2022 Budapest U23 Judo Grand Slam

Privacy Policy

PREAMBLE

The 2022 Budapest Judo Grand Slam (hereinafter referred to as: the "GS Hungary 2022") will be held in Budapest between 8 July, 2022 and 10 July, 2022, organized by the Hungarian Judo Association (hereinafter referred to as: the "Organizer or Data Manager").

During the performance of the tasks related to the preparation and conduct of the GS HUNGARY 2022, the Organizer intends to ensure the observance of and compliance with the data protection regulations and other regulations for the participants, sportsmen and other professionals, furthermore, the persons performing any task during the GS HUNGARY 2022. In addition to the above, it is a key goal of the Organizer to organize both events in the safest possible way under the circumstances existing due to the COVID-19 pandemic, classified as a global pandemic by the World Health Organization (WHO), which also requires the processing of special personal data.

In order to achieve the above objections, under 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, repealing Directive no. 95/46/EC, applicable from 25 May, 2018 (hereinafter referred to as: the "General Data Protection Regulation" or "GDPR"), furthermore, in the scope not regulated by the GDPR, under Act CXII of 2011 on information self-determination and freedom of information (Hungarian abbreviation: "Infotv."), as well as the current Hungarian regulations on the emergency situation due to the COVID-19 pandemic, the Organizers prepared the following policy:

I. Data of the Data Manager

1. **Data of the Data Manager:**
   Hungarian Judo Association (abbreviated name: HJA (Hung.: MJSZ; registered address: H-1146 Budapest, Istvánmezei út 1-3., registration number: 01-02-0000015, registry authority: Metropolitan Tribunal Court, tax number: 18157750-2-42, represented by: dr. László Tóth, Chairman)

2. **Contact details of the Data Manager:**
   Correspondence address: H-1146 Budapest, Istvánmezei út 1-3.
   Telephone: +36 (1) 460-6865
   E-mail: iroda@judo.hu

II. Definitions

For the purposes of this Policy:

1. **Data Processor**: is the natural person or legal entity, public authority, agency or any other body which manages / processes personal data on behalf of the Data Manager.

2. **Data management**: it 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. **Data Manager**: it means the natural person or legal entity, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the management / processing of personal data; where the purposes and means of such management / processing are determined by Union or Member State law, the data manager or the specific criteria for its nomination may be provided for by Union or Member State law.

4. **Privacy incident:** is a breach of security resulting in an accidental or unlawful destruction, loss, alteration, unauthorized disclosure or unauthorized access to personal data which are transmitted, stored or otherwise managed.

5. **GS HUNGARY 2022**: means the 2022 Judo Grand Slam to be held in Budapest between 8 July, 2022 and 10 July, 2022 and the related events organized by the Data manager.

6. **Data Subject** or the **Rightholder of personal data**: means a natural person, identified based on any personal data or identifiable - directly or indirectly.

This Privacy Policy distinguishes between the following categories of data subjects:

- Sportspeople: Athletes participating and contesting in the GS HUNGARY 2022 arriving from Hungary or abroad (Hungarian or other citizens);
- Sports professionals: Sports professionals (coaches, masseurs, etc.) participating in the GS HUNGARY 2022 arriving from Hungary or abroad (Hungarian or other citizens);
- Staff, agents, contracted partners and contributors of the Organizer;
- Volunteers.
- VIP Guests: VIP guests coming to the GS HUNGARY 2022;
- IJF staff: International Judo Federation (IHF) associates;
- International press associates,
- spectators

7. **IJF Covid Protocol:** a document containing the measures and recommendations issued by the International Judo Association to be followed for the safe implementation of the GS HUNGARY 2022 due to the COVID-19 pandemic, available at: covid.ijf.org

8. **Authority**: means the Hungarian National Authority for Data Protection and Freedom of Information.

9. **Consent**: means any voluntarily 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. **Policy**: means these regulations, which constitute the data management policy issued by the Data Manager for the GS HUNGARY 2022.

11. **Personal data**: any information relating to an identified or identifiable natural person, as a result of which the natural person may be individually, directly or indirectly identified, in particular, on the basis of an identifier, such as a name, identification card data or location data.

III. Scope of the Policy

1. The scope of this Policy covers all senior officers, employees, agents of the Data Manager and other persons in a legal regal relationship - aimed at employment - with the Data Manager who are obliged to comply with the statutory provisions on data protection in force at any time during their activities related to the GS HUNGARY 2022, together with the provisions of the GDPR, the Infotv. and this Policy.

