MAGYAR EVEZŐS SZÖVETSÉG

ALAPÍTVA: 1893

PRIVACY POLICY

HUNGARIAN ROWING ASSOCIATION 2024.

Organization name: Hungarian Rowing Association

Headquarters: 1146 Budapest, Istvánmezei út 1-3.

Registration number: 01-07-0000007

Name of person entitled to representation: President
Otto Cseh

I. PURPOSE OF THESE REGULATIONS

The purpose of these regulations is the Hungarian Rowing Association (hereinafter:**"ASSOCIATION" or "Data Manager"**) establishing the internal rules establishing its data protection and data management policy Regulation (EU) 2016/679 of the European Parliament and Council (April 27, 2016) (hereinafter: "GDPR Regulation") on the protection of natural persons with regard to the processing of personal data and such on the free flow of data and the repeal of Regulation 95/46/EC (general data protection GDPR, hereinafter:**"GDPR"**) by complying with the data protection and data management provisions, by enforcing which during the use of all activities and services of the ASSOCIATION, it ensures

that the data subjects' right to the protection of personal data is respected during the processing and management of data subjects' personal data.

II. SCOPE OF THE REGULATION

1. Personal scope

The scope of these regulations covers the ASSOCIATION and the natural persons to whom the data management activities of the ASSOCIATION cover. The data management activities set out in these regulations are aimed at the personal data of natural persons. The scope of the regulation does not cover the data management of legal entities.

2. Temporal effect

These regulations will enter into force on February 15, 2024 and will last indefinitely. These regulations will be reviewed as necessary, but at least annually.

III. DEFINITIONS

1. **"Personal data":**any information relating to an identified or identifiable natural person ("Data Subject"); a natural person can be identified directly or indirectly, in particular on the basis of an identifier such as name, number, location data, online identifier or one or more factors relating to the physical, physiological, genetic, mental, economic, cultural or social identity of the natural person identifiable;

2. **"Data management"**: any operation or set of operations performed on personal data or data files in an automated or non-automated manner, such as collection, recording, organization, segmentation, storage, transformation or change, query, insight, use, communication, transmission, distribution or making available in any other way through, alignment or connection, restriction, deletion or destruction;

3. **"Restriction of data management"**: indication of stored personal data for the purpose of restricting their future processing;

4. **"Data manager"**: the natural or legal person, public authority, agency or any other body that determines the purposes and means of processing personal data independently or together with others; if the purposes and means of data management are determined by EU or member state law, the data controller or the special aspects regarding the designation of the data controller may also be determined by EU or member state law;

5. **"Data Processor"**: the natural or legal person, public authority, agency or any other body that processes personal data on behalf of the data controller;

6. **"Recipient"**: the natural or legal person, public authority, agency or any other body with whom the personal data is communicated, regardless of whether it is a third party. Public authorities that have access to personal data in accordance with EU or Member State law in the context of an individual investigation are not considered recipients; the management of said data by these public authorities must comply with the applicable data protection rules in accordance with the purposes of data management;

7. **"Third Party"**: the natural or legal person, public authority, agency or any other body that is not the same as the data subject, the data controller, the data processor or the persons who have been authorized to handle personal data under the direct control of the data controller or data processor;

8. **"Consent of the Data Subject"**: a voluntary, concrete and clear declaration of the Data Subject's will based on adequate information, by means of which the Data Subject indicates by means of a statement or an act clearly expressing the confirmation that he/she consents to the processing of personal data concerning him/her;

9. **"Data protection incident"**: a breach of data security that results in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure or unauthorized access to personal data transmitted, stored or otherwise handled;

ARC. BASIC PRINCIPLES

(1) Your person Personal data can only be processed for specific purposes, in order to exercise rights and fulfill obligations.

(2) In all stages of data management, the purpose of data management must be met, the collection and management of data must be fair and legal. Only personal data that is essential for the realization of the purpose of data management and suitable for achieving the purpose can be processed.

