

**WEBSITE PRIVACY NOTICE**  
**/to the visitors of the [meccsiegy.fradi.hu](http://meccsiegy.fradi.hu) website/**

The Controller pays particular attention to the processing, storage and use of personal data in its systems in accordance with the provisions of Regulation (EU) 2016/679 of the EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Regulation (EC) No 95/46/EC (General Data Protection Regulation) ("Regulation").

In relation to processing, the Controller hereby informs the visitors of the Website (hereinafter referred to as "User") of the personal data processed by it, the principles and practices applied to the processing of personal data and the method and possibilities to exercise the rights of Users.

Users are entitled to withdraw consent to the processing, in whole or in part, or to request the deletion of their data by written notice to the Controller, as specified in the notice.

**NAME OF THE CONTROLLER**

Data are processed by **FTC Labdarúgó Zrt.**

Data of the Controller

Name:	<b>FTC Labdarúgó Zrt.</b>
Registered address:	1091 Budapest, Üllői út 129.
Company registration number:	Cg.01-10-044877
E-mail:	<a href="mailto:adatvedelem@fradi.hu">adatvedelem@fradi.hu</a>
Website:	<a href="http://meccsiegy.fradi.hu">meccsiegy.fradi.hu</a>

Legislation on which the processing is based

- Act CXII of 2011 on the right of informational self-determination and on freedom of information (hereinafter, the "Info Act");
- Regulation (EU) 2016/679 of the EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Regulation 95/46/EC (General Data Protection Regulation) (hereinafter referred to as "Regulation");
- Act XLVIII of 2008 on basic requirements of and certain restrictions of commercial advertising activities.

**I. INSTANCES OF PROCESSING**

**1. Personal data logged by the system**

Personal data	Purposes of processing
IP address	Identification number assigned by the Internet service provider to the User's device when logging in to the system. The Controller processes it for the purpose of ensuring the

	IT security of the system.
Browser type	Sending the html code according to the browser type.

Legal grounds for processing: User's voluntary consent pursuant to Article 6(1)(a) of the Regulation.

Possible consequences of not providing data: inaccuracy of analytical measurements.

Duration of processing: The system will store the data marked here for 6 months from the date of their creation, after which they will be automatically deleted.

## 2. Data processed during registration on the website

Purpose of processing: To ensure that website visitors do not have to enter all the necessary information every time they buy a ticket.

Legal basis of processing: Your consent (as per Article 6(a) of EU Regulation 2016/679)

Scope of processed data:

Processed data	Purpose of processing
Full name	User identification
e-mail	Communication and sending password
Password	Encryption

Duration of processing: Until the registration is withdrawn.

Consequences of not processing: The data subject misses the convenience services related to registration and cannot buy tickets or passes.

## 3. Personal data related to the use of the chat window

Personal data	Purposes of processing
Name	User identification
E-mail address	identification of problem, sending discussion/reply afterwards,

Legal grounds for processing: User's voluntary consent pursuant to Article 6(1)(a) of the Regulation.

Source of data: Collected directly from the User.

Possible consequences of not providing data: The data subject cannot use the chat function.

Duration of processing: We will automatically delete the relevant personal data on the 30th day after the end/closing of the conversation.

**4. Scope of the processing of personal data relating to the use of the chat window by those who have consented to the processing of personalised marketing communications**

Purpose of processing: Developing effective marketing communications, sending personalised messages to the data subjects based on their behaviour on the FTC platforms.

Personal data	Purposes of processing
Name	User identification
E-mail address	Personalised communication

Legal grounds for processing: User’s voluntary consent pursuant to Article 6(1)(a) of the Regulation.

Source of data: Collected directly from the User.

Possible consequences of not providing data: the data subject does not receive personalised service and promotions from the Controller.

Duration of processing: Until the consent is withdrawn.

**5. Use of cookies**

Types of cookies and their names	Scope of processed data	Purpose of processing	Duration of processing
Persistent cookie: Google Analytics Google maps Facebook pixel Salesmanago	Recording site visits	To provide a better user experience (e.g. providing optimised navigation, relevant advertising).	They are stored in the browser's cookie file for a longer time. The duration thereof depends on the settings of the User’s browser.

Legal basis of processing: The legal basis for processing is the voluntary consent of the User pursuant to Article 6(1)(a) of the Regulation.

Source of data: Collected directly from the User.

Possible consequences of not providing data: Inaccuracy of analytical measurements, lack of relevant targeted advertising.