2. The scope of the Policy also covers the sportspersons, sports professionals participating in the GS HUNGARY 2022, their relatives, the volunteers, press officers, natural persons performing tasks during the GS HUNGARY 2022 and other accredited persons, VIP guests, IJF staff, etc., whose personal data must be handled by the Data Manager in compliance with the provisions included in this Policy.

IV. Data management / data processing related to the GS HUNGARY 2022

IV/A. Accredited data subjects

This group contains the persons below:

- Sportspeople: Athletes participating and contesting in the GS HUNGARY 2022 arriving from Hungary or abroad (Hungarian or other citizens);
- Sports professionals: Sports professionals (coaches, masseurs, etc.) participating in the GS HUNGARY 2022 arriving from Hungary or abroad (Hungarian or other citizens);
- Staff, agents, contracted partners and contributors of the Organizer;
- Volunteers.
- VIP Guests: VIP guests coming to the GS HUNGARY 2022;
- IJF staff: International Judo Federation (IHF) associates;
- International press associates,

For these persons, the Data Manager provides accreditation, provides healthcare, if necessary, and these persons are also obliged to participate in COVID screening, which requires further data management.

1. **Purpose of data management:**

The purpose of the data management performed by the Data Manager is to ensure that the Organizer provides all services to these persons which are necessary for participating in a sports event, including, in particular, the following:

- implementation of accommodation reservation;
- providing transportation;
- accreditation for the GS HUNGARY 2022, secure access control to the GS HUNGARY 2022 sites and preparation of the accreditation card required for entry;
- performance of a contract in which one of the parties is the Data Subject or if it is necessary for taking steps at the request of the Data Subject prior to the conclusion of the contract;
- conducting and organizing the competition;
- provision of healthcare.
- broadcasting the GS HUNGARY 2022 to the public, newsfeed;
- compliance with the legal obligation for the Data Manager;
- enforcement of the legitimate interest of the Data Manager and the Data Subject;
- protection of the vital interests of the Data Subject and of other natural persons;
- protection against serious threats to health spreading across the border;
- adequate healthcare.

2. **Categories of personal data concerned; scope of data processed**

The Data Manager is authorized to learn about and manage the following personal data for the purposes specified in Article IV/A.:

a) Full name (last name and first name); *purpose: accommodation reservation, covid-screening, accreditation*

b) Full birth name; *purpose: accommodation reservation, covid-screening, accreditation*

c) Place of birth; *purpose: accommodation reservation,*

d) Date of birth; *purpose: accommodation reservation, covid-screening*

e) Mother's name; *purpose: accommodation reservation*

f) ZIP code; *purpose: accommodation reservation*

g) Residential address; *purpose: entering into contract*

h) 'TAJ' (Hungarian social security) number; *purpose: covid-screening*

i) Number of identity card (or passport for foreigners); *purpose: accommodation reservation, covid-screening*

j) Citizenship; *purpose: accommodation reservation, covid-screening, entering into contract*

k) Telephone number, E-mail address; *purpose: entering into contract*

l) Tax number; *purpose: entering into contract*

m) Sex; *purpose: covid-screening*

n) Photo; *purpose: accreditation*

o) Image and video recording of the Data Subject

p) Special data:

- The result of the COVID screening, which the Data Manager is obliged to pass on the National Public Health Center (NNK) in accordance with the relevant rules.

3. **The legal basis of data management:**

Pursuant to Article 6 Paragraph (1) f) of the GDPR, the legal basis for the data management is the legitimate interest of the Data Manager as the Organizer that:

- the requirements and regulations required by the IJF and relevant to the GS HUNGARY 2022 can be implemented, and that it can be organized and conducted in accordance with the relevant rules and customs;
- the Data Manager as the Organizer can implement the security and other regulations for access to the venues of the GS HUNGARY 2022;
- the GS HUNGARY 2022 is organized in accordance with the general professional sporting regulations and rules;

- the Data Manager can broadcast the GS HUNGARY 2022 to the public, give news about it, make reports, document it by means of photographs and videos, thus the Data Manager can promote the GS HUNGARY 2022 and the sport type of Judo;

In connection with the enforcement of the legitimate interest of the Organizer, the rights and freedoms of the data subjects have been considered, which necessitate the protection of personal data. In this context, the Data Manager took into account that the scope of the processed personal data was determined partly on the basis of an official call and epidemiological legislation, the regulation for the implementation of accommodation reservation, and partly in accordance with the process of accreditation and the conduct of the GS HUNGARY 2022. All personal data mentioned in Article 2 will be used by the Organizer exclusively in connection with the participation of the Data Subject in the GS HUNGARY 2022, to the extent and for the period necessary for the purpose of data management.
Considering that the processing of personal data is unconditionally necessary in connection with the participation of the Data Subjects in the GS HUNGARY 2022, and that the personal data will be processed explicitly and exclusively in connection with the participation of the Data Subject in the GS HUNGARY 2022, the Organizer has concluded that in connection with the use of the legal basis for data processing pursuant to Article 6 Paragraph (1) f) of the GDPR, there are no circumstances in which the rights and freedoms of Data Subjects would be given priority over the enforcement of legitimate interests of the Organizer as the Data Manager, precluding data management.

