



**ANTI-DOPING  
INFORMATION (INTELLIGENCE)  
COLLECTION AND PROCESSING POLICY**

**INFORMATION (INTELLIGENCE)  
COLLECTION AND PROCESSING POLICY  
OF THE INTERNATIONAL JUDO FEDERATION**

**2018**

## **Aim**

Pursuant to Article 5.8 of the World Anti-Doping Code, anti-doping organizations must obtain, assess and process anti-doping intelligence from all available sources in order to help deter and detect doping, to inform about the development of an effective and proportionate test distribution plan and/or to form the basis of an investigation into a possible anti-doping rule violation.

All investigative activities conducted by the International Judo Federation (IJF) and/or its affiliates are carried out in compliance with the regulations and standards of the World Anti-Doping Code, investigation rules and regulations of the applicable law. The Analysis and Investigation Team shall perform its tasks with respect for integrity, professionalism and confidentiality.

## **Definitions**

**Data Controller** – International Judo Federation (IJF)

**Anonymous Informant** – a person who anonymously provides information via e-mail, telephone, or at [www.ijf.org](http://www.ijf.org)

**PSI** - personal source of information / informant - a person cooperating in a secret and conscious manner with IJF, whose identity is known only to IJF and a designated person at ITA.

**APMU** – Athlete Biological Passport Management Unit

**Athlete Support Personnel** - Any coach, trainer, manager, agent, team staff, official, medical, paramedical personnel, parent or any other person working with, treating or assisting an Athlete participating in or preparing for sports competition.

**Athlete** - Any person who competes in sport at the international level (as defined by each International Federation) or the national level (as defined by each National Anti-Doping Organization). An Anti-Doping Organization has discretion to apply anti-doping rules to an athlete who is neither an International-Level Athlete nor a National-Level Athlete, and thus to bring them within the definition of "Athlete." In relation to Athletes who are neither International-Level nor National-Level Athletes, an Anti-Doping Organization may elect to: conduct limited testing or no Testing at all; analyze samples for less than the full menu of prohibited substances; require limited or no whereabouts information; or not require advance TUEs. However, if an Article 2.1, 2.3 or 2.5 anti-doping rule violation is committed by any Athlete over whom an Anti-Doping Organization has authority who competes below the international or national level, then the Consequences set forth in the Code (except Article 14.3.2) must be applied. For purposes of Article 2.8 and Article 2.9 and for purposes of anti-doping information and education, any person who participates in sport under the authority of any signatory, government, or other sports organization accepting the Code is an Athlete.

**IJF** – International Judo Federation

**IJF Analysis and Investigation Team** – an Ad Hoc team appointed on a case-by-case basis by the IJF President and, where needed, upon consultation with the ITA.

**ITA** – International Testing Agency

## **1. Collection of anti-doping intelligence**

1.1 IJF shall obtain information on activities and behaviors suggesting or indicating the use of doping from all available sources, including from athletes and athlete support personnel (including Substantial Assistance provided in accordance with Article 10.6.1 of the Code) and from representatives of the public, including from PSIs or anonymous informants, sample collection agencies and personnel (through reports of sample collection sessions, event reports or otherwise), laboratories, pharmaceutical companies, national sports associations, event organizers, law enforcement agencies, other regulatory and disciplinary bodies, and the media. For purposes of further illustration, the collection of anti-doping intelligence may occur, *inter alia*, through/via the following sources, channels and/or means:

### **External Sources / Means**

- IJF whistleblowing online platform
- WADA SpeakUp
- Media and news reports
- Social media and other open source tools
- Law enforcement authorities reports/information
- Other Anti-Doping Organizations' (ADOs) reports
- Laboratory reports

### **Internal Sources / Means (including IJF partners)**

- APMU reports, comments and recommendations
- Analysis of testing history
- Rankings and competition results
- Sample Collection reports and on-field observations
- Doping Control Officers and Chaperones reports and observations
- Doping Control Forms and Sample Collection documentation
- National Federations reports
- Athletes and Athletes' entourage reports
- IJF staff, officials and affiliates reports and observations
- ITA reports and observations

1.1.1 The IJF Analysis and Investigation Team shall be responsible for any investigation conducted within the scope of this Policy and shall cooperate with ITA and WADA in the conducting of the investigative proceedings.

1.2 All information and/or evidence provided by the relevant source will be assessed by the IJF Analysis and Investigation Team in cooperation with ITA, in order to determine its degree of validity and usefulness. The IJF Analysis and Investigation Team shall ensure that the PSIs and other

sources are maintained confidential at all times, unless disclosure of confidentiality is permitted in writing by the PSI. At all stages of the process, communication with the informant may be recorded and reported - in whole or in part - in a written report.

- 1.3 In order to obtain more information and evidence, the Analysis and Investigation Team may conduct a secure conversation with the informant without incurring costs at a neutral location indicated by the informant.
- 1.4 Interviews will be recorded using a recording device according to the format of communication (eg. phone, video call, etc.). The recorded material may be made available to the informant upon written request in the form of prepared transcripts or recordings of recorded conversations. The produced materials are classified, stored in a secure location in the IJF Presidential office, and access to them is limited. The method of storage generally depends on the type of classification given to the material concerned.
- 1.5 IJF shall collect and process anti-doping data by introducing policies and procedures that guarantee the safe handling of anti-doping information obtained or received, prevent the disclosure of the source of information, protect against leakage and unintentional disclosure of information, and process and disclose anti-doping information provided to it by law enforcement agencies, other competent authorities and/or other third parties only for legitimate anti-doping purposes.
- 1.6 Physical evidence (documents, photos, videos, products and/or related packaging, discarded medical equipment, etc.), audio recordings, etc. shall be stored in a secure environment with restricted access as specified in this document. All physical evidence will be deposited in a secured armored cabinet.
- 1.7 The IJF confidential e-surface may be accessed at <https://reportdoping.judobase.org/form>.

## **2 Assessment and analysis of anti-doping intelligence**

- 2.1 IJF (or ITA on behalf of the IJF) shall assess all anti-doping intelligence as soon as it is received for its materiality, reliability and accuracy, taking into account the nature of the source and the circumstances in which the information was obtained or received.
- 2.2 All anti-doping information obtained or received by IJF should be compared and analyzed in order to determine the patterns, trends and relationships that may help the anti-doping organization to develop an effective anti-

doping strategy and/or determine (when the information relates to a particular case) whether there is a reasonable reason to suspect that a violation of anti-doping rules may have occurred, justifying further investigation in accordance with Section 12.0 of the International Standard for Testing and Investigations.

- 2.3 IJF collects and records all relevant information and documentation as soon as possible. IJF shall ensure that investigations are conducted fairly, objectively and impartially at all times. The conduct of investigations, the assessment of information and evidence identified during the investigation and the outcome of the investigation shall be fully documented.
- 2.4 Analytical and Non-Analytical Intelligence shall be used by the IJF and/or ITA, amongst others, for the following purposes:
- to design, amend and/or adapt the IJF Registered Testing Pool and/or Testing Pool;
  - to review and revisit the Test Distribution Plan as needed;
  - to conduct ad hoc Out-of-Competition doping control tests;
  - to conduct In-competition or Out-of-Competition target testing;
  - to direct further and/or specific analyses on a sample
  - to retain specific samples for Long Term Storage;
  - to conduct further investigations and determine whether an anti-doping rule violation by an Athlete or other Person under the IJF jurisdiction has occurred;
  - To develop and compile evidences that support the initiation of disciplinary proceedings in accordance with IJF Anti-Doping Rules.
- 2.5 In the framework of the Athlete Biological Passport program, the IJF shall be bound by any and all determinations, requests and/or recommendations issued by the APMU and shall duly implement any such recommendations without delay, including without limitation any requests for additional or target testing or supplementary analyses, such as IRMS, ESA, etc.
- 2.6 Any APMU recommendations shall be conveyed to the IJF and/or ITA via ADAMS and/or other secured channels in compliance with the WADA International Standards as applicable.

### **3 Intelligence outcomes**

- 3.1 Anti-doping intelligence shall be used to assist in developing, reviewing and revising the Test Distribution Plan and/or in determining when to conduct Target Testing, in each case in accordance with Section 4.0 of the

International Standard for Testing and Investigations, and/or to create targeted intelligence files to be referred for investigation in accordance with Section 12.0 of the International Standard for Testing and Investigations.

- 3.2 Upon completion of the investigation, the IJF Analysis and Investigation Team will inform the IJF President and prepare a report containing recommendations and references. All relevant information on which the investigation was based will then be passed on to the relevant anti-doping organizations for resolution. IJF may, if necessary, refer the case to law enforcement agencies.
- 3.3 In accordance with the International Standards for Testing and Investigation, the IJF shall inform WADA of any relevant outcomes connected with an investigation under the scope of this Policy and shall seek WADA's Intelligence Team assistance in all instances when required or needed.

#### **4. Data security**

4.1 Access to the gathered data shall be granted solely to:

- 1) Data Controller: International Judo Federation
- 2) ITA on behalf of IJF
- 3) Members of the IJF Analysis and Investigation Team
- 4) World Anti-doping Agency

4.2 The data are processed and protected in accordance with the current IJF Privacy Policy.

4.3 The following organizational and technical measures to secure the data processing area shall be implemented:

- 1) The building of IJF is equipped with an electronic anti-burglary system with non-stop alarm signal monitoring (external protection);
- 2) The places designated for the processing of personal data shall be in rooms protected by ordinary, Yale-type locks;
- 3) Direct security (protection) of the data processing area against unauthorized access is provided by Users during the performance of their duties;
- 4) The presence of unauthorized persons in the premises of the personal data processing area is allowed only in the presence of at least one

User;

- 5) The premises of the data processing area shall be closed during the absence of Users, in such a way that access by unauthorized persons is prevented;
- 6) Screen monitors shall be located in such a way that the data cannot be read by unauthorized persons;
- 7) Issue and return of the keys to the data processing area shall be recorded with simultaneous confirmation by the receiving person, if the Data Controller so decides;
- 8) The keys to rooms are collected by the Users from the place designated for their storage; during and after work keys to rooms and keys to cabinets and desks shall be kept in a place which is inaccessible to unauthorized persons. It is forbidden to leave room keys in doors or public areas. After completion of work, the keys to rooms and cabinets or desks should be taken away and deposited in an appropriately secured place known only to the Users, the Data Controller or a person authorized by the Data Controller. If the Data Controller so decides, the keys to rooms and cabinets or desks can be removed from the personal data processing area, provided that duplicate keys remain at the disposal of the Data Controller and, if the Data Controller so decides, at the disposal of another person authorized by the Data Controller;
- 9) If it is necessary to temporarily leave the room during which time it will be unattended by another User, the room should be locked, the key should be taken by the User or deposited in a place designated by the Data Controller, if the Data Controller so decides;
- 10) Duplicate keys to rooms, cabinets and desks should be at the sole disposal of the Data Controller and, if the Data Controller so decides, also at the disposal of another person authorized by the Data Controller;
- 11) Duplicate keys to rooms, cabinets or desks should only be issued to authorized persons, only in justified circumstances, e. g. for example in case of burglary, fire, rescue operations, evacuation, prolonged absence of the User, etc., unless the Data Controller has specified a different procedure in this respect;
- 12) Access to the premises of the data processing area by law enforcement service, repair, technical, maintenance or other services shall only be possible in the presence of at least one authorized User, unless the



possibility of accessing personal data has been eliminated by appropriate protection against their seizure, loss, destruction or damage. The decision on how to proceed and the data protection measures taken in the case described above is made by the Data Controller or a person authorized by the Data Controller;

13) The entrance door to the data processing area must be closed during the presence and absence of the Users;

14) After the completion of work all windows in the building must be closed;

15) Users must monitor movement or stay of any unauthorized persons in the data processing area. Attention should be paid to the presence in the premises of persons who behave in a non-routine manner, e. g., who are nervous, improperly dressed at the time of the day, year or weather, who stay in the premises without a clear purpose or need, who carry suspicious luggage or objects with them.

4.4 The Data Controller shall keep records of persons authorized to process data, which shall contain the following information:

- 1) first and last name of the authorized person;
- 2) the date on which the data processing authorization was granted;
- 3) an identifier if the data are processed in the information system.

4.5 Persons who have been authorized to process data shall be obliged to keep these data and the methods of their protection confidential.

4.6 Persons involved in the information processing process shall have appropriate authority and participate in the process to a degree commensurate with their tasks and responsibilities in ensuring the security of information.

## **5. Information exchange**

5.1 IJF shall exchange the anti-doping information obtained (on the terms and in accordance with the applicable legal regulations) with other anti-doping organizations (e.g. if the information collected relates to athletes or other persons subject to these anti-doping organizations and/or law enforcement authorities and/or other relevant regulatory or disciplinary bodies (e.g. if the information obtained suggests possible commission of a statutory offence or violation of other rules of conduct)).

- 5.2 Data obtained through an exchange with law enforcement authorities and/or other competent regulatory or disciplinary authorities shall be retained by IJF for the time necessary to achieve the purpose for which the data were obtained or for the time necessary to detect and prosecute perpetrators of a crime or offence and to prevent or combat crime, in accordance with the time limits and rules for processing data in data files controlled by IJF, but for a maximum period of 10 years from the date of their acquisition.
- 5.3 IJF shall verify the collected data once every two years and shall delete or anonymize unnecessary data.
- 5.4 When transferring or making data available to, or receiving them from law enforcement authorities and/or other relevant regulatory or disciplinary authorities, IJF shall record or document the fact that it has transferred, made available or received such data in order to verify the legality of data processing, their integrity and security.
- 5.5 The recording or documentation in question shall be carried out in accordance with the rules on data processing in data filing systems controlled by the concerned authorized entity.