact with Service Provider on the contact details provided in this information leaflet or via the contacts specified on the website. Service Provider deletes all received emails, together with sender`s name, email address, date, time and other personal data provided in the email no later than 5 years after the disclosure.

21. Web analytics

Google Analytics as an external service provider helps to independently measure website visits and other web analytics data. For detailed information on how measured data is handled please visit the following link: http://www.google.com/analytics. Google Analytics data is used by the Service Provider for statistical purposes only to optimize the functionality of the site.

22. Other data management

We provide information on data management not specified in this document at the time of the registration of such data. Please note that the court, prosecutor, investigating authority, offense authority and administrative authority, National Authority for Data Protection and Freedom of Information, Hungarian National Bank as well as other bodies under the authorization of the legislation may request Service Provider to provide information, provide and hand over data or provide documents. Service Provider shall only disclose personal information to the authorities – if the authority has specified the exact purpose and the scope of data – to the extent necessary for the purposes of the request.

23. Data controller shall not check the provided personal information. The person providing the information will be solely responsible for the compliance of the provided information. When Users provide their email address, they assume responsibility that only they will use the Service from this email address. In this respect the person who registers the email address will be responsible for every login used with the given email address. If User is not providing their own personal data, they have the duty to obtain consent from the affected person.

24. People in the employment of or in contractual relationship with Service Provider, employees of the courier company arranging the delivery of the products as well as the data processors will be entitled to get to know the personal data.

III/A. Special data management related to certain sporting events of major importance

1. According to the agreement between Interticket Ltd. and HFF (Hungarian Football Federation), Interticket Ltd. is entitled to sell tickets for the matches of the Hungarian national team on the order of HFF. The ticketing process and the essential elements of data management were jointly defined by KFF and Interticket, the ticketing process is carried out with the help of HFF, since HFF is the organizer of the matches HFF and Interticket Ltd. act as joint data controllers in ticket sales.

2. Introducing specific data management cases related to sporting events of major importance and the scope of the data managed:

Ticket sales are realized through the following data management process:

a)Ticket purchase online or at the cashier with club card or by providing personal information

b)Verification in the Register of Sports Security (hereinafter: RSS) in the case of sale of tickets by name

c)Checking Fan Club membership, applying discounts

d)Issue of tickets

e)Ticket exchange

f)Transmission of the ticket barcode to the Puskás Arena's access control system

g)Transfer of reporting data to HFF

3. Purchase of tickets [data management pursuant to points a)-d)]

Process, purpose of data management; the identity of the data controller

The purchaser can buy tickets for the matches of the Hungarian national team held in the Puskás Arena both at the cashier and online.

Tickets can be purchased in person through InterTicket's national ticket office network. The contact details of the ticket offices can be found on the Jegy.hu website.

Ticket purchase at cashier

If the purchaser wants to buy a ticket at the cashier and the sale is made by name, then he or she has to provide three mandatory details (name, date and place of birth), which must be entered in the Interticket Ltd. ticket sales system and, as optional data, the mother's name can be recorded.

The purchase can also be made for another person, in which case the data management is no different than buying a ticket in their own name.

In principle, purchasing a ticket is not subject to a proof of identity. However, HFF, as the organizer, may decide to require the purchaser to present his or her Club Card, Football Card (collectively referred to as: "fan card") or ID when purchasing a ticket.

A Club Card issued by club teams can also be used at HFF-organized matches for the purpose of ticket purchase.

Interticket Ltd. performing sale on commission carried out on behalf of HFF, manages the data provided in connection with the purchase of tickets. HFF's role in data management is to require name-based ticketing and to process the data provided, as explained below, due to adherence to security and admission requirements.

Interticket Ltd. issues an invoice of the purchase to the purchaser, for which it manages the purchaser's name and address.

According to Article 72/B of Act I of 2004 on Sports the purpose of data management related to the sale of name tickets and passes is to implement ticket sales in accordance with stadium safety requirements.

Under the legislation referred to, the data may be used for the purpose of criminal or infringements proceedings initiated in connection with criminal or administrative law offences committed during the approach to or departure from the venue of the sporting event or for the exclusion of participation in the sporting event.

Data management related to ticket sales, in case of using an access control system, based on Subsections (3) and (4) of Article 72 of the Sports Act is mandatory, but the use of a fan card is only mandatory if the HFF requires so for that match.

