INTERNAL WHISTLEBLOWING POLICY

I. Foundation

The purpose of this policy (hereinafter: ”Policy”) is to ensure that the International Federation of Teqball (*Nemzetközi Teqball Szövetség*; registered seat: Expo tér 5-7., 1011 Budapest, Hungary; registration number: 01-02-0017651; hereinafter: ”FITEQ”) has full and accessible channels to facilitate the effective detection, investigation and remediation of possible violations of law or other breaches.

Our goal is to fully ensure transparent and ethical organisational operation, for which the establishment of a whistleblowing system that provides appropriate guarantees and also enables FITEQ to handle whistleblowing reports properly, is an essential tool.

Our FITEQ is committed to protecting whistleblowers, as they are the starting point and cornerstone of ethical organisational practices. Creating an environment of trust and protection encourages whistleblowers to report in a confident and responsible manner, which contributes to the integrity and long-term success of FITEQ.

II. Definitions

For the purposes of this Policy, the following definitions apply:

1. „to report” “reporting” “to raise an allegation”: the oral or written communication of information on breaches;
2. „report” “allegation”: oral or written communication containing information on breaches;
3. „whistleblower”: a natural person, as defined in point III.1. of this Policy, who reports information about breaches obtained in the context of a specific legal, contractual or other relationship;
4. „person implicated in the report”: the natural or legal person involved in the report;
5. „employment relationship”: any legal relationship in which the employee carries out an activity for and under the direction of the Employer for consideration or otherwise employed, including, but not limited to, employment relationship;
6. „Employer”: FITEQ;
7. „employee”: a natural person who carries out an activity for and under the direction of the Employer within the framework of an employment relationship for consideration or otherwise employed, including in particular, but not limited to, the Employer's employees;
8. „Investigator”: the person investigating the reports as defined in point III.3.2. of this Policy;
9. “Code of Conduct” means Employer’s internal policies collectively;
10. “breach” means an act or omission for which at least one of the following conditions is fulfilled:
    a) unlawful,
    b) against the Employer's Code of Conduct,

c) constitutes other misconduct within the meaning of Act XXV of 2023 on complaints, disclosures in public interest, and related rules on reporting abuses (hereinafter "Complaints Act").

III. Channels of the whistleblowing system

III.1. The following persons can raise allegations in the whistleblowing system:

a) employed by the Employer;
b) an employee whose existing employment relationship with the Employer has been expired or terminated;
c) a person wishing to enter into an employment relationship with the Employer and for whom the procedure for the establishment of such a relationship has commenced;
d) the sole proprietor, the sole proprietorship, if it has a contractual relationship with the Employer;
e) a person with an ownership interest in the Employer and a member of the Employer's administrative, executive or supervisory board, including a non-executive member;
f) a contractor, subcontractor, supplier or agent that has initiated a procedure for establishing a contractual relationship, is or has been under a contractual relationship with the Employer, as well as the persons under the supervision and control thereof;
g) trainees and volunteers of the Employer;
h) a person intending to enter into a legal relationship described in Subclauses (d), (e) or (g) with the Employer provided that the procedure for the establishment of such a legal relationship has been initiated, and
i) a person whose legal relationship described in Subclauses (d), (e) or (g) with the Employer has expired or has been terminated.

III.2. When raising an allegation, in order to ensure that it can be investigated efficiently, the whistleblower shall provide their name, email address (or, in the absence thereof, telephone contact details) and reference to their legal, contractual or other relationship (e.g. employment relationship) with the Employer as defined in Section II.1. of this Policy. In the allegation, the whistleblower shall also provide the name(s) of the person(s) implicated in the allegation and the name(s) of the person(s) who may have relevant information about the facts of the whistleblowing, a detailed description of the case and any relevant information about the case.