A group of the Data subjects (volunteer, Organizer's staff, agents, other contributors) with whom the Organizer enters into a contract to perform their duties, therefore Article 6 Paragraph (1) b) of the GDPR also serves as a basis for the management of personal data of these persons.

The legal basis for data management is also the fulfilment of the legal obligation of the Data Manager under Article 6 Paragraph (1) c) of the GDPR, including also the following:

- the Organizer should be able to provide adequate healthcare to those in need;
- the Organizer should be able to comply with the restrictive measures related to the COVID-2018 epidemic at the highest possible level and to exclude the risk of infection as much as possible.

In case of special data, the legal basis for data management is Article 9 Paragraph (2) a), c) and i) of the GDPR, given that:

- due to the epidemiological measures related to COVID-19, it is necessary to screen the participants for COVID-19, as well as to manage and transmit the test results, to identify the persons tested;
- knowledge of the COVID-19 antecedents (vaccination data, etc.) is required in connection with the COVID-19 epidemic (e.g.: due to the need for a quarantine obligation);

The legal basis for data management is also the consent of the Data Subject (Article 6 Paragraph (1) a), Article 9 Paragraph (2) a) of the GDPR). Obtainment of the consent of the Participant shall be collected by the Organizer in an online system where Data Subject is obliged to upload such a declaration with signing the proper rubric. By making the consent statement, the consent of the Data Subject to the data management shall be deemed to have been given.

4. Duration of data management:

The Data Manager will process the personal data of the Data Subject from the time they are transferred / provided until 10 days after the GS HUNGARY 2022 – with a special regard to the follow-up in case of COVID-19 infection – provided that the competent authority does not call on the Data Manager to preserve the personal data for another specified period.

5. Data transmission

The Data Manager shall only transfer the data of the data subjects to a third party in the following cases:

a) if the data transmission is required by the law (especially if a court, an authority or other body - as the addressee of the data transmission - delivers its official request to the Data Manager);

b) In accordance with the relevant Hungarian legislation, the Data Manager shall be obliged to forward the results of the SARS-CoV2 PCR tests and antigen tests performed on the data subjects to the National Public Health Center;
c) in order to provide accommodation, transportation and other services, the data necessary for the provision of the given service will be transmitted to the partner of the Data Manager providing accommodation, transportation and services;
d) If necessary, the Data Manager may transfer the data to the organizing body performing the access control.

IV/B. Spectators

The spectators can registrate for the GS Hungary 2022 by submitting their request on website www.judohungary.hu and submitting a scope of personal data.

1. Purpose of data management:

- Broadcasting the GS HUNGARY 2022 to the public, newsfeed;
- Access for the GS Hungary 2022, seating of spectators and organizing the auditorium

2. **Categories of personal data concerned; scope of data processed**

The Data Manager is authorized to learn about and manage the following personal data of the foreign persons living inside the Bubble for the purposes specified in Article IV/A. 1.:

a) Full name (last name and first name)
b) E-mail address
c) Image and video recording of the Data Subject

One requiring person is allowed to require more than one ticket.
On the website for registration, only the full name and e-mail address of the requiring person shall be collected. The other persons that the tickets are required for do not have to give their full name or e-mail address.
Following their accession, a photo can be taken of certain groups of spectators (eg. judo teams) based on a separate consent of such persons or their representative. The team photo may be used by the Data Manager on its own website or other own media interface. In case a minor person can be seen on such team photo, the consent of the legal representative is needed. For providing of such consent, the requiring person is responsible.
By knowing and accepting the present Privacy Policy, the persons performed on such team photos acknowledge that the Data Manager is entitled to use the team photos on its own website or other own media interface for the purpose of promoting the judo sport and to broadcast the GS HUNGARY 2022 to the public.
Any spectator accepts and acknowledges that by entering the GS Hungary 2022, image and video-recordings can be made of him/her, and that he/she accepts this by entering the GS Hungary 2022.

3. The legal basis of data management:

The legal basis for data management is the consent of the Data Subject (Article 6 Paragraph (1) a), Article 9 Paragraph (2) a) of the GDPR). Obtainment of the consent of the Participant shall be collected by the Organizer in an online system and is given also by entering the GS Hungary 2022.