(3) Personal data may only be processed to the extent and for the time necessary to achieve the purpose.

(4) The ASSOCIATION declares that it stores the personal data it manages at its headquarters in the form of an electronic file or on paper-based documents in compliance with the legal requirements for data security. This provision applies to
all data management and data processing activities carried out by the ASSOCIATION.

V. LEGAL BASIS OF DATA MANAGEMENT

1. Voluntary consent of the Data Subject

(1) The legality of processing personal data must be based on the Data Subject's voluntary consent, or must have some other legal basis established by law.

(2) In case of data management based on the Data Subject's consent, the Data Subject may give his consent to the processing of his personal data in the following form:

a) in writing, in the form of a statement giving consent to personal data processing,

b) electronically, if it isinfo@hunrowing.hu sends a corresponding message to your email address.

(3) Silence does not constitute consent.

(4) Consent covers all data management activities carried out for the same purpose or purposes.

(5) If the data management serves several purposes at the same time, the consent must be given for all data management purposes.

(6) The data subject is entitled to withdraw his consent at any time. Withdrawal of consent does not affect the legality of data processing based on consent prior to withdrawal. Before giving consent, the Data Subject must be informed of this. Withdrawal of consent should be possible in the same simple way as giving it.

2. Contract performance

(1) Data processing is considered lawful if it is necessary for the performance of a contract in which the Data Subject is one of the parties, or it is necessary for taking steps at the Data Subject's request prior to the conclusion of the contract.

(2) The consent of the data subject to the processing of personal data that is not necessary for the performance of the contract shall not be a condition for the conclusion of the contract.

3. Fulfilling the legal obligation of the Data Controller or protecting the vital interests of the Data Subject or other natural persons

(1) The legal basis for data management is determined by law in the event of the fulfillment of a legal obligation, so the Data Subject's consent is not required for the processing of his personal data.

(2) The Data Controller is obliged to inform the Data Subject about the purpose, legal basis and duration of the data management, about the person of the Data Controller, as well as about his rights and legal remedies.

(3) In order to fulfill a legal obligation, the Data Controller is entitled, after withdrawing the Data Subject's consent, to manage the data that is necessary for the fulfillment of a legal obligation concerning him.

4. Execution of a task carried out in the public interest or in the context of the exercise of a public authority conferred on the Data Controller, enforcing the legitimate interests of the Data Controller or a third party.

(1) The Data Controller - including the data controller with whom the personal data may be disclosed - or the legitimate interest of a third party may create a legal basis for data processing, provided that the interests, fundamental rights and freedoms of the Data Subject do not take precedence, taking into account their relationship with the Data Controller based on the Data Subject's reasonable expectations. Such a legitimate interest may exist, for example, when there is a relevant and appropriate relationship between the Data Subject and the Data Controller, for example in cases where the Data Subject is a client of the Data Controller or is employed by the Data Controller.

(2) In order to establish the existence of a legitimate interest, it must be carefully examined, among other things, whether the Data Subject can reasonably expect, at the time and in connection with the collection of personal data, that data processing may take place for the given purpose.

(3) The interests and fundamental rights of the Data Subject may take precedence over the interests of the Data Controller if the personal data are processed under circumstances in which the Data Subjects do not expect further data processing.

VI. RANGE OF PERSONS AUTHORIZED TO KNOW THE DATA

(1) The employees of the ASSOCIATION with access rights related to the relevant data management purpose, or the data processor performing payroll, accounting, bookkeeping and legal services for the ASSOCIATION can see the personal data to the extent necessary for the performance of the service. In addition to the above, the Ministry of Human Resources is entitled to access the data, if this is necessary for the assessment, disbursement and accounting of state aid.

VII. RIGHTS OF THE PERSON CONCERNED

1. Right to information

(1) The data subject has the right to receive information about the information related to data management before the start of the activity aimed at managing his data.

(2) If the Data Controller wishes to carry out further data processing of personal data for a purpose other than the purpose of their acquisition, he must inform the Data Subject about this different purpose and all relevant additional information before further data processing. The ASSOCIATION does not process personal data for purposes other than the purpose for which they were obtained.