Before purchasing tickets, Interticket Ltd. checks for the existence of Fan Club membership discounts and applies a discount in case of a name ticket sale.

In case of mandatory proof of identity:

•the purchaser must present his or her fan card or ID card (in case the purchase is made on behalf of another person, the club card or ID card of the person in whose name will be on the ticket),

•through the fan card register, the fan card number (barcode) can be used to load the name, date and place of birth and time of the ticket purchase (including mother's name, if provided when the card was redeemed),

•in the absence of the above, the data required for the purchase of the ticket will be recorded in the system by the cashier on the basis of the identity card or fan card provided.

If the ticket purchase does not require the presence and presentation of a fan card, the cashier will record the data required for ticket purchase based on the information provided by the purchaser and issue a ticket based thereon, but may require a club card or the presentation of an ID card.

However, in the event of a ticket sale by name, it should be taken into account that in this case the identity check is performed at the time of entry, and if the information on the ticket and the identity card information do not match, the purchaser cannot enter the match.

Based on the data provided by the purchaser, the IT system operating the ticket purchase verifies whether the person is banned, prohibited or excluded (ie, queries the Sports Security Registry - SSR).

If there is a match in the system based on the personal information provided in advance, the purchaser may provide the name of his or her mother even if he or she has not provided it first. The system then performs another check. This option does not apply to the purchaser when purchasing with a Club Card or Football Card.

A person who is listed in the SSR for that match and / or venue may not may not purchase a ticket and no ticket may be purchased for a person listed in the SSR for such match and / or venue.

If the answer is positive (banned / prohibited or excluded status), the ticket system does not store the personal data of the purchaser or the ticket holder, but the data of the affected person will be available in the SSR log, which can be traced back to the fact that the attempt to purchase constitutes an offence as well.

If the purchaser or the ticket holder is not listed in the SSR, the personal details of the customer (name, place and date of birth, optionally mother's name) required to purchase the ticket are stored in the central ticketing information system database.

When selling a name ticket, the name and the date of birth are also included on the ticket.

Purchasing tickets online

Data required for ticket purchase:

•in the case of name-based ticket sales: name, place and date of birth, an optional data: the name of the purchaser's mother, and

•in the case of ticket sales related to a fan card, the card's number and PIN.

When buying online, the ticket purchase is done via the web system operated by Interticket Ltd. The scope of the personal data processed and the process of purchasing tickets are the same as that of the cashier.

If ticket sales for a particular match are not made by name and are purchased online, the Interticket Ltd. manages only the data provided by the ticket purchaser upon registration.

If you provide the information with a club card, the card number and associated secret PIN will be entered into the system, and the IT system will load the purchaser's personal details required for the purchase based on the information provided.

If the payment is made by credit card, the purchaser shall provide the information requested by the bank concerned on the payment service provider's own interface, in this connection Interticket Ltd. shall not have access to the card details or carry out any data processing operation.

Duration of data management

The data provided during the registration in the online ticketing system will be processed by Interticket Ltd. until the registration is cancelled or the consent is withdrawn.

Data processed from the ticketing system for the purpose of ticket sales will be deleted from the ticketing system three business days after the match, unless the competent authority instructs HFF as the organizer to retain the data for a maximum of 30 days.

The invoices, as accounting documents are kept by Interticket Ltd. for 8 years.

Legal grounds for data processing

The legal basis for data processing is the legal obligation defined in Article 6 (1) (c) of the Regulation, as pursuant to Subsection (1) of Article 72 of the Sports Act the organizer may use a security access and control system (hereinafter referred to as the access control system) that uniquely identifies participants. With regard to football sports, in the case of a special security risk sporting event and an increased security risk sporting event, where the obligation to use an access control system has been ordered by the National Police Headquarters or the organizer decides so independently, the organizer shall apply an access control system.

Where an access control system is applied pursuant to Subsection (2) of the same Article, the organizer or any person selling tickets and acting on behalf of the organizer may sell only name tickets or passes.

Pursuant to Subsection (4) of the same Article, the organizer or the person selling tickets on behalf of the organizer, at the time of sale of tickets, passes and entry tickets, is entitled to establish the identity of the spectator on the basis of an identity card.