4. Data transmission

The Data Manager shall only transfer the data of the data subjects to a third party in the following cases:
e) if the data transmission is required by the law (especially if a court, an authority or other body - as the addressee of the data transmission - delivers its official request to the Data Manager);
f) If necessary, the Data Manager may transfer the data to the organizing body performing the access control.

V. <u>Rights of rightholders of personal data</u>

V/A. Provision of information and access to personal data

1. If the personal data concerning the rightholder of the personal data are collected from the rightholder of the personal data, the Data Manager shall, at the time of obtaining the personal data – while, if the personal data were

not obtained from the rightholder of the personal data by the Data Manager, then within a reasonable time limit calculated from the obtainment of the personal data, but no later than within one month, or if the personal data are used for the purposes of communication with the rightholder of the personal data, then at the time of contact – be obliged inform the rightholder of the following:

a) the identity and contact details of the Data Manager;
b) the purposes and legal basis of data managements;
c) the scope of data subjects and data processed;
d) in case of data transmission, its recipient, legal basis and the scope of transmitted data;
e) the duration of data management;
f) the source of personal data;
g) the method of data management (manual or automated);
h) measures taken to ensure the security of personal data;
i) the rights of the rightholder of personal data and how to exercise them.

2. The Data Manager shall be authorized to fulfill the obligation to provide information - specified in Article V/A. 1. - through the privacy information note, privacy policy published on the website www.judohungary.hu or in the online accreditation system of GS HUNGARY 2022, as well as verbally, in writing (by e-mail) or in other ways suitable for providing information. If the rightholder of personal data requests special information from the Data Manager in connection with the processing of his / her personal data, the Data Manager shall immediately, but not later than within 30 days, provide personalized information specifying the data processing related to the rightholder of personal data. Exceptionally, in view of the complexity of the request and the number of requests, the 30-day period may be extended by the Data Manager by a further 60 days.

V/B. The right to rectification

1. If the Data Manager handles any personal data of the rightholder of the personal data inaccurately or incompletely, the rightholder may request the Data Manager to immediately rectify the inaccurately handled personal data or to immediately supplement the incompletely processed personal data on the basis of the data provided and justified by the rightholder.

2. The rightholder of the personal data (or his or her certified, authorized representative acting on his or her behalf) shall submit the request for rectification by appropriately completing ***Annex 1*** or making a declaration identical in content and sending it to the Data Manager. If the personal data are contained in a public document (e.g. an official card), the applicant is obliged to present or provide a copy of the public document certifying the content of the personal data to the Data Manager.

V/C. The right to data erasure

1. The rightholder of the personal data is authorized to request from the Data Manager the deletion of their personal data from all records of the Data Manager. Upon receipt of this request, the Data Manager shall immediately delete the personal data requested, if any of the following reasons exists:
   a.) the personal data are no longer needed for the purpose that constituted the basis of data management;
   b.) the rightholder of the personal data has withdrawn their consent to data management, and there is no other legal basis for the data management;
   c.) it is established that the personal data have been unlawfully handled by the Data Manager;
   d.) the Data Manager is obliged to delete personal data due to its statutory obligation.

2. The rightholder of the personal data shall submit the request for deletion by appropriately completing ***Annex 2*** or making a declaration identical in content and sending it to the Data Manager.

3. The Data Manager may refuse to delete personal data if any of the circumstances specified in Article 17 Paragraph (3) of the GDPR exists.

V/D. The right to restriction data management

1. The rightholder of the personal data is authorized to request the Data Manager to restrict the processing of data concerning his or her personal data if:

a) the rightholder of the personal data disputes the accuracy of the personal data collected and stored by the Data Manager, for the period of time to verify the accuracy of these data; or
b) the data processing performed by the Data Manager is illegal and the rightholder of the personal data objects to the deletion of the personal data collected and stored; or
c) the purpose of data management has ceased and the Data Manager does not need the personal data collected and stored, but the rightholder of the personal data requests further (restricted) data management in order to submit, enforce or protect his or her legal claims; or
d) the rightholder of the personal data exercises his or her right of protest for the duration of the investigation into the lawfulness of the right of protest.

2. The rightholder of the personal data (or his or her certified, authorized representative acting on his or her behalf) shall submit the request for restriction by appropriately completing ***Annex 3*** or making a declaration identical in content and sending it to the Data Manager.

3. The Data Manager is only authorized to store the personal data subject to the restriction. The Data Manager is authorized to process personal data subject to the restriction only in order to obtain the prior written consent or to present, enforce or protect the legal interest of the Data Subject and in the important public interest of the European Union or its Member State.