III.3.1. The report can be made in the following ways:

a) oral, by means of a personal meeting with the person designated in point III.3.2 of the Policy, which can be initiated personally, or by sending an email to the email address specified in point III.3.2 of the Policy,
b) written:
    i. electronically, by sending an e-mail to the e-mail address set out in point III.3.2. of the Policy,

III.3.2. The following person will be the Employer's Investigator:

Name:	Blascsák Szilvia Mária
Email adress:	whistleblowing@fiteq.org

III.4. (1) The whistleblower raise their allegation in good faith. An allegation shall be considered to be raised in good faith if the whistleblower had reasonable grounds for believing, at the time of raising the allegation, that the reported information was true.

(2) If determined beyond doubt that the whistleblower has provided false data or information in bad faith, and

(a) it gives rise to an indication that a crime or an infraction was committed, the Employer shall, upon request, hand over the personal data of the whistleblower to the designated authority or person entitled to initiate or conduct the proceedings,

(b) where it is likely that the whistleblower caused unlawful damage or other harm to the rights of others, the Employer shall hand over the personal data of the whistleblower to the designated authority or person entitled to conduct the proceedings.

IV. Procedural rules

IV.1. Procedural principles:

a) All persons involved in the investigation shall act in accordance with the principles and rules set out in this Policy.

b) The Employer shall deal with reports impartially, fairly and within a reasonable time, and shall give reasons for its decisions.

c) Whistleblowers shall have the right to have their reports processed by an independent Investigator in a fair procedure. The Investigator shall not be instructed and shall not accept any instructions in connection with the initiation, conduct or conclusion of any proceedings under this Policy.

d) All participants in the investigation shall act in good faith and cooperate with the other participants.

IV.2. (1) If a report orally in accordance with Section III.3.1. a) of this Policy, the Employer shall, in its option:

(a) make a recording of the oral report in a durable and retrievable form - after providing information relating to the protection of personal data, or;

(b) make a transcript of the oral report and shall offer the reporting person the opportunity to check, rectify and agree with the content of the transcript of the oral report by signing it, and shall provide the whistleblower with a copy thereof.

(2) The Employer shall make a complete and accurate transcript of the oral report.

(3) In the case of an oral report, the whistleblower shall be advised of the consequences of raising an allegation in bad faith, to the procedural rules governing the investigation of the report, and that their identity - if they provide the necessary details for establishing their identity - shall be treated confidentially at all stages of the investigation.

IV.2. The Employer shall send the whistleblower an acknowledgement of the notification within 7 days of receipt of the written report made in accordance with point III.3.1. b) of this Policy. The Employer shall provide the whistleblower with general information on the procedural and

data management rules under this Policy as part of the confirmation. Annex 1 to this Policy contains the relevant information on data management.

The Employer – if the nature of the report so indicates – shall draw up an internal investigation plan, which shall involve the Data Protection Officer to the extent reasonable.

IV.3. At the start of the investigation, the person implicated in the report shall be informed in detail about the report, about their rights with respect to the protection of his or her personal data, and about the rules on handling their data. In accordance with the principle of procedural fairness, the person implicated in the report shall be given the opportunity to express their position regarding the report personally or through their legal representative, and to provide corroborating evidence. In exceptional cases, the person implicated in the report may be informed at a later time if immediate information would hinder the investigation of the report.

Present Clause shall apply to any person who may have relevant information about the contents of the report.

IV.4. (1) The Employer shall investigate the allegations contained in the whistleblowing within the shortest time allowed by the circumstances, but not later than thirty days from the receipt of the report.

(2) The Employer may extend the time limit provided for in Subclause (1) for a duly justified reason, of which the whistleblower shall be notified at the same time. In that case, the reporting person shall be informed of the estimated duration of the investigation and the reasons for extending the investigation. In either case, the time limit for the investigation of the report and for the information of the reporting person may not exceed three months.

(3) In the course of the investigation of the report, the Employer shall maintain contact with the whistleblower, and may invite the whistleblower to supplement or clarify the report, to clarify the facts of the case and to provide additional information.