According to Subsection (5) of the same Article, where an access control system is used, the organizer or the person selling tickets on behalf of the organizer may, at the time of sale of the

ticket or pass, verify the spectator's identity with that of the SSR.

In the case of online registration, the legal basis for data processing is the voluntary consent of the purchaser pursuant to Article 6 Subsection (1) (a) of the Regulation.

The issue and preservation of the invoice is a legal obligation pursuant to Article 6 Subsection (1) (c) of the Regulation; the issue of an invoice is required by Article 159 Subsection (1) of the Act CXXVII of 2007 on value added tax, the preservation of the proof of payment is governed by Article 169 Subsection (2) of Act C of 2000 on Accounting.

The processing of ticket purchase data is supported by the legal grounds defined in to Article 6 Subsection (1) (b) of the Regulation related to the performance of the contract, since without processing the data provided for the purchase of tickets, Interticket Ltd. cannot sell the tickets to the customer.

4. Ticket exchange

Process, purpose of data management; the identity of the data controller

If the customer has bought a name ticket and would like to hand it over to another person, he / she has the opportunity to exchange it. At the request of the customer Interticket Ltd. shall exchange the tickets.

Regarding the ticket exchange, the new ticket holder shall also be subject to the data management of the ticket purchase process, except that the new ticket holder will not be billed by Interticket Ltd.

Duration of data management

The storage of new ticket purchaser’s data is governed by the rules of the ticket purchase.

Legal grounds for data processing

The legal basis for data processing for the exchange of tickets pursuant to Article 6 Subsection (1) (b) of the Regulation is the performance of a contract with the former ticket holder which includes the possibility of exchanging tickets. For the new ticket holder, the legal basis for data management is the same as for the ticket purchase.

5. Transmission of the ticket barcode to the Puskás Arena’s access control system

Process, purpose of data management; the identity of the data controller

It is the obligation of Interticket Ltd. to forward the barcode given at the time of the ticket purchase to Puskás Arena’s access control system. The barcode itself does not contain any personal information, however, together with other data, Interticket Ltd. and HFF can identify purchaser of the ticket associated to the bar code (in the case of a name ticket sale).

The transmission of the barcode is essential, as otherwise the valid tickets will not be recognized by the access control system.

Duration of data management

The barcode loses the quality of personal data when Interticket Ltd. and HFF delete the accessed personal data related to it. Cancellation is governed by the rules of ticket purchase.

Legal grounds for data processing

The legal basis for the data management is the fulfilment of the contract between Interticket Ltd. and the purchaser according to Article 6 Subsection (1) (b) of the Regulation, as without data transfer, entry to the match cannot be ensured when an access control system is used.

6. Transmission of report data to HFF

Interticket Ltd., in the framework of this data management, transfers personal data to HFF, as the organizer of the matches of the Hungarian national team. In this case, HFF acts as data controller. In the context of data management, the HFF receives the data provided for the purchase of tickets in the ticketing system provided by Interticket Ltd., supplemented with the exact seating data. The purpose of data management is to enable the HFF, as the organizer of the matches, to perform its duties in connection with entry and secure organization as required by the Sports Act. Additionally, HFF's processing of data is required by sections 16.01 and 16.02 and 16.03 of the UEFA Safety and Security Regulations, which require HFF to have the personal information of ticket holders. The MLSZ can identify the ticket holder based on the personal data associated with the seat, provide information to the incoming health care personnel in case of a medical emergency, and in the case of the commission of an offense or a crime, or a violation of the rules of the course, the processing of the data is also necessary for the purpose of making a complaint or taking action.

7. Special rules for ticket buyers in wheelchairs and their companions

Process and purpose of data management

In some stadiums for certain matches or events, it is possible to watch matches from an area specially designed for disabled spectators or those in a wheelchair, or to reserve occasionally a limited number of parking spaces designed for disabled people. These spaces can only be accessed through proof of entitlement, which is verified during the online ticketing process and at the check-in for the event. Such ticket and parking requests must be sent to InterTicket Kft. on a form prepared for this purpose. By submitting the online form, the disabled ticket buyer explicitly consents to the processing of his/her information detailed below, including that the controller also manages health information in order to provide special wheelchair and parking spaces. The following information must be provided on the online form: e-mail address to which the tickets are to be sent, name, place and date of birth, mother's name, both for the handicapped buyer or the buyer in a wheelchair and the accompanying person (if an appropriate space is created for the accompanying person at the event) and, in addition, the wheelchair person’s disability card number.