4. If the conditions for the restriction of personal data are not met, the Data Manager shall lift the restriction and shall be obliged to inform the rightholder of the personal data in advance.

V/E. The right to data portability

1. In respect of personal data which are processed automatically by the Data Manager with the consent of the rightholder of the personal data, the rightholder of the personal data may request the Data Manager to make his or her personal data provided by him / her available in electronic format, as defined in Article 20 Paragraph (1) of the GDPR.

2. When transmitting the collected and stored personal data in electronic form, the Data Manager is obliged to take into account that the rightholder of personal data is authorized to transmit the personal data collected and stored in electronic form to another data manager, or to ask the Data Manager to send these personal data directly to another data manager.

3. The rightholder of the personal data (or his or her certified, authorized representative acting on his or her behalf) shall submit the request for data porting by appropriately completing ***Annex 4*** or making a declaration identical in content and sending it to the Data Manager.

V/F. The right to object

1. The rightholder of the personal data may object to the processing of his / her personal data by the Data Manager, if the Data Manager performs the data processing in order to enforce the legitimate interest of the Data Manager or a third party.

2. The rightholder of the personal data (or his or her certified, authorized representative acting on his or her behalf) shall submit the objection request by appropriately completing ***Annex 5*** or making a declaration identical in content and sending it to the Data Manager.

3. Following the acceptance of the statement of objection by the Data Manager, the Data Manager shall not be authorized to process the personal data affected in order to enforce the legitimate interests of the Data Manager or a third party, unless the Data Manager proves that the data management is justified by an overriding legitimate reason which takes precedence over the interests, rights and freedoms of the Data Subject, or which relates to the submission, enforcement or defense of legal claims.

VI. <u>Data security and data storage procedures</u>

1. The Data Manager carries out the data processing in a way that respects the fundamental right to family and private life, other rights and freedoms of the rightholder of the personal data, while complying with the GDPR and other data protection legislation.

2. The provisions on the storage of personal data specified in this Policy apply both to personal data stored on paper or in electronic form, which form part of the registration system or which are handled in part or in full by the Data Manager in an automated manner. The Data Manager uses devices owned by the Data Manager for the electronic storage of personal data; any paper-based records are kept and stored at the headquarters of the Hungarian Judo Association.

3. Personal data collected and stored by the Data Manager for the purpose of data management may only be processed for the purposes specified in this Policy and legislation, under an appropriate legal title.

4. The personal data collected and stored by the Data Manager must be stored by the Data Manager during the data processing in such a way that they cannot be accessed by an unauthorized person. The Data Manager is obliged to ensure that the personal data collected and stored:
   - cannot be learned or accessed by unauthorized third parties;
   - are not subjected to unauthorized data processing;
   - cannot be altered, transmitted, disclosed or deleted by an unauthorized person;
   - are not transmitted in a manner different from the one specified in this Policy;
   - are not unauthorized modified, accidentally or unauthorizedly destroyed, deleted or made inaccessible;
   - are protected from loss and damage.

5. The Data Manager takes into account the current state and development of science and technology in its data management and related organizational activities. It seeks to use the most secure and risk-based data protection technology possible to protect the rights and freedoms of natural persons, in order to maintain data security.

6. The Data Manager shall implement appropriate technical and organizational measures aimed at implementing the data protection principles both when determining the method of data management and during data management.

7. The Data Manager shall take appropriate technical and organizational measures to ensure that only personal data which are necessary for the specific purpose of the processing are processed, with a particular regard to the amount of data, the extent of their processing, the duration of their storage and their availability.

VII. <u>Order of data transmission</u>

1. The Data Manager is not authorized to transmit the personal data managed and stored by it to another person or to make it available in any other form, except for cases where:
   a) the data transmission is required by the law;
   b) a court, an authority or other body - as the addressee of data transmission - delivers its official request to the Data Manager;
   c) the Data Subject has given their express consent to the data transmission;
   d) the recipient of the data transmission is a person in a legal relationship with the Data Manager and the purpose of the data transmission is to fulfill the legal relationship between the rightholder of the personal data and the Data Manager.

2. In case of necessity of the data transmission specified in Article VII. 1. c), the Data Manager shall be obliged to inform the rightholder of the personal data on the following:

   a) the name and contact details of the recipient / addressee of the data transmission and their representative;
   b) the fact that it contributes to the knowledge of information related to the data transmission and the data transmission itself;
   c) the exact purpose and specific scope of the data transmission;
   d) the rights of the rightholder of personal data;
   e) the possibility of lodging a complaint addressed to the Authority or a judicial remedy.

   The rightholder of the personal data may give his / her consent to a specific data transmission at the same time as the data processing consent, if the need for the specific data transmission is already known at the time of making this declaration.