2.**The Data Subject's right of access**

(1) The Data Subject is entitled to receive feedback from the Data Controller as to whether his personal data is being processed, and if such data processing is underway, he is entitled to receive access to the personal data and the following information:

the. the purposes of data management;

b. categories of personal data concerned;

c. the recipients or categories of recipients to whom or to whom the personal data has been or will be communicated, including in particular recipients in third countries and international organizations;

d. where appropriate, the planned period of storage of personal data or, if this is not possible, the criteria for determining this period;

e. the Data Subject's right to request from the data controller the correction, deletion or restriction of processing of personal data concerning him and to object to the processing of such personal data;

f. the right to submit a complaint to a supervisory authority.

(2) The Data Controller shall make a copy of the personal data subject to data management available to the data subject. For additional copies requested by the Data Subject, the Data Controller shall bear the administrative costs

can charge a reasonable fee based on If the Data Subject submitted the request electronically, the information must be provided in a widely used electronic format, unless the Data Subject requests otherwise.

3. The Data Subject's right to correction and deletion

3.1. Right to rectification

(1) The Data Subject has the right to have inaccurate personal data corrected without undue delay upon request by the Data Controller. Taking into account the purpose of the data management, the Data Subject is entitled to request the completion of incomplete personal data, among other things, by means of a supplementary statement.

3.2. The right to erasure ("the right to be forgotten")

(1) The Data Subject has the right to request that the Data Controller delete the personal data concerning him without undue delay, and the Data Controller is obliged to delete the personal data concerning the Data Subject without undue delay if one of the following reasons exists:

the. the personal data are no longer needed for the purpose for which they were collected or otherwise processed;

b. The data subject withdraws the consent that forms the basis of the data management pursuant to point a) of Article 6 (1) of the GDPR (consent to the processing of personal data) or point a) of Article 9 (2) of the GDPR (giving express consent), and the data management has no other legal basis;

c. the data subject objects to the processing of his data on the basis of Article 21 (1) of the GDPR (right to object) and there is no overriding legitimate reason for data processing, or the data subject on the basis of Article 21 (2) of the GDPR (personal data processing for the purpose of obtaining business) objection to) object to data processing;

d. personal data has been processed unlawfully;

e. personal data must be deleted in order to fulfill the legal obligation prescribed by EU or member state law applicable to the Data Controller.

(2) Subsection (1) does not apply if data management is necessary:

the. for the purpose of fulfilling the obligation under EU or Hungarian law applicable to the Data Controller requiring the processing of personal data, or for the execution of a task carried out in the public interest or in the context of the exercise of a public authority vested in the Data Controller;

b. for the presentation, enforcement and defense of legal claims.

4. The right to restrict data processing

(1) The Data Subject is entitled to request that the Data Controller restricts data processing if one of the following is met:

the. the Data Subject disputes the accuracy of the personal data, in which case the limitation applies to the period that allows the data controller to check the accuracy of the personal data;

b. the data processing is illegal and the Data Subject opposes the deletion of the data and instead requests the restriction of its use;

c. The Data Controller no longer needs the personal data for the purpose of data management, but the Data Subject requires them to present, enforce or defend legal claims; obsession

d. the Data Subject has objected to data processing in accordance with Article 21 (1) of the GDPR; in this case, the restriction applies to the period until it is established whether the data controller's legitimate reasons take precedence over the data subject's legitimate reasons.

(2) If data processing is subject to restrictions based on paragraph (1), such personal data, with the exception of storage, will only be processed with the Data Subject's consent, or for the presentation, enforcement or defense of legal claims, or for the protection of the rights of other natural or legal persons, or the Union , or can be handled in the important public interest of a member state.

(3) The Data Controller informs the Data Subject at whose request the data processing was restricted on the basis of paragraph (1) in advance of the lifting of the data processing restriction.

5. Notification obligation related to the correction or deletion of personal data or the limitation of data management

(1) The Data Controller informs all recipients of the correction, deletion or limitation of data management to whom or to whom the personal data was disclosed, unless this proves to be impossible or requires a disproportionately large effort.

6. The right to data portability

(1) The Data Subject is entitled to receive the personal data relating to him/her provided to a data controller in a segmented, widely used, machine-readable format, and is also entitled to forward this data to another data controller without being hindered by the data controller to whom the personal data has been made available, if the data processing is in accordance with point a) of Article 6 (1) of the GDPR (the consent of the person concerned to the processing of personal data) or point a) of Article 9 (2) of the GDPR (the express consent of the person concerned) to data management) or the contract according to Article 6 (1) point b).
(2) When exercising the right to data portability in accordance with paragraph (1), the Data Subject is entitled - if this is technically possible - to request the direct transfer of personal data between data controllers.

7. Right to protest

(1) The Data Subject has the right to object at any time for reasons related to his own situation to the processing of his personal data carried out in the public interest or in the exercise of public authority, or to processing necessary to enforce the legitimate interests of the data controller or a third party (GDPR Article 6 (1) against data processing based on points e) or f) of paragraph In this case, the Data Controller may no longer process the personal data, unless the Data Controller proves that the data processing is justified by compelling legitimate reasons that take precedence over the interests, rights and freedoms of the Data Subject, or that are necessary for the presentation, enforcement or defense of legal claims are connected.

8. The data subject's right to complaint and legal remedy

8.1. The right to complain to the supervisory authority.

(1) Based on Article 77 of the GDPR, the Data Subject has the right to file a complaint with the supervisory authority if, in the opinion of the Data Subject, the processing of his/her personal data violates the GDPR regulation.

(2) The Data Subject may exercise his right to file a complaint at the following contact details:

National Data Protection and Freedom of Information Authority (address: Budapest, Falk Miksa u. 9-11, 1055,; Phone: +36 (1) 391-1400; Fax: +36 (1) 391-1410 www: http://www. naih.hu e-mail: ugyfelszolgalat@naih.hu)

(3) The supervisory authority, to which the complaint was submitted, is obliged to inform the customer about the procedural developments related to the complaint and its result, including that the customer is entitled to legal remedies based on Article 78 of the GDPR.

8.2. The right to an effective judicial remedy against the supervisory authority

(1) Without prejudice to other administrative or non-judicial remedies, all natural and legal persons are entitled to an effective judicial remedy against the legally binding decision of the supervisory authority.

(2) Without prejudice to other administrative or non-judicial remedies, all data subjects are entitled to effective judicial remedies if the competent supervisory authority does not deal with the complaint or does not inform the Data Subject within three months of the complaint submitted under Article 77 of the GDPR about procedural developments or their results.

(3) Proceedings against the supervisory authority must be initiated before the court of the Member State where the supervisory authority is based, i.e. the Hungarian court.

8.3. The right to an effective judicial remedy against the Data Controller or the Data Processor

(1) Without prejudice to the available administrative or non-judicial remedies, including the right to complain to the supervisory authority according to Article 77 of the GDPR, all Data Subjects are entitled to an effective judicial remedy if, in their opinion, their personal data does not comply with the GDPR as a result of its processing, your rights under the GDPR have been violated.

(2) Proceedings against the Data Controller or the Data Processor must be initiated before the court of the Member State where the Data Controller or the Data Processor operates, i.e. the Hungarian court. Such a procedure can also be initiated before the court of the Member State of the Data Subject's habitual residence, unless the data controller or the data processor is a public authority of a Member State acting in its public authority.

9. Information about the data protection incident

(1) If the data protection incident likely involves a high risk for the rights and freedoms of natural persons, the Data Controller shall inform the Data Subject of the data protection incident without undue delay.

(2) In the information provided to the Data Subject referred to in paragraph (1), the nature of the data protection incident must be clearly and comprehensibly described, and at least the name and contact details of the contact person providing further information, the likely consequences of the data protection incident, the actions taken by the Data Controller on the measures taken or planned to remedy a data protection incident, including, where applicable, measures aimed at mitigating any adverse consequences resulting from a data protection incident.

VIII. PROCEDURE TO BE APPLIED IN THE EVENT OF A REQUEST BY THE PARTICIPANT

(1) The ASSOCIATION facilitates the exercise of the Data Subject's rights, the Data Subject may not refuse to fulfill a request to exercise the Data Subject's rights, also set out in these regulations, unless it proves that the Data Subject cannot be identified.

(2) The ASSOCIATION shall inform the Contact of the measures taken following the request without undue delay, but in any case within one month from the receipt of the request. If necessary, taking into account the complexity of the application and the number of applications, this deadline can be extended by another two months. The Data Controller shall inform the Data Subject of the extension of the deadline, indicating the reasons for the delay, within one month of receiving the request.

(3) If the Data Subject submitted the request electronically, the information must be provided electronically, if possible, unless the Data Subject requests otherwise.

(4) If the ASSOCIATION does not take measures following the Data Subject's request, it shall inform the Data Subject without delay, but at the latest within one month of the receipt of the request, of the reasons for the failure to take action, and of the fact that the Data Subject may file a complaint with the supervisory authority and take legal action with his right of redress.

(5) The ASSOCIATION provides information and measures related to data management (feedback on the management of personal data, access to managed data, correction, addition, deletion of data, restriction of data management, data

portability, objection to data management, information on data protection incidents) free of charge to the Data Subject for.

(6) If the Data Subject's request is clearly unfounded or - especially due to its repetitive nature - excessive, the Data Controller, taking into account the administrative costs associated with providing the requested information or information or taking the requested measure: may charge a fee to the extent specified in a government decree, or may refuse to process the request measure.

(7) It is the responsibility of the Data Controller to prove that the request is clearly unfounded or exaggerated.

(8) Without prejudice to Article 11 of the GDPR, if the Data Controller has reasonable doubts as to Articles 15–21 of the GDPR. regarding the identity of the natural person who submitted the application pursuant to Article, you may request the provision of additional information necessary to confirm the Data Subject's identity.

IX. PROCEDURE IN CASE OF DATA PROTECTION INCIDENT

(1) According to the GDPR, a data protection incident is a breach of data security that results in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure or unauthorized access to personal data transmitted, stored or otherwise handled.

(2) A data protection incident is the loss or theft of a device containing personal data (laptop, mobile phone), or the loss or inaccessibility of the code used to decrypt files encrypted by the Data Controller, infection by ransomware (blackmail virus), which makes the data managed by the Data Controller inaccessible until the ransom is paid, attacking the IT system, publishing an e-mail containing wrongly sent personal data, an address list, etc.

(3) If a data protection incident is detected, the representative of the ASSOCIATION shall immediately conduct an investigation in order to identify the data protection incident and determine its possible consequences. Necessary measures must be taken to prevent damage.

(4) The data protection incident must be reported to the competent supervisory authority without undue delay and, if possible, no later than 72 hours after becoming aware of the data protection incident, unless the data protection incident does not likely pose a risk to the rights and freedoms of natural persons looking at. If the notification is not made within 72 hours, the reasons justifying the delay must also be attached.

(5) The data processor shall report the data protection incident to the Data Controller without undue delay after becoming aware of it.

(6) In the notification referred to in paragraph (3), at least:

the. the nature of the data protection incident must be described, including - if possible - the categories and approximate number of Data Subjects, as well as the categories and approximate number of data affected by the incident;

b. the name and contact details of the data protection officer or other contact person providing additional information must be provided;

c. the likely consequences of the data protection incident must be described;

d. the measures taken or planned by the Data Controller to remedy the data protection incident must be described, including, where appropriate, measures aimed at mitigating any adverse consequences resulting from the data protection incident.

(7) If and to the extent that it is not possible to provide the information at the same time, it can be provided later in parts without further undue delay.

(8) The Data Controller keeps records of data protection incidents, indicating the facts related to the data protection incident, its effects and the measures taken to remedy it. This register enables the supervisory authority to check compliance with the requirements of Article 33 of the GDPR.

X. THE ASSOCIATION CONTINUED IN CONNECTION WITH EMPLOYMENT

DATA MANAGEMENT ACTIVITIES

1. Data management prior to the establishment of the Employment Relationship

The data management that takes place before the establishment of the employment relationship is carried out in connection with the application procedure that precedes it, as well as the examination of suitability for the position.

1.1. Data management during the tender process for hiring employees

(1) The legal basis for data management during the recruitment process is the Data Subject's consent.

(2) The purposes of data management: evaluation of applications, conclusion of employment contracts.

(3) Data affected by data management: name, address, place of birth, time, mother's name, education, professional qualifications, phone number, e-mail address, photo, social security number, all data that is voluntarily included in the resume of a person applying for a job .

(4) Categories of persons affected by data management: persons applying for job applications.

(5) Recipients of personal data: the practitioner of the employer's authority, the member who undertakes personal cooperation.

(6) Duration of data management: after the selection of the employee, the purpose of data management for non-selected applicants ceases, therefore the applicants' personal data must be deleted immediately.

(7) The cancellation obligation also exists in the event that the Data Subject changes his mind or withdraws his application during the application process. The applicant must be informed of the result of the decision made regarding the selection.

1.2. Data management during the job suitability test

(1) Based on Section 10 (1) of the Mt., only two types of aptitude tests can be applied to employees: aptitude tests that are required by the employment rule, and on the other hand, tests that are not prescribed by the employment rule, but which it is necessary in order to exercise the right and fulfill the obligation defined in the rules on the employment relationship.

(2) In both cases of the aptitude test, the employees must be informed in detail about, among other things, what kind of skills and abilities the aptitude test is aimed at assessing, and what means and methods are used to conduct the test. If a law requires the examination to be carried out, the employees must be informed of the title of the law and the exact location of the law.

(3) The legal basis for data management is the legitimate interest of the employer.

(4) Purpose of data management: determination of suitability for a position, establishment of an employment relationship.

(5) The persons authorized to handle personal data with regard to the examination result are the specialist conducting the examination and the examined person. The employer can only receive information on whether the examined person is suitable for the job or not, and what conditions must be provided for this. However, the employer may not know the details of the investigation or its complete documentation.

(6) Duration of handling personal data related to the aptitude test: 5 years after the termination of the employment relationship.

2. Data management during the employment relationship

2.1. Data management in the framework of employment records

(1) The ASSOCIATION manages the below-named employee personal data managed in the labor register based on the legitimate interests of the employer, the fulfillment of legal obligations, and the fulfillment of contracts. The ASSOCIATION informs the employee about the legal basis and purpose of the data management before starting the data management activity.

(2) The range of employee personal data managed by the ASSOCIATION in the employment register:

- name
- residential address, temporary residential address, postal address,
- place and time of birth
- His mother's name,
- his image
- contact details, telephone number, e-mail address,
- TAJ number, tax identification number, identity card number,
- wage amount,
- Bank account number,
- addresses of bans, deductions, or bank account numbers,
- number of children, dependents and their TAJ, • next of kin to be notified.

(3) The scope of persons affected by data management: employees of the ASSOCIATION.

(4) Recipients of the personal data recorded above: the employer, the data processor providing accounting, auditing and legal services.

(5) Purpose of data management: fulfillment of obligations arising from an employment relationship, (payment of wages), exercise of rights arising from an employment relationship. Creation and termination of an employment relationship.

(6) Duration of data management: 50 years after termination of employment.

2.2. Checking the employee's employment-related behavior

(1) The employer may only monitor the employee's behavior related to the employment relationship. The inspection and the tools and methods used during it must not involve a violation of human dignity. The employee's private life cannot be monitored.

(2) The employer shall inform the employee in advance of the use of the technical devices used to monitor the employee.

2.3. Ad hoc data management for employees

(1) The employer organizes team-building trainings and other events in which employees can participate in order to improve communication between employees, promote more effective cooperation among employees and increase their level of trust, and strengthen mutual respect and commitment.

(2) The legal basis for data management during the activity specified in point (1) is the consent of the employee.

(3) The purpose of data management is to improve communication between employees, promote more effective cooperation and increase the level of trust of employees, and strengthen mutual respect and commitment.

(4) The range of stakeholders: all employees who participate in the training and other events.

(5) Scope of personal data: image, voice, passport, identity card number of employees.

(6) Data deletion deadline: withdrawal of consent or 6 months after publication in the employer's internal system.

(7) Those entitled to access the data (categories of recipients): none.

XI. DATA MANAGEMENT ACTIVITY RELATED TO CONTRACT PERFORMANCE

(1) The ASSOCIATION manages the personal data of natural persons and sole proprietors who contract with it in connection with the contractual relationship. The Data Subject must be informed about the handling of personal data.

(2) The range of stakeholders: all natural persons and sole proprietors who wish to establish or are establishing a contractual relationship with the ASSOCIATION.

(3) The legal basis of data management is the performance of a contract, the purpose of data management is to maintain contact, assert claims arising from the contract, and ensure compliance with contractual obligations. (4) Recipients of personal data: employees and data processors of the ASSOCIATION.

(5) Scope of processed personal data:

- in the case of a natural person: name, address, mother's name, portrait, place of birth, time, tax identification number, social security number, telephone number, e-mail address, bank account number,
- in the case of an individual entrepreneur: name, registered office, tax number, registration number, telephone number, e-mail address, bank account number.

(6) Duration of data management: 5 years from the termination of the contract.

XII. DATA MANAGEMENT ACTIVITY RELATED TO ATHLETES

(1) The ASSOCIATION manages the personal data of rowing athletes for the purpose of issuing competition permits, assisting with other administrative tasks related to competition, assessing and disbursing subsidies to athletes, and issuing school transcripts/certificates.

(2) The range of stakeholders: all athletes who apply for a competition license, who have a competition license, and who receive FEDERAL support.

(3) The legal basis for data management is a legal obligation, a legitimate interest, and the Data Subject's consent.

(4) Recipients of personal data: employees and data processors of the ASSOCIATION.

(5) Scope of processed personal data: name, address, place of birth, time, mother's name, telephone number, tax identification number, TAJ number, e-mail address, bank account number, photo, passport data (number, validity, copy), gender, citizenship, school information, parents' contact information.

(6) Duration of data management: no data deletion or destruction.

XIII. RULES RELATED TO DATA PROCESSING

1. General rules related to data processing

(1) ASSOCIATION uses an external data processor entrusted with the personal data it manages for the purpose of performing the following tasks:

- performing payroll tasks:**Benefit Consulting Kft.**
- performing accounting tasks:**Benefit Consulting Kft.**
- provision of legal services:**Fiák Ügyvédi Iroda, a member of the Fiák és Társai Ügyvédi Társulás**
- athlete and coach register:**NSR - Ministry of Human Resources**
- **Hungarian Olympic Committee, Hungarian Paralympic Committee, Hungarian Coaches Association, Hungarian University College Sports Association, National Sports Health Institute**

(2) The rights and obligations of the Data Processor in relation to the processing of personal data are defined by the Data Controller within the framework of the law and separate laws on data management.

(3) The ASSOCIATION declares that the Data Processor does not have the competence to make substantive decisions regarding data management in the course of its activities, it may process the personal data it has come to know only in accordance with the provisions of the Data Controller, it may not carry out data processing for its own purposes, and it is also obliged to process the personal data in accordance with the provisions of the Data Controller store and preserve.

(4) The ASSOCIATION is responsible for the legality of the instructions given to the data processor regarding data management operations.

(5) The ASSOCIATION's obligation is to provide Data Subjects with information about the person of the Data Processor and the place of data processing.

(6) The ASSOCIATION does not authorize the Data Processor to use additional data processors.

(7) The contract for data processing must be in writing. Data processing cannot be entrusted to organizations that are interested in business activities that use the personal data to be processed.

XIV. DATA SECURITY PROVISIONS

1. Principles of implementing data security.

(1) The ASSOCIATION may process personal data only in accordance with the activities set out in these regulations and according to the purpose of data management.

(2) The ASSOCIATION ensures the security of the data, in this context it undertakes to take all the technical and organizational measures that are absolutely necessary for the enforcement of the legislation on data security, data and privacy protection rules, and to establish the procedural rules necessary for the enforcement of the above-defined legislation .

(3) The technical and organizational measures to be implemented by the ASSOCIATION are aimed at the following:

the. ensuring the continuous confidentiality, integrity, availability and resilience of the systems and services used to manage personal data;

b. in the event of a physical or technical incident, the ability to restore access to and availability of personal data in a timely manner;

c. application of a procedure for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures taken to guarantee the security of data management.

(4) When determining the appropriate level of security, the risks arising from data management must be specifically taken into account, which in particular arise from the accidental or unlawful destruction, loss, alteration, unauthorized disclosure or unauthorized access to personal data transmitted, stored or otherwise managed.

(5) The ASSOCIATION protects the data with appropriate measures against unauthorized access, alteration, transmission, disclosure, deletion or destruction, as well as against accidental

against destruction and damage, as well as against becoming inaccessible due to changes in the technology used.

(6) The ASSOCIATION shall keep records of the data it manages in accordance with the governing legislation, ensuring that only those employees and other persons acting in the ASSOCIATION's sphere of interest who need it in order to perform their duties and responsibilities can see the data.

(7) The ASSOCIATION stores personal data provided in the course of each data management activity separately from other data, with the provision that - in accordance with the above provision - the separated data files can only be seen by employees with appropriate access rights and members who undertake personal cooperation.

(8) The ASSOCIATION does not forward personal data to third parties, it takes the necessary measures to exclude unauthorized access.

(9) The ASSOCIATION grants access to personal data to those employees who have submitted themselves to the obligation to comply with the data security rules by issuing a declaration of confidentiality with regard to the managed personal data.

(10) When determining and applying data security measures, the ASSOCIATION takes into account the state of the art at all times, and in the case of several possible data management solutions, chooses a solution that ensures a higher level of protection of personal data, unless it would represent a disproportionate difficulty.

2. Protection of IT records of the ASSOCIATION

(1) The ASSOCIATION undertakes the following necessary measures for the implementation of data security with regard to its IT records:

the. It provides the data files it manages with permanent protection against computer viruses (it uses real-time virus protection software.)

b. Takes care of the physical protection of the hardware devices of the IT system, including protection against elemental damage,

c. Ensures the protection of the IT system against unauthorized access, both in terms of software and hardware devices,

d. It takes all the measures necessary for the recovery of data files, performs regular backups, and performs separate, secure management of backup copies.

3. Protection of paper-based records of the ASSOCIATION

(1) In order to protect the paper-based records, the ASSOCIATION takes the necessary measures, especially in terms of physical security and fire protection.

(2) The employees of the ASSOCIATION, members who undertake personal cooperation and other persons acting in the interest of the ASSOCIATION are obliged to securely store and protect the data carriers that contain personal data that they use or possess, regardless of the method of recording the data, and protect them from unauthorized access , alteration, transmission, disclosure, deletion or destruction, as well as against accidental destruction and damage.

XIV. OTHER PROVISIONS

(1) The management of the ASSOCIATION is obliged to inform all employees of the ASSOCIATION of the provisions of these regulations.

(2) The management of the ASSOCIATION is obliged to ensure that all employees of the ASSOCIATION comply with the provisions contained in these regulations.

Budapest, 2024. 02.14

Czech Otto
president