**6. Deletion of cookies**

Users can delete the cookies from their computer or disable the use of cookies in the browser. You can usually manage cookies by going to the Tools/Preferences menu of your browser and selecting Privacy/Preferences/Custom Preferences and then under the menu item Cookies or Tracking.

If you would like to find out more about the cookies your browser uses, please visit one of the following websites appropriate for your browser:

- Google Chrome (<https://support.google.com/chrome/answer/95647?hl=hu>)
- Mozilla Firefox ([weboldak-haszn](https://support.mozilla.org/hu/kb/sutik-engedelyezese-es-tiltasa-amit-weboldak-haszn))
- Windows Internet Explorer (<https://support.microsoft.com/hu-hu/help/260971/description-of-cookies>)
- Safari (<https://support.apple.com/hu-hu/guide/safari/manage-cookies-and-website-data-sfri11471/mac>)

Possible consequences of not providing data: Incomplete availability of the services of the Website, inaccuracy of analytical measurements.

## 7. Processing by external service providers

The html code of the portal is independent of the Controller and contains links from and to external servers. The external service provider’s server is connected directly to the User’s computer. Visitors are advised that the providers of these links are able to collect user data due to the direct connection from their server and direct communication with the User’s browser.

The interface of the Website may contain information, in particular advertisements, which come from third parties and advertising service providers who are not related to the Controller. These third parties may also place cookies and web beacons on the User’s computer or collect data using similar technologies in order to send the User advertising messages in connection with their services. In such cases, the processing is governed by the data protection standards set by these third parties and the Controller does not assume any responsibility for such processing.

The controllers listed below can provide detailed information on the processing of data by the server of external service providers.

For the sake of customized service, service external providers place on the User’s computer and read back a small data packet called cookie. When the browser sends back a previously saved cookie, the service provider managing that cookie has the opportunity to link the User’s current visit to the former ones, but only in respect of its own content.

### 7.1. Cookies set by Google Analytics

Personal data	Purposes of processing
IP address	External servers help to independently measure and audit the Website’s traffic and other web analytics data (Google Analytics). These cookies are not able to identify the User personally (the currently used IP address is only partially recorded).
Which part of the Website did the User click on?	The Controller intends to use it to improve the Website and to enhance the experience provided to the User.
How many sites have you visited?	The Controller intends to use it to improve the Website and to enhance the experience provided to the User.

Duration of processing 365 days. If you do not want Google Analytics to measure your data in the way and for the purposes described, please install a blocking add-on in your browser.

Legal basis of processing: The legal basis for processing is the voluntary consent of the User pursuant to Article 6(1)(a) of the Regulation.

Source of data: Collected directly from the User.

Possible consequences of not providing data: inaccuracy of analytical measurements.

For more information about processing by Google Analytics, please visit <http://www.google.com/intl/hu/policies/>. The document “How Google uses data when you use one of our partners’ sites or apps” is available at the link below: <http://www.google.com/intl/hu/policies/privacy/partners/>

## 7.2. Facebook pixel

Processed data	Purposes of processing
Recording site visits	To provide a better user experience (e.g. providing optimised navigation, relevant advertising).

Duration of processing 180 days.

Legal basis of processing: The legal basis for processing is the voluntary consent of the User pursuant to Article 6(1)(a) of the Regulation.

Source of data: Collected directly from the User.

Possible consequences of not providing data: The Website uses Facebook’s retargeting tracking codes. This allows the Controller to address the visitors to the site with retargeting ads on Facebook later. The retargeting code uses cookies to tag visitors. No retargeting ads if disabled.

The content that may be personalised for the User is served by the server of the external service provider. The advertisements of the Controller may be displayed on Facebook and Instagram.

## 7.3. Processing in relation to SALESmanago

Scope of processed data	Purpose of processing
User’s IP address	External servers help to independently measure and audit the Website’s traffic, other web analytics and other data related to its marketing activities. Also, to achieve a better user experience, for example, providing online navigation, personalising the site, providing relevant advertising. A cookie can only be used to uniquely identify a user with the user’s consent.

Visiting the site	To provide a better user experience (e.g. providing optimised navigation, relevant advertising).
Subscription to webpush message	For a better user experience, to enable the sending of personalised webpush messages.

Duration of processing Until the consent is withdrawn.

Legal basis of processing: The legal basis for processing is the voluntary consent of the User pursuant to Article 6(1)(a) of the Regulation.

Source of data: Collected directly from the User.

Possible consequences of not providing data: The data subject does not receive personalised service and promotions from the Controller.

## **II. ACCESS TO DATA AND DATA SECURITY MEASURES, DATA TRANSMISSION**

### **1. Access to data. Data transmission**

Personal data may be accessed by the Controller and the employees of the Controller's Processor for the performance of their tasks.

The Controller will only transfer personal data processed by it to other bodies or public authorities in the manner and for the purposes specified by law.

The Controller informs the Users that the court, the prosecutor, the investigation authority, the law enforcement authority, the public administration authority, the National Authority for Data Protection and Freedom of Information, and other bodies authorised by law may contact the Controller to provide information, disclose or transfer data, or provide documents.

Where the public authority has specified the precise purpose and scope of the data, the Controller will disclose to the public authority only such personal data as are strictly necessary for the purpose of the request.

### **2. Data security measures**

The Controller shall take all reasonable steps to ensure the security of the data and ensure an adequate level of the protection thereof, in particular, against unauthorised access, alteration, transmission, disclosure, erasure or destruction, as well as accidental destruction or damage. The Controller shall ensure the security of the data through appropriate technical and organisational measures.

The IT systems of the Website are located on the servers of the Controller's Processor Lagardere Sports Hungary Korlátolt Felelősségű Társaság (1091 Budapest, Üllői út 129.).

The Controller shall select and operate the IT tools used to process personal data in the course of providing the service in such a way that:

- the processed data are accessible to authorised persons (availability);
- the authenticity and verification of the processed data are ensured (authenticity of processing);
- it can be verified that the processed data are unchanged (data integrity);
- the processed data are protected against unauthorised access (data confidentiality).

During the processing, the Controller shall maintain:

- confidentiality: it shall protect the information so it can only be accessed by persons with the adequate authority;
- integrity: it shall protect the accuracy and completeness of the information and the processing method;
- availability: it shall ensure that when the authorised user needs it, he/she can actually access the desired information and that the means to do so are available.

### **III. PROCESSING**

The Controller is entitled, in accordance with the applicable law, to use a processor for certain technical operations or for the provision of the service. The processor is only entitled to implement the instructions and decisions of the Controller.

**Lagardere Sports Hungary Korlátolt Felelősségű Társaság**

Registered address: 1091 Budapest, Üllői út 129.

Email address: [info@groupamaarena.com](mailto:info@groupamaarena.com)

Telephone number: 003614552300

Activity: database operation, data recording

### **IV. RIGHTS OF USERS**

#### **1. Information and access to personal data**

Users may request information from the Controller in writing via the contact details provided above, so that the Controller can inform them on:

- what personal data,
- on what legal basis,
- for what purpose,
- from what source,
- how long will be processed by it,

to whom, when, under which legislation, to which personal data has the Controller given access or to whom has the Controller transferred the personal data.

The Controller will provide the information to the User in a commonly used electronic form, except if the User requests it in writing on paper. The Controller does not provide oral information over the telephone.

The Controller will provide the User with a copy of the personal data (in person at the customer service) free of charge for the first time. For any further copies requested by the Data Subject, the Controller may charge a reasonable fee based on administrative costs. If the User requests a copy to be issued electronically, the information will be provided by the Controller by e-mail in a commonly used electronic form.

Following the information, if the User disagrees with the processing and the accuracy of the data processed, he/she may request rectification, supplementation, erasure or restriction of the processing of personal data concerning him/her as specified in clause IV, or object to the processing of such personal data, or initiate the procedure specified in clause V.

## **2. Right to rectification and right to have incomplete personal data completed**

At the User's written request, the Controller shall, without undue delay, rectify inaccurate personal data specified by the User in writing or in person at one of the Controller's shops, or complete the incomplete data with the content specified by the User. The Controller notify any rectification or completion carried out to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The User will be informed of the data of these recipients if he/she so requests in writing.

## **3. Right to restriction of processing**

Users may, by written request, request the Controller to restrict processing his/her data if the

- the accuracy of the personal data is contested by the User, for a period enabling the Controller to verify the accuracy of the personal data;
- processing is unlawful and the User 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 User for the establishment, exercise or defence of legal claims;
- the User has objected to processing; in this case the restriction applies to the period pending the verification whether the legitimate grounds of the Controller override those of the data subject.

Where data processing is restricted, the personal data of the User may, with the exception of storage, only be processed with the User'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 or for reasons of important public interest of the Union or of a Member State. The User who has obtained restriction of processing at his/her request will be informed by the Controller before the restriction of processing is lifted.

## **4. Right to erasure (to be forgotten)**

Users have the right to obtain from the Controller the erasure of personal data concerning the User without undue delay where one of the following grounds applies:

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



- ii.) the User withdraws consent on which the processing is based, and there is no other legal ground for the processing;
- iii.) the User objects to the processing for reasons relating to his/her particular situation and there is no legitimate ground for the processing,
- iv.) the User objects to the processing of personal data relating to him/her for direct marketing purposes, including profiling, insofar as it relates to direct marketing,
- v.) the personal data have been unlawfully processed by the Controller;
- vi.) the personal data have been collected in relation to the offer of information society services directly to a child.

Users may not exercise the right to erasure or blocking if the processing is necessary

- i.) for exercising the right of freedom of expression and information;
- ii.) for reasons of public interest in the area of public health;
- iii.) for archiving in the public interest, scientific or historical research purposes or statistical purposes in so far as the right to erasure would render impossible or seriously impair the achievement of the objectives of that processing; or
- iv.) ) for the establishment, exercise or defence of legal claims.

## **5. Right to data portability**

Where processing is necessary for the performance of a contract or if the processing is based on the User's voluntary consent, the User has the right to request to receive the data provided by the User to the Controller in a machine-readable form. If technically feasible, he/she may request that we transfer the data to another controller. In any case, the right is limited to the data provided by the User, and portability of other data is not possible (e.g. statistics, etc.).

As regards the personal data relating to him/her that are available in the Controller's system (e.g. when subscribing to a newsletter), the User may:

- can be obtained by the Data Subject in a structured, widely used, machine-readable form,
- may be forwarded to another controller by the Data Subject,
- request the direct transfer of the data to another controller - if this is technically feasible in the Controller's system.

The Controller will only grant a request for data portability on the basis of a written request sent by email or post. In order to comply with the request, the Controller must ensure that it is indeed the User who intends to exercise such right. Under this right, the User may request portability of the data that he/she has provided to the Controller. The exercise of this right does not automatically entail the erasure of the data from the Controller's systems, therefore the User will be recorded in the Controller's systems even after exercising this right, unless he/she requests erasure of his/her data.

## **6. Objection to the processing of personal data**

User may object to the processing of his/her personal data by means of a statement addressed to the Controller if the legal basis for the processing is

- public interest under Article 6(1) e) of the GDPR, or
- legitimate interest under Article 6(1) f) of the GDPR.

In case the right to object is exercised, 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 User or for the establishment, exercise or defence of legal claims. The Controller will decide whether the processing is justified by compelling legitimate grounds. It shall inform the User of its position in this regard in an opinion.

User can object in writing (by e-mail or post) or, in the case of a newsletter, by clicking on the unsubscribe link in the newsletter.

## **7. Enforcement by another party of the rights of a deceased User**

Within five years after the death of the User concerned, the rights of the deceased during his/her lifetime, such as the rights of access, rectification, erasure, restriction of processing, data portability and objection, may be exercised by the person authorised by the deceased by means of an administrative instruction or a declaration in a public document or a private document with full probative value made to Data Controller. If the deceased has made more than one such declaration to the Controller, the person named in the declaration made at a later date may exercise those rights.

If the deceased did not make such a declaration, the rights to which the deceased was entitled during his/her lifetime and which are set out in the previous paragraph may be exercised by his/her close relative under the Civil Code within five years of the death of the data subject (in the case of more than one close relative, the first of the closest relatives who exercises this right may assert these rights).

According to point 1 of Section 8:1(1) of the Civil Code, close relatives include the spouse, next of kin, adoptive, step and foster children, adoptive, step and foster parents, as well as siblings. The next of kin of the deceased must:

- prove the fact and date of the death of the deceased data subject by means of a death certificate or court order, and
- verify his/her identity and, if necessary, that he/she is a close relative, by means of a public document.

The person asserting the rights of the deceased, in particular, in proceedings against the Controller and before the National Authority for Data Protection and Freedom of Information and the courts, shall be entitled to the rights and shall be subject to the obligations to which the deceased was entitled or be bound by during his/her lifetime in accordance with the Info Act and the Regulation.

The Controller shall, upon written request, inform the next of kin of the action taken, unless the deceased has expressly prohibited this in his/her statement.

## **8. Deadline for fulfilling the request**

The Controller shall inform the User of the measures taken without undue delay, but in any event within one month of receipt of any of the requests pursuant to clauses IV.1 to IV.7. If necessary, taking into account the complexity of the request and the number of requests, this time limit may be extended by a further two months, but in this case the Controller shall inform the User within one month of receipt of the request, stating the reasons for the delay, and that the User may lodge a complaint with the supervisory authority and exercise his/her right to judicial remedy.

If the User's request is manifestly unfounded or excessive (in particular, in view of its repetitive nature), the Controller may charge a reasonable fee for complying with the request or refuse to act on the basis of the request. The proof of this lies with the Controller.

If the User submitted his/her request by electronic means, the information will be provided by the Controller electronic means, except requested otherwise by the User.

The Controller 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 User about those recipients requested by the User.

## **8. Damages and compensation**

Any person who has suffered material or non-material damage as a result of an infringement of the Regulation shall have the right to receive compensation from the Controller or processor for the damage suffered. The processor shall be liable for the damage caused by processing only where it has not complied with the obligations specified by the law specifically directed to processors or where it has disregarded or acted contrary to the lawful instructions of the Controller. The Controller or the processor shall be exempt from liability able to prove that it is not in any way responsible for the event giving rise to the damage.

## **V. ENFORCEMENT OPTIONS**

Users may exercise their rights by sending a written request by e-mail or post.

The User cannot enforce his/her rights if the Controller proves that it is not in a position to identify the User. If the User's request is manifestly unfounded or excessive (in particular, in view of its repetitive nature), the Controller may charge a reasonable fee for complying with the request or refuse to act. The proof of this lies with the Controller. If the Controller has doubts about the identity of the natural person making the request, it may request providing further information necessary to confirm the identity of the applicant.

Pursuant to the Info Act, the Regulation and the Civil Code (Act IV of 2013), Users may

- address the National Authority for Data Protection and Freedom of Information (1125 Budapest, Szilágyi Erzsébet fasor 22/c.; [www.naih.hu](http://www.naih.hu)), or

- enforce their rights in court. At the User's option, the lawsuit may be brought before the court of his/her place of residence (for a list of regional courts and their contact details, click on the link below: <http://birosag.hu/torvenyszekek>).

## **VI. HANDLING OF PERSONAL DATA BREACH**

A 'personal data breach' is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. The Controller shall keep records for the purpose of monitoring the measures taken in relation to the data breach, informing the supervisory authority and informing the User, which shall include the scope of personal data affected by the breach, the number and scope of the data subjects, the time and date of the breach, its circumstances and effects, and the measures taken to remedy the breach. In the event of a personal data breach, the Controller shall inform the User and the supervisory authority of the personal data breach without undue delay and within 72 hours at the latest, unless the personal data breach does not pose a risk to the rights and freedoms of natural persons.

## **VII. BACKUP MANAGEMENT POLICY**

In the context of its duties related to IT security, the Controller shall ensure, in particular, that measures are in place to ensure the possibility of restoring data files, including regular backups and the separate and secure handling of copies (backup).

Accordingly, in order to prevent the loss of electronically stored data, the Processor shall regularly back up the data in its database containing personal data to a separate storage medium three times a day.

Location where backups from the website server are stored: Lagardere Sports Hungary Korlátolt Felelősségű Társaság /1091 Budapest üllői út 129./

Duration for which backups are stored: 5 years

Order of erasing backups: individual erasure can be tracked in an anonymised registry and automatic erasure takes place according to the settings.

Access to backup: Access to backups is restricted, only persons with special authorisation may access them. Access to the data is only possible after proper identification (at least username and password).

## **VIII. MISCELLANEOUS PROVISIONS**

The Controller reserves the right to unilaterally modify this Privacy Policy, with prior notice to Users using the Website through its website. The amendments shall enter into force vis-à-vis the Users on the date specified in the notice, unless the User objects to the amendments.

The Controller may enforce a claim for damages against the User if the User has provided the data of any third party to subscribe to the newsletter or for any other purpose in order to use the service or caused damage in any manner while using the Website.

The Controller does not verify the personal data provided to it. The person providing the data is solely responsible for the correctness of the data. By providing this/her personal data, each User also accepts responsibility for that the data provided by him/her are true and that it is only him/her who uses the service by using such personal data.

**Contact details of the Data Protection Officer**

Name: Dr. Vanda Juhász

Telephone number: 06 1/ 91-00-241

E-mail: [vanda.iuhasz@fradi.hu](mailto:vanda.iuhasz@fradi.hu)

Date of entry into force of this Privacy Notice: 4 June 2019

Available for download: <https://www.fradi.hu/labdarugas/ferfi->