The identity of the data controller and the duration of the data processing is the same as described in the section for online ticket purchases.

The legal basis for data processing is the explicit consent of the data subject, as stated above, by completing the online form and submitting it to the controller (Article 6 (1) (a) GDPR).

III/B. Special rules for online events

1. Personal customer account

Online events can be live or broadcast theatrical or other performances, events, which - at the time or during the period specified during the ticket purchase - the Buyer acquires the right to watch with the ticket purchase.

Purpose of data processing: To view online events creating a personal customer account is needed. For this it is necessary to give a valid e-mail address, name and a password. After entering the data, the Service Provider's system will send a message to the indicated email address, requesting its confirmation. The rights to view each content are tied to a personal customer account. The

design of the personal customer account is not the same for non-online events - optionally offered, used on a non-mandatory basis - in accordance with the registration detailed in Section III / 9 of this Privacy Policy. For technical reasons, customers registered in accordance with III / 9. also need to create a personal customer account if they want to view an online event. The registration and the personal customer account are therefore not linked, their use is independent of each other.

Grounds for data processing: fulfilment of a contract, subsection b) Paragraph 1 of Section 6 of the GDPR.

Scope of processed data: email address, name, password

Deadline to erase data: Data provided will be handled by Service Provider until such time as User prohibits use for this purpose by asking for deleting personal customer account. If the User does not do any activity, the Service Provider, therefor does not use the services offered by the service Provider, the Service Provider will delete the personal customer account 3 years after the last activity.

Possible consequences of failure to provide data: the user cannot watch the online events

Source of data: the affected person

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

2. IP address

Purpose of data processing: The Service Provider provides its services related to online events - if no other information can be found in the description of the given performance - without territorial restrictions. However, some events might have territorial restrictions, based on restrictions of copyright, performer rights, or other reasons. In these cases, prior to the purchase, the Service Provider provides this information at the event description. In case of territorial restriction, the Service Provider is entitled to check the IP address of the Customer, to monitor compliance with the territorial limitation, and to refuse access if the place of viewing would violate the territorial restriction.

Grounds for data processing: fulfilment of a contract, subsection b) Paragraph 1 of Section 6 of the GDPR.

Scope of processed data: IP address.

Deadline to erase data: Until the end of the online event.

Possible consequences of failure to provide data: the user cannot watch online events that are restricted on a territorial basis.

Source of data: the affected person (by device communication).

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

IV. Date forwarding, specifying the Data Processors

1. By using the Service, User agrees that Service Provider may forward data to the following partners. Grounds for data forwarding: fulfilment of a contract, subsection b) Paragraph 1 of Section 6 of the GDPR.

- to the organizer of the given event in order to make it possible for the organizer of the event to inform customer directly and without delay if the event is cancelled, its time is changed or of any other detail that might be of interest, furthermore, if the event is cancelled, to refund or exchange tickets directly, and to allow entry to the event and fulfil the contract (appropriate management of the event). With the data transfer the organizer of the given event will become independent data processor in relation to the transferred data. Data transfer may also take place in such a way that Service Provider gives the organizer of the event suitable access to the IT system used for ticketing (Tickets system).

- to the service provider providing the technical conditions for invoicing, as data processor, as follows: Számlázz.hu, operator: KBOSS.hu Kft. (tax number: 13421739-2-13, company registration number: 13-09-101824, head office: 2000 Szentendre, Táltos u. 22/b) or Billzone.hu, operator: N-Ware Kft. (head office: 1139 Budapest, Csongor utca 7/A fszt. 1., tax number: 14825679-2-41, EU tax number: HU14825679, company registration number: 01-09-921789).

- Tasks related to sending emails to the Users and if the person concerned has given permission for profiling, any tasks related to such are carried out by Wanadis Kereskedelmi és Szolgáltató Kft. (1118 Budapest, Rétköz u. 7.), or Emarsys eMarketing Systems AG (Marzstrasse 1, 1150 Vienna, Austria) as data processors, based on their contracts with data controller.

- to OJT Kft.- which provides customer services (Only relevant to those customers who use Service Provider`s contact information to seek help, information or voice a complaint.