VIII. Protocol to be followed in the event of a privacy incident

1. A privacy incident, in accordance with Article 4 Paragraph (12) of the GDPR, is a breach of security which may be:
   - breach of confidentiality, such as unauthorized disclosure of or access to personal data transmitted, stored or otherwise handled;
   - damage to access, such as accidental or unlawful destruction or loss of personal data transmitted, stored or otherwise handled;
   - breach of integrity, such as alteration of personal data transmitted, stored or otherwise handled.

2. If a senior officer, officer, employee of the Data Manager or other person in an employment relationship with the Data Manager finds that there is a possibility of security breaches in relation to the personal data collected and stored by the Data Manager, he or she shall immediately inform the Data Manager thereof (hereinafter referred to as: the "Alert").

   Security breach is any circumstance as a result of which damage occurs in the data management system and records of the Data Manager in a manner contrary to the data security provisions. A breach of security does not necessarily mean that a data protection incident has occurred.

3. The Data Manager is obliged to examine and evaluate the situation immediately after making the Alert. The investigation shall cover all elements of the circumstance indicated as a possibility of security breach, as well as the situation of all records, including personal data, affected by the Alert.

4. During the investigation, the Data Manager is primarily obliged to determine whether or not the security breach has actually occurred. If the Data Manager determines that the security has not been compromised, it shall terminate its proceedings and report the results of its investigation to the Management of the Data Manager and enter them in a record of privacy incidents.

5. If the Data Manager determines that security has been compromised, it is obliged to investigate whether or not a privacy incident has occurred. If the Data Manager determines that a privacy incident has not occurred, it is obliged to take all necessary measures to restore security, terminate their proceedings and report the results of the investigation to the Data Manager's Management and enter it in the privacy incident report.

6. If the Data Manager determines that a privacy incident has occurred at the same time as the security breach, it is obliged to examine, thirdly, whether the data protection incident poses a risk to the rights and freedoms of the rightholders of the personal data affected. If it finds that such a risk is not posed by the privacy incident, it shall be obliged to take all necessary measures to restore security, terminate their proceedings and report the results of the investigation to the Management of the Data Manager and enter them in a record of privacy incidents.

7. If the Data Manager finds that the privacy incident poses a risk to the rights and freedoms of the rightholders of the personal data affected at the same time as the security breach, the Data Manager shall be obliged to examine the extent of this risk.

   If the privacy incident poses a risk to the rights and freedoms of the rightholders of the personal data affected, it is obliged to report the results of the investigation to the Data Manager's Management and record it in the registry kept on privacy incidents and inform the Authority and the rightholders of the personal data affected of the privacy incident.

8. The Data Manager is obliged to fulfill the obligation to report without undue delay, but no later than within 72 hours of becoming aware of the privacy incident. The Data Manager becomes aware of the privacy incident when the Data Manager can establish with sufficient certainty the fact of the security breach. The Data Manager is obliged to assess the situation immediately after establishing the fact of the security breach.

   If the Data Manager is unable to carry out the recorded investigation within 72 hours, he or she shall be obliged to make the notification or provision of information within the time limit and is obliged to continue with the investigation. If the result of the investigation is available to the Data Manager, he or she shall be obliged to make an additional notification / additional provision of information or an amending notification / amending provision of information thereof.

9. The Data Manager is obliged to fulfill the notification obligation by filling in an electronic form systematized by the Authority or sending it to the Authority, or in case of another privacy authority of a Member State, in the form specified by this authority or the law of the given Member State. The following information must be provided in the notification:
   - the type of the privacy incident;
   - the category of rightholders of personal data affected by the privacy incident;
   - the (approximate) number of rightholders of personal data affected by the privacy incident;
   - the type of personal data affected by the privacy incident;
   - the (approximate) number of personal data affected by the privacy incident.

10. The Data Manager shall be obliged to make separate reports on privacy incidents involving personal data belonging to different data types.

11. The Data Manager is not obliged to make a notification if the privacy incident is not likely to endanger the rights and freedoms of natural persons. The Data Manager is obliged to perform the assessment of the existence of the risk, taking into account all the circumstances of the case. The fact that the privacy incident does not endanger the rights and freedoms of natural persons must be proved and reported, and the necessary measures must be taken to restore security.

12. The Data Manager is obliged to fulfill the obligation to provide information without undue delay. The Data Manager is obliged to assess the nature of the risk during the investigation, taking into account all the circumstances of the case. In this context, the Data Manager is obliged to take into account, inter alia:
   - the type of the privacy incident;
   - the type of personal data affected by the privacy incident;
   - the sensitivity of personal data affected by the privacy incident;
   - the extent of personal data affected by the privacy incident;
   - the vulnerability of the natural person affected by the privacy incident.