IV.5. The investigation of the report may be omitted if:

a) the report is made by an unidentifiable whistleblower,

b) the report was not made by a person entitled to raise allegations pursuant to Clause III.1 of this Policy,

c) the report is submitted by the same whistleblower with the same content as a previous report, or

d) the harm to the public interest or a compelling private interest would not be proportionate to the restriction of the rights of the person implicated in the report resulting from the investigation of the report.

IV.6. (1) In the course of the investigation, the Employer shall assess the correctness and relevance of the circumstances included in the report and shall take appropriate measures to remedy the breach(es). The Employer may decide involve an expert if it is deemed necessary to reach an appropriate decision.

(2) If the investigation establishes that a breach has taken place, the Employer shall apply labour law or economic measures proportionate to the seriousness of the breach, otherwise the investigation shall end without taking any measures.

(3) If the report justifies the initiation of criminal proceedings, the Employer shall arrange for the filing of a criminal complaint.

IV.7. (1) The Employer shall inform the whistleblower in writing of the investigation of the report or of the decision not to investigate the report, the reasons for the decision not to investigate, the result of the investigation of the report and the measures taken or planned.

(2) Written information may be omitted if the operator of the internal whistleblowing system has orally informed the whistleblower of the information referred to in subsection (1) who has taken note of the information.

V. Persons operating the whistleblowing system

Reports are received only by the impartial person designated by the Employer, the Investigator, who cannot be instructed in the investigation and the activities related to the report.

The name of the person appointed as Investigator is indicated in Section III.3.2 of this Policy.

The Investigator shall decide within 3 (three) working day after the start of the processing of the report whether the examination and investigation of the report requires special expertise. If the investigation of the report requires special expertise, the Investigator may, after having duly anonymised all files pertaining to the case, consult another person in a legal relationship with the Employer or call upon an external expert with expertise in the matter, within the limits of a budget approved by the Employer.

In the course of the investigation, the Investigator may interview any person and exercise any powers of control that the employer is entitled to pursuant to the provisions of Act I of 2012 on the Labour Code, provided that it may be justified for the proper investigation of the report.

VI. Privacy notice

VI.1. The purpose of processing under the whistleblowing system is to investigate the report and to remedy or stop the conduct that is the subject of the report. Where personal data processed under the whistleblowing system are intended to be processed for a purpose other than the above, the Data Protection Officer must be informed prior to the processing for the other purpose, who will examine the compatibility of the original and the new processing purposes and inform the controller accordingly.

VI.2. During the recording and examination of the report, personal data of the whistleblower, the natural person concerned by the report and the person who may have relevant information on the subject matter of the report may be collected. Personal data which are manifestly not relevant for the processing of a particular report should not be collected and should be deleted without delay if such data are collected accidentally.

VI.3 Where the personal data of the whistleblower (or other data subject) are transferred to a designated authority competent to handle the procedure initiated on the basis of the whistleblowing, it should be examined whether the recipient is entitled to process those personal data under the law. If the right exists, consent from the whistleblower need not be obtained. In the absence of entitlement, the prior written consent of the whistleblower is required.

VI.4. The consent of the whistleblower is not required for the transfer of data if they have communicated false data or information in bad faith and there are indications that a crime or

infraction has been committed. In such a case, the personal data must be transmitted to the designated authority or person.

VI.5. The consent of the whistleblower is not required for the transfer of data if the whistleblower has communicated false data or information in bad faith and there are reasonable grounds to believe that they have caused unlawful damage or other harm to another person. In such a case, personal data must be disclosed to the designated authority or person entitled to initiate or conduct the proceedings, upon request.