- Service Provider will hand over those data to financial institutions that take part in the purchase process by carrying out the payment which are required by the financial institution for executing the payment. The range of required data may vary by financial institutions. Service Provider will not obtain any of the personal data provided at the financial institution`s own data request page.

- If user carries out the purchase using a method providing special discount (e.g. Supershop card) data controller will forward the requested customer information to the company providing the discount. User may request further information on the relevant data processing rules directly from the company providing this service. Data controller will only handle identifiers and other data of such methods in an automatic format insofar it is required by the service provider company to carry out the purchase and provide the discount.

- Analysis of Service Provider`s web usage data, operation of the blog system and the related commenting and rating system, as well as the messaging service of the following service are carried out by Webb & Flow LTD. (Kemp House, 152-160 City Road, London, EC1V 2NX, UK), as data processor.

2. Service Provider as Data Controller is entitled and obliged to transmit to the competent authorities any personal data that is available and is legally stored which is subject to statutory or legally binding obligation by a public authority. Data Controller cannot be held responsible for such data transmission or consequences resulting from such.

3. Service Provider performs the above-mentioned data transfer only in the case of prior and informed consent of the User.

V. The method of storing personal data, security of processing

1. Service Provider`s IT systems and other data retention systems are located at its own seat and at its data processors`.

2. Service provider selects and manages the IT tools used to manage personal data in the provision of the service so that the data:

a) is available for those entitled (availability);

b) authenticity and validation is provided (data authenticity);

c) integrity can be verified (data integrity);

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

3. Service Provider will protect the data with appropriate measures, especially against unauthorized access, alteration, transmission, disclosure, deletion or loss, as well as accidental destruction, harm, as well as unavailability due to any change to the technology used.

4. In order to provide security to the data stored electronically in its various registers, Service Provider shall ensure, by using suitable technology, that the stored data could not be directly linked and linked to the data subject, unless permitted by law.

5. Service Provider will employ such technical, structural and organizational measures to defend the security of data management that provides appropriate level of security to the risks arising in connection with data management.

6. During data processing Service Provider shall maintain:

a) confidentiality: to protect information so that only persons authorized are able to aces it;

b) integrity: to protect accuracy and totality of information and method of processing;

c) availability: to ensure that if eligible user needs it, they can actually access the required information and have the tools available for such.

7. Service Provider's IT System and network, as well as its partners`, are protected against computer-assisted fraud, espionage, sabotage, vandalism, fire, flood, furthermore against computer viruses, cyber intrusions and attacks leading to refusal of Services. Service Provider uses server-level and application-level protection features to ensure security.

8. In the automated processing of personal data, Service Provider provides additional measures

a) to prevent unauthorized data entry;

b) to prevent the use of automatic data processing systems by unauthorized persons by means of data transmission devices;

c) verifiability and determination of which bodies personal data has been or may be transmitted to by means of data transmitting equipment;

d) verifiability and determination of when and who entered which personal data into the automatic data-processing systems;

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

f) report are prepared on errors occurring during automated processing.

9. Service Provider shall take into account the prevailing development of technology when determining and applying measures for data security. If there are several possible solutions for data processing, the one that ensures the highest possible protection of personal data must be chosen unless this would be disproportionate.

10. Service Provider shall ensure the protection of data procession security by such means of technical, organizational and institutional measures that provide a level of protection appropriate to the risks associated with data processing.

11. Electronic messages transmitted via the Internet are vulnerable to network threats irrespective of protocol (email, web, ftp, etc.) which may result in fraudulent activity or disclosure or modification of information. Service Provider shall take all reasonable precautions to protect from such threats. Service Provider shall monitor the Systems in order to record any security deviation and to provide proof in case of all security related events. However, the Internet is commonly – therefore, also to the User – known to be not one hundred percent secure. Service Provider shall not be responsible for damages caused by inevitable attacks despite its best efforts.

VI. Data subjects` rights

1. Data subject may request information on the use of their personal data, furthermore may request correction and, with the exception of compulsory data processing, erasure or revocation of such, may exercise their right to recording and to object as indicated at the time of data recording a well as via the contacts of Service Provider specified in Section 1 of the present document.

Requests for changes in personal details or for deleting personal details can be sent from the registered email address or by post, via a written, fully conclusive private document expressing such request. Certain personal data can also be modified using the website’s personal profile page.

2. Right to be informed: Service Provider shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language. The information shall be provided in writing via the contacts specified in section I of the present Information on Data Processing document. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.