   Through a privacy incident, the risk to the rights and freedoms of a natural person is high if it could cause physical, material and non-material damage to the rightholder of the personal data.

13. The Data Manager is obliged to inform the rightholders of personal data of the following:
   - the fact and character of the privacy incident;
   - the name and contact details of the Data Manager;
   - the possible consequences of the privacy incident;
   - the means used by the Data Manager to mitigate the high risk resulting from the privacy incident and to restore the situation prior to the incident.

14. The Data Manager is obliged to provide the information in a form that is simple and (commonly) comprehensible by the rightholders of personal data, in the relevant language and without delay through a communication channel through which, based on the Data Manager's assessment, the information reaches the rightholders of personal data as soon as possible. The Data Manager may use several forms of communication at the same time in order to fulfill the obligation to provide information.

15. The Data Manager may omit the provision of information to the rightholders of personal data if
   a) the privacy incident does not pose a high risk to the rights and freedoms of the rightholders of personal data because, for example, the personal data communicated to an unauthorized third party cannot be accessed (due to encryption) and the Data Manager has a copy of the personal data affected;
   b) as a result of the measures taken immediately after becoming aware of the possibility of a privacy incident, the possibility of a high risk has not been raised;
   c) the risk resulting from the privacy incident cannot be considered high for other reasons.

16. Simultaneously with the fulfillment of the notification and information obligation, the Data Manager is obliged to take all measures that eliminate the security breach and the privacy incident immediately after learning of the results of the investigation. Within the framework of this, the Data Manager – taking into account its possibilities and circumstances – isobliged to restore the integrity, availability and confidentiality of the personal data involved in the privacy incident.

IX. Remedies

1. If you have any questions, suggestions or objections, please contact the Data Manager:

   Correspondence address: H-1146 Budapest, Istvánmezei út 1-3.
   Telephone: +36 (1) 460-6865
   E-mail: iroda@judo.hu

2. If the rightholder of personal data finds that the Data Manager violates the provisions of the data protection legislation regarding the processing of his / her personal data, he / she may apply to the competent court or the Hungarian National Authority for Data Protection and Freedom of Information in order to protect his / her rights.

   Contact details of the National Authority for Data Protection and Freedom of Information:
   Registered address: H-1055 Budapest, Falk Miksa u. 9-11.
   Telephone: +36 (1) 391-1400
   Fax: +36 (1) 391-1410
   Electronic availability: ugyfelszolgalat@naih.hu
   Website: http://naih.hu

Legislation referred to:

Regulation (EU) 2016/679 of the European Parliament and of the Council (27 April 2016) on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, repealing Directive 95/46/EC and applicable from 25 May, 2018 (hereinafter referred to as: the General Data Protection Regulation (GDPR))
Act CXII of 2011 on the Right of Informational Self-determination and the Freedom of Information
Act CLIV of 1997 on Healthcare
Act XLVII of 1997 on the Management and Protection of Healthcare and Related Personal Data
Government Decree No. 409/2020. (30 August) on certain rules applicable in case of epidemiological surveillance related to COVID-19
National Public Health Center (NNK): Procedural order for the new coronavirus identified in 2020 (epidemiological and infection control rules to be followed) 7 November, 2020
National Public Health Center (NNK): Procedural order In case of COVID-19-vaccinated persons, 28 January, 20211/2014. (16 January) EMMI (Ministry of Human Resources) Decree on the order of reporting of infectious diseases

X. Annexes

Annex 1 – Request for rectification

REQUEST FOR RECTIFICATION
ARTICLE 16 of the GDPR

To the Attention of the Hungarian Judo Association

Budapest
Istvánmezei út 1-3.
H-1146

Dear Data Manager,

I, the undersigned, _____ (name), (residential address: _____; place and date of birth: _____, mother's name: _____), as the rightholder of personal data, hereby submit the following

r e q u e s t

to the **Hungarian Judo Association**, as the data manager (hereinafter referred to as: the **Data Manager**).

I request the Honourable Data Manager **to rectify or supplement** my personal data in relation to **my inaccurate / incomplete personal data** managed by the Data Manager as follows:

INACCURATE PERSONAL DATA CURRENTLY MANAGED:

RECTIFIED, SUPPLEMENTED PERSONAL DATA:

I **enclose** a copy of the document containing the correct personal data to certify the rectification or addition to this declaration.

I ask the Honourable Data Manager to consider my above request.