VI.6. The processing of data in the whistleblowing system requires an enhanced level of confidentiality and secrecy. The identity of the whistleblower who discloses his/her identity, the person who may have material information about the facts contained in the whistleblowing report and the personal data of the person concerned by the report must not be disclosed to any person other than the authorised person. When anonymising personal data and documents processed in the whistleblowing system, where appropriate, special care should be taken to ensure that the identity of the data subjects cannot be identified from the context after anonymisation.

VI.7 Pending the conclusion of the investigation or the initiation of formal prosecution as a result, the Investigators of the report may share information on the content of the report and the person concerned with other departments – in addition to informing the person concerned by the report – or staff of the employer to the extent strictly necessary for the conduct of the investigation.

VI.8 In the case of a data subject's request for information and access, the Data Controller shall not disclose to the applicant the identity of the whistleblower or of the person who may have access to the information contained in the whistleblowing. The data subject making the request shall have the right to access only the personal data relating to him / her.

VI.9 If the investigation reveals that the report is unfounded or that no further action is necessary, the data relating to the report shall be deleted within 60 days of the end of the investigation.

If action is taken on the basis of the investigation, – including action taken against the whistleblower in legal proceedings or disciplinary action – the data relating to the report may be processed within the framework of the whistleblowing system until the final conclusion of the proceedings initiated on the basis of the report at the latest.

VII. Protection of whistleblowers

The Employer is committed to protecting whistleblowers from any adverse legal consequences that they may suffer in connection with their reporting.

The freedom of whistleblowers to report freely and without interference is an essential organisational interest, which must be safeguarded accordingly.

The Employer seeks to protect whistleblowers primarily, but not exclusively, through full and high compliance with data management and data protection rules. In its procedures, the Employer shall share information with the persons involved based on strict necessity in order to ensure the confidentiality and secrecy of the report.

VIII. Final provisions

This Policy shall enter into force on the day of their publication.

In matters not regulated by this Policy, the provisions of Hungarian law, in particular Act I of 2012 on the Labour Code, and Act XXV of 2023 on complaints, disclosures in public interest, and related rules on reporting abuses shall apply.

This Policy is published in English and Hungarian. In case of any discrepancy between the two versions, the Hungarian version shall prevail.

ANNEX 1.

Data management information regarding to the whistleblowing-system

Name of the Data Controller: International Federation of Teqball (registered office: 1011 Budapest, Expo tér 5-7., registration number: 01-09-174699; tax number: 24390305-2-42, hereinafter: Data Controller)

Contact details of the Data Controller:

- Postal address: 1101 Budapest, Expo tér 5-7.
- E-mail: whistleblowing@fiteq.org

Contact details of the Data Protection Officer:

- Name: KCG Partners Ügyvédi Társulás
- E-mail: privacy@fiteq.org

Purpose of the handling of personal data: investigating the whistleblowing and remedying or ending the conduct that is the subject of the whistleblowing.

Legal basis for handling personal data:

- the Data Controller shall process the personal data of the persons concerned in the report that is necessary in order to comply with the Employer's legal requirement to operate an internal whistleblowing system, including the receipt and investigation of reports containing information on unlawful or suspected-to-be unlawful acts, omissions and other breaches, as well as the actions to be taken in response thereof. [GDPR Art.6.(1)c); Complaints Act Section 18(1) and 18(3); Complaints Act Section 26(4)]

The source of the personal data:

- the whistleblower;
- the person who may have substantive information on the matters contained in the report; and
- the natural person whose conduct or omission gave rise to the report (hereinafter: **the natural person concerned by the report**).

Possible consequences of not handling the data:

- The whistleblower has the discretion to decide whether or not to make a report. In case a report is not made, the Data Controller will not become aware of the act or omission that is the subject of the report and will not investigate it.
- If the person who may have substantive information on the subject of the report does not make a statement, the Data Controller will investigate the report on the basis of the available information.
- If the natural person concerned by the report does not make a statement, the Data Controller will investigate the report based on the information available.

The categories of personal data concerned:

- name and e-mail address of the whistleblower (if not available, telephone number), the legal relationship with the Employer within the meaning of point III.1 of this Policy (e.g. employment); and
- the name(s) of the person(s) concerned by the report, in addition to the name(s) of the person(s) who may have substantive information on the matter of the report, and any additional personal data and relevant information in the detailed description of the case that has emerged in relation to the case which are indispensable for the investigation of the report.
- depending on the facts of the case to which the report relates, there may also be processing of personal data falling under a special category of personal data (personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, personal data relating to trade union membership, genetic and biometric data for the purpose of uniquely identifying natural persons, health data and personal data concerning the sex life or sexual orientation of natural persons). Processing of special data shall be subject to the condition that the processing is necessary for compliance with the obligations of the controller or the data subject arising from legal requirements governing employment and for the exercise of his or her specific rights, if Union or Member State law, which also provides for adequate safeguards to protect the fundamental rights and interests of the data subject, so allows (GDPR article 9. paragraph (2) point b)), and data processing necessary for the establishment, exercise or defence of legal claims (GDPR article 9. paragraph (2) point f)).

The recipients of personal data and the categories of recipients:

- the personal data of the data subjects may be transferred to the competent authority to carry out the procedure initiated on the basis of the report; if the report justifies the initiation of criminal proceedings, arrangements must be made to file a criminal report.
- if *the whistleblower has communicated false data or information in bad faith* and *there are indications that a criminal offence or infraction has been committed*, their personal data must be handed over to the authority or person responsible for the procedure.
- where it has become apparent that *the whistleblower has supplied false data* or information in bad faith and there are reasonable grounds for believing that *they have caused unlawful damage or other legal harm to another person*, their personal data must be handed over to the authority or person entitled to initiate or continue the proceedings, *at the request of that authority or person*.

There will be no transfers to third countries or international organisations.

No automated decision-making or profiling takes place during the processing.

Duration of storage of personal data:

- If the investigation reveals that the report is unfounded or that no further action is necessary, the data relating to the report must be deleted within 60 days of the end of the investigation.
- If action is taken based on the investigation, – including taking legal action or disciplinary action against the whistleblower – the data relating to the report may be

processed within the framework of the reporting system until the final conclusion of the proceedings initiated on the basis of the report at the latest.

Protection of personal data within the organisation: no person other than those entitled to do so may know the identity of the person disclosing his or her identity, the person who may have substantial information about the facts contained in the report and the personal data of the person concerned by the report. The persons investigating the notification may, pending the conclusion of the investigation or the initiation of formal charges as a result of the investigation, share information - in addition to informing the person concerned by the report - on the content of the notification and on the person concerned with other departments or staff of the employer to the extent strictly necessary for the conduct of the investigation. When responding to a data subject's request for information and access, the Data Controller shall not disclose to the applicant the identity of the whistleblower or of the person who may have access to the information contained in the report.

Rights and remedies of the data subject

The data subject may contact the Data Controller in order to enforce the following rights. The Data Controller shall, without undue delay and in any event within one month of receipt of the request, inform the data subject of the action taken on the request. If necessary, taking into account the complexity of the application and the number of requests, this deadline may be extended by a further two months. The Data Controller shall inform the data subject of the extension of the time limit within one month of receipt of the request, stating the reasons for the delay. If the data subject has made the request by electronic means, the information shall be provided by electronic means wherever possible, unless the data subject requests otherwise. In order to comply with requests, the Data Controller needs to be able to identify the data subject. The Data Controller is entitled to refuse to fulfil the data subject's request if it can prove that it is unable to identify the data subject.

Right to access

If the data subject so requests, the Data Controller shall, within one month of receipt of the request, provide feedback to the data subject on whether the processing of his or her personal data is ongoing and, where such processing is in progress, inform the data subject of the characteristics of the processing and provide him or her with a copy of the personal data which are the subject of the processing. The Data Controller can comply with the data subject's request if the Data Controller can identify the data subject in a credible manner. The Data Controller shall not disclose the personal data of the whistleblower and the witness to the person requesting access in the course of fulfilling requests for access and information.

Right to rectification

If the data subject so requests, the Data Controller shall correct inaccurate personal data relating to the data subject without undue delay from the date of receipt of the request. The data subject has the right to request that incomplete personal data – by means of, inter alia, a supplementary declaration – be completed. The Data Controller can only comply the data subject's request if the Data Controller can credibly identify the data subject.

Right to erasure

Upon the data subject's request, the Data Controller shall delete personal data concerning the data subject without undue delay where one of the following grounds applies:

- the personal data are no longer necessary for the purposes for which they were collected or otherwise processed;
- the data subject withdraws the consent on which the processing is based and there is no other legal basis for the processing;
- the data subject objects to the processing and there are no overriding legitimate grounds for the processing;
- the personal data have been unlawfully processed; or
- the personal data must be erased in order to comply with a legal obligation applicable to the Data Controller.

The Data Controller can only comply with the data subject's request if the Data Controller can credibly identify the data subject.

The Data Controller is not obliged to comply with a data subject's request for erasure where the processing of personal data is necessary for compliance with a legal obligation to which the Data Controller is subject or for the establishment, exercise or defence of legal claims.

Right to restriction of processing

At the request of the data subject, the Data Controller shall, within one month of receipt of the request, restrict the processing of personal data relating to the data subject where one of the following conditions is met

a) the data subject contests the accuracy of the personal data, in which case the restriction applies for the period of time necessary to allow the Data Controller to verify the accuracy of the personal data;
b) the processing is unlawful and the data subject opposes the erasure of the data and instead requests the restriction of their use;
c) the Data Controller no longer needs the personal data for the purposes of processing, but the data subject requires them for the establishment, exercise or defence of legal claims; or
d) the data subject has objected to the processing; in this case, the restriction applies for the period until it is established whether the legitimate grounds of the controller override those of the data subject.

The Data Controller can comply with the data subject's request if the Data Controller can identify the data subject in a credible manner. In case of restriction of processing, the personal data handled, with the exception of storage, may only be processed with the consent of the data

subject or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person. The Data Controller shall inform the data subject requesting the restriction in advance of the lifting of the restriction.

The right to protest

The data subject shall have the right to object at any time, on grounds relating to his or her particular situation, to the processing of his or her personal data based on the legitimate interests of the Data Controller. If the data subject so requests, the Data Controller shall examine whether the processing is justified by compelling legitimate grounds which override the interests, rights and freedoms of the data subject or are related to the establishment, exercise or defence of legal claims. If these grounds do not apply, the Data Controller may no longer process the personal data. The Data Controller shall inform the data subject of the outcome of the investigation within one month. The Data Controller can comply with the data subject's request if the Data Controller can identify the data subject in a credible manner.

Enforcement of rights, legal remedies

The data subject has the right to contact the Data Controller directly if he or she has a question about the processing of his or her personal data or wishes to exercise his or her data protection rights. The name and contact details of the Data Protection Officer are indicated at the beginning of this privacy notice.

If the data subject considers that the processing of personal data relating to him or her is unlawful, he or she has the right to lodge a complaint with the National Authority for Data Protection and Freedom of Information („Nemzeti Adatvédelmi és Információszabadság Hatóság"), (registered office: 1055 Budapest, Falk Miksa utca 9-11., postal address: 1363 Budapest, Pf.: 9., e-mail: ugyfelszolgalat@naih.hu, telephone number: +36 (30) 683-5969, +36 (30) 549-6838, +36 (1) 391 1400).

If you consider that your rights under the GDPR have been infringed as a result of the unlawful processing of your personal data, you have the right to bring a civil action against the Data Controller. You can also file a lawsuit in the court of the place where you live (https://birosag.hu/torvenyszekek).