3. Right of access by the data subject: The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

- 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 organisations;
- the envisaged period for which the personal data will be stored
- the right to request rectification or erasure or restriction of processing of personal data;
- the right to lodge a complaint with a supervisory authority;

- any available information as to the source of data;

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

Data Controller shall only see credible any information request sent by email – unless the person concerned otherwise identifies the credibility – if the request is sent from the User`s registered email address. Request for information must be sent via email tointerticket@interticket.huaddress.

4. Where personal data are transferred to a third country or to an international organisation, 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. For any further copies requested by the data subject, the data controller may charge a reasonable fee based on administrative costs. Service Provider shall provide information to data subject by electronic means. Information shall be provided within a maximum of one month from the request.

6. Right to rectification: Affected person may request from Service Provider to rectify or complete the processed personal data.

If personal data is not accurate and accurate data is available to the data controller, data controller shall rectify the personal data.

7. Right to erasure: The data subject shall have the right to obtain from the Service Provider the erasure of personal data concerning him or her 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 withdrew consent on which the processing is based and where 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;

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

The previous (erased) data can no longer be recovered after the request for erasure or modification has been completed.

8. Erasure of the data cannot be requested if the processing is necessary for either of the following reason: for compliance with a legal obligation which requires processing by Union or Member State law or if the data are needed for the establishment, exercise or defence of legal claims of Service Provider.

9. Right to restriction of processing: The data subject shall have the right to obtain from the

controller restriction of processing where one of the following applies:

- the accuracy of the personal data is contested by the data subject, for a period enabling the 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 defence of legal claims; or

- the data subject has objected to processing; in this case restriction shall apply for a period enabling the verification 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 defence of legal claims or for the protection of the rights of another natural or legal person. The data subject shall be informed by the Service Provider 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 him or her, which he or she has 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 his or her particular situation, at any time to processing of personal data concerning him or her, including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims. 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 him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing. Where the data subject objects to processing for direct marketing purposes, the personal 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 him or her or similarly significantly affects him or her. The above right shall not apply of the data processing

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

- is authorised 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 withdrawal: The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent does not affect the lawfulness of processing based on consent before its withdrawal.

15. Procedural rules: Service Provider shall provide information on action taken on a request under Articles 15 to 22 to the data subject without undue delay and in any event within one month of

receipt of the request. 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 form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.

16. If the Service Provider does not take action on the request of the data subject, the controller 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. Service Provider shall provide the requested information and any communication free of cha Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the Service Provider may 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 or erasure of personal data or restriction of processing carried out to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller 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. 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, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.

20. Compensation and grievance money: 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 of the data protection regulation 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 where they are responsible for any damage caused by processing, each controller or processor shall be held liable for the entire damage. A 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. Law enforcement options:

1. For questions and comments please contact the Data Protection Officer at the contact details specified in section I of this Information on Data Processing document.

2. Right to Court: In case of infringement of his or her rights the data subject may bring these to the attention of the court. The court shall hear the case without delay.

3. Data Protection Authority procedures: Complaints may be made to the National Authority for Data Protection and Freedom of Information.

Name: National Authority for Data Protection and Freedom of Information

Seat: 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

ANNEX

Definitions used in the present Information on Data Processing document

1. personal data: means 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: means 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: means the marking of stored personal data with the aim of limiting their processing in the future;

4. profiling: means 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: means the legal person which, alone or jointly with others, determines the purposes and means of the processing of personal data;

6. processor: means a legal person which processes personal data on behalf of the controller;

7. recipient: means 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: means 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. consent: of the data subject means 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. data processing: carrying out technical tasks connected to data processing operations, irrespective of the method and tool used to carry out this operations as well as the place of application, provided that the technical task is carried out on the data;

11. data erasure: making the data unrecognizable in such a way that they may not be restored;

12. EEA country: a member state of the European Union and another state party to the Agreement on the European Economic Area, as well as a state the national of which enjoy the same legal state as a citizen of the state party to the Agreement on the European Economic Area on the basis of the 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 specified natural person identified or – directly or indirectly – identifiable by personal data;

14. customer: any natural person who registers on the website of Service Provider or carries out a purchase without registration:

15. third country: any stat the is not a member of the EEA;

16. disclosure: making personal data available for anyone.