Done at: _____

Sincerely,

NAME:

SIGNATURE:

Annex 2: Request for erasure

REQUEST FOR ERASURE
ARTICLE 17 of the GDPR

To the Attention of the Hungarian Judo Association

Budapest
Istvánmezei út 1-3.
H-1146

Dear Data Manager,

I, the undersigned, _____ (name), (residential address: _____; place and date of birth: _____, mother's name: _____), as the rightholder of personal data, hereby submit the following

r e q u e s t

to the **Hungarian Judo Association**, as the data manager (hereinafter referred to as: the **Data Manager**).

I request the Honourable Data Manager **to delete my personal data** managed by the Data Manager as detailed below, **from all records without any delay:**

PERSONAL DATA REQUESTED TO BE DELETED:

REASON FOR ERASURE: *(PLEASE MARK THE APPROPRIATE)*

a.) the personal data are no longer needed for the purpose that constituted the basis of data management;
b.) the rightholder of the personal data has withdrawn their consent to data management, and there is no other legal basis for the data management;
c.) it is established that the personal data have been unlawfully handled by the Data Manager;
d.) the Data Manager is obliged to delete personal data due to its statutory obligation.

I ask the Honourable Data Manager to consider my above request.

Done at: _____

Sincerely,

NAME:

SIGNATURE:

Annex 3 – Request for restriction on data management

REQUEST FOR RESTRICTION ON DATA MANAGEMENT
ARTICLE 18 of the GDPR

To the Attention of the Hungarian Judo Association

Budapest
Istvánmezei út 1-3.
H-1146

Dear Data Manager,

I, the undersigned, _____ (name), (residential address: _____; place and date of birth: _____, mother's name: _____), as the rightholder of personal data, hereby submit the following

r e q u e s t

to the **Hungarian Judo Association**, as the data manager (hereinafter referred to as: the **Data Manager**).

I request the Honourable Data Manager **to restrict the data processing of my personal data managed by the Data Manager** as detailed below:

PERSONAL DATA AFFECTED BY RESTRICTION OF DATA MANAGEMENT:

REASON: *(PLEASE MARK THE APPROPRIATE)*

a.) The Data Subject disputes the accuracy of the personal data.
b.) The data processing is illegal and the Data Subject opposes the deletion of the data.
c.) The Data Manager 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.
d.) The Data Subject objects to the data processing and it is necessary to establish the priority of the legitimate reasons of the Data Manager.

I ask the Honourable Data Manager to consider my above request.

Done at: _____

Sincerely,

NAME:

SIGNATURE:

Annex 4 – Data porting request

DATA PORTING REQUEST
ARTICLE 20 of the GDPR

To the Attention of the Hungarian Judo Association

Budapest
Istvánmezei út 1-3.
H-1146

Dear Data Manager,

I, the undersigned, _____ (name), (residential address: _____; place and date of birth: _____, mother's name: _____), as the rightholder of personal data, hereby submit the following

r e q u e s t

to the **Hungarian Judo Association**, as the data manager (hereinafter referred to as: the **Data Manager**).

I request the Honourable Data Manager **to release my personal data managed by the Data Manager** as detailed below, **for data porting purposes**:

PERSONAL DATA AFFECTED BY DATA PORTING:

REASON (PLEASE MARK THE APPROPRIATE):

The Data Manager manages the personal data on the basis of MY CONSENT / PERFORMANCE OF A CONTRACT.

I declare that the porting of my personal data above does not adversely affect the rights and freedoms of another person.

I ask the Honourable Data Manager to judge my above request, and to release my requested personal data in a structured, widely used, machine-readable format to ME / A THIRD PERSON *(please underline).*

In case of a third person, their name, address and e-mail address:
_____

Done at: _____

Sincerely,

NAME:

SIGNATURE:

Annex 5 – Objection

OBJECTION
ARTICLE 21 of the GDPR

To the Attention of the Hungarian Judo Association

Budapest
Istvánmezei út 1-3.
H-1146

Dear Data Manager,

I, the undersigned, _____ (name), (residential address: _____; place and date of birth: _____, mother's name: _____), as the rightholder of personal data, hereby submit my

o b j e c t i o n

to the Hungarian Judo Association, as the data manager (hereinafter referred to as: the Data Manager) against the data management performed by the Data Manager as follows:

PERSONAL DATA AFFECTED BY THE OBJECTION:

REASON: *(PLEASE MARK THE APPROPRIATE)*

a.) Enforcing the legitimate interests of the Data Manager or a third party.
b.) Direct marketing.

I ask the Honourable Data Manager to consider my above request and not to further process the requested personal data for the purpose indicated in the above reason.

Done at: _____

Sincerely,

NAME:

SIGNATURE: