



EST. 2014 · 52 COUNTRIES · 4 CONTINENTS · 5 WORLD
CHAMPIONSHIPS
The International Governing Body for the Sport of
Alpabut

DATA PROTECTION

...

POLICY

Federation-Level Data
Governance Regulation

VERSION 1 · EDITION 2026



OFFICIAL DOCUMENT

WAF Data Protection Policy

Federation-Level Data Governance Regulation

Document	WAF Data Protection Policy
Version	1.0
Edition	2026
Effective Date	19 May 2026
Adopted by	WAF Board of Directors at the meeting held on 19 May 2026 in Baku, pursuant to Board Resolution WAF-BOD-2026-001; subject to ratification by the General Assembly in December 2026.
Official Language	English
Registration	2014
Headquarters	AZ1010 Mikayil Rafili str. 32, Nasimi dist., Baku, Azerbaijan
Email	office@alpabut federation.org
Website	alpabut federation.org
Document ID	WAF-DPP-2026-001



© 2026 World Alpaut Federation · All rights reserved

This Policy is the binding internal data protection regulation of the World Alpaut Federation. It establishes federation-level data governance applicable to all WAF activities, member organisations, athletes, athlete support personnel, officials, and third-party processors. The Policy is aligned with the EU General Data Protection Regulation (GDPR) 2016/679 and shall be interpreted, where applicable national law provides higher protection, in accordance with that higher standard.



OPENING

Preamble

The World Alpaut Federation (WAF) recognises that the personal data of athletes, athlete support personnel, officials, and other natural persons under its jurisdiction is among the most sensitive assets entrusted to the Federation. The proper protection of this data is fundamental to the trust placed in WAF by its member organisations, by athletes, and by the broader sporting community.

This Policy establishes WAF's data governance framework and is aligned with the European Union General Data Protection Regulation 2016/679 (the "GDPR"), which represents the international gold standard for personal data protection. WAF operates as a multi-jurisdictional international federation, and accordingly this Policy shall apply as a baseline. Where applicable national law provides protection higher than this Policy, that higher national protection shall apply to data subjects to whom such law applies.

This Policy operates as the principal data governance regulation of the Federation. It is binding on all WAF officers, employees, volunteers, member organisations, accredited bodies, and third-party processors acting on behalf of WAF. Compliance with this Policy is a condition of participation in any WAF activity that involves the processing of personal data.

LEGAL FOUNDATION

GDPR baseline · Higher national protection prevails · Council of Europe Convention 108+ · WAF Statutes Article 26 · Linked to: Anti-Doping Code, Safeguarding Policy, Disciplinary Code, Licensing System, Coach Framework. This is a federation-level data governance regulation, not a website privacy notice.



REFERENCE

Definitions

For the purposes of this Policy, the following terms shall have the meanings set out below. Terms not defined here shall bear the meanings assigned to them in the GDPR or, where the term is specific to sport, in the WAF Statutes.

Personal Data	Any information relating to an identified or identifiable natural person (the data subject); an identifiable natural person is one who can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that person.
Special Category Data	Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data processed for the purpose of uniquely identifying a natural person, data concerning health, data concerning a natural person's sex life or sexual orientation. Anti-doping data, medical records, TUE applications, and safeguarding incident records constitute Special Category Data under this Policy.
Processing	Any operation or set of operations performed on personal data, whether or not by automated means, including collection, recording, organisation, structuring, storage, adaptation, retrieval, consultation, use, disclosure by transmission, dissemination, alignment, restriction, erasure, or destruction.
Controller	The natural or legal person which determines the purposes and means of the processing of personal data. WAF acts as Controller for personal data processed in connection with its core activities. Member organisations may act as separate Controllers in respect of their own activities.
Processor	A natural or legal person which processes personal data on behalf of the Controller. Laboratories, NADO partners, IT service providers, and competition organisers acting on WAF's instructions are Processors.
Joint Controllers	Two or more controllers that jointly determine the purposes and means of processing. WAF and a host member organisation may act as Joint Controllers in respect of an event held in that member's territory.



Data Subject	An identified or identifiable natural person to whom personal data relates; under this Policy, data subjects include athletes, athlete support personnel, referees, officials, member-organisation representatives, employees, volunteers, parents and guardians of minor athletes, and complainants and witnesses in safeguarding or disciplinary matters.
Consent	Any freely given, specific, informed, and unambiguous indication of the data subject's wishes by which they, by a statement or by a clear affirmative action, signify agreement to the processing of personal data relating to them.
Data Protection Officer (DPO)	The officer designated by WAF in accordance with Article 7 of this Policy to oversee data protection compliance and to act as the contact point for data subjects and supervisory authorities.
Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed.
Pseudonymisation	The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure non-attribution.
Standard Contractual Clauses (SCCs)	Model contractual clauses approved by the European Commission for the transfer of personal data to processors or controllers in third countries.
Adequacy Decision	A decision by the European Commission, the Council of Europe, or another competent authority that a third country provides an adequate level of protection for personal data.
Binding Corporate Rules (BCR)	Internal rules adopted by a multinational organisation to allow intra-group transfers of personal data to entities located in third countries that do not provide an adequate level of protection.
Supervisory Authority	An independent public authority established by a Member State of the European Union or by a Council of Europe Convention 108+ Party for the supervision of the application of data protection law.

**Protected Person**

An athlete or other natural person who, at the time of processing, is under the age of 16, or under the age of 18 and not classified as elite under the WAF Anti-Doping Code Article 26.1, or for reasons other than age has been determined to lack legal capacity. The Protected Person category triggers heightened safeguards under this Policy.



PART I

General Provisions

Purpose, scope, application, and fundamental principles

**PART I****General Provisions**

Article 1 Purpose and Scope

- 1.1. The purpose of this Policy is to establish the federation-level framework governing the lawful, fair, and transparent processing of personal data within WAF, to safeguard the rights of data subjects, and to ensure compliance with applicable data protection law across the multi-jurisdictional reach of the Federation.
- 1.2. This Policy applies to all processing of personal data carried out:
 - (a) By WAF, its officers, employees, volunteers, and committees;
 - (b) By member organisations, in connection with WAF activities;
 - (c) By accredited bodies and third-party processors acting on behalf of WAF;
 - (d) In connection with WAF-sanctioned competitions, training, licensing, examinations, and disciplinary, anti-doping, or safeguarding proceedings;
 - (e) Through WAF's information systems, databases, and online platforms.
- 1.3. This Policy applies whether processing is carried out in or outside any particular jurisdiction, where the processing is carried out in connection with WAF's activities.

Article 2 Applicable Legal Regime

- 2.1. This Policy is grounded in the principles of the EU General Data Protection Regulation 2016/679 (GDPR), which is recognised as the baseline international standard for personal data protection. WAF adopts the GDPR principles as its operational standard regardless of whether GDPR has direct legal application to a particular processing activity.
- 2.2. Where the national law of any member organisation, the country of residence of a data subject, or the country of any processing activity provides protection higher than this Policy, that higher national protection shall apply to the data subject and processing concerned. WAF and its member organisations shall give effect to higher national protection without prejudice to the application of this Policy as a baseline.
- 2.3. Where a conflict arises between this Policy and a higher national protection law, the higher national protection law shall prevail. The DPO shall maintain a register of jurisdictional deviations from this Policy and shall make the register available to data subjects upon request.
- 2.4. Reference Frameworks — In addition to GDPR, this Policy takes into account: (a) Council of Europe Convention 108+ for the protection of individuals with regard to the processing of personal data; (b) the WADA International Standard for the Protection of Privacy and Personal Information (ISPPPI);



(c) the IOC Olympic Movement Medical Code; and (d) the UN Convention on the Rights of the Child in respect of Protected Persons.

Article 3 Fundamental Principles of Processing

3.1. All processing of personal data within WAF shall comply with the following principles:

- (a)** Lawfulness, fairness, and transparency — processing shall be lawful, fair, and transparent in relation to the data subject;
- (b)** Purpose limitation — personal data shall be collected for specified, explicit, and legitimate purposes and not further processed in a manner incompatible with those purposes;
- (c)** Data minimisation — personal data shall be adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed;
- (d)** Accuracy — personal data shall be accurate and, where necessary, kept up to date;
- (e)** Storage limitation — personal data shall be kept in a form which permits identification of data subjects for no longer than necessary for the purposes for which the data is processed (see Article 14);
- (f)** Integrity and confidentiality — personal data shall be processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical and organisational measures;
- (g)** Accountability — WAF shall be responsible for, and shall be able to demonstrate compliance with, the principles set out in this Article.

FOUNDATIONAL PRINCIPLES

Lawfulness · Fairness · Transparency · Purpose Limitation · Data Minimisation · Accuracy · Storage Limitation · Integrity and Confidentiality · Accountability. Every processing activity within WAF must be measurable against these seven principles.



PART II

Legal Basis & Data Classification

Lawful grounds for processing and the four data sensitivity levels

**PART II****Legal Basis and Data Classification**

Article 4 Legal Basis for Processing

4.1. Personal data shall not be processed by WAF unless one or more of the following lawful bases applies:

- (a)** Consent — the data subject has given consent to the processing for one or more specific purposes;
- (b)** Contract — processing is necessary for the performance of a contract to which the data subject is party (including the WAF licence agreement, athlete entry, and member organisation affiliation), or for the taking of steps at the request of the data subject prior to entering into such a contract;
- (c)** Legal obligation — processing is necessary for compliance with a legal obligation to which WAF is subject;
- (d)** Vital interests — processing is necessary to protect the vital interests of the data subject or another natural person, including in connection with medical emergencies and safeguarding;
- (e)** Legitimate interests — processing is necessary for the legitimate interests pursued by WAF or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject, in particular where the data subject is a Protected Person.

4.2. Necessity for International Sporting Administration — In addition to the bases set out in Article 4.1, WAF recognises a specific operational legal basis grounded in the necessity of international sporting administration. This basis applies to processing that is necessary for: (a) the management of competition entries, results, and rankings; (b) anti-doping testing, results management, and TUE adjudication; (c) safeguarding obligations under the WAF Safeguarding Policy; (d) the licensing of athletes, coaches, and referees; (e) the verification of identity, eligibility, and qualifications; and (f) the discharge of WAF's regulatory responsibilities under its Statutes. This operational basis shall be construed as falling within the legitimate interests basis under Article 4.1(e), with the necessity test satisfied by the fact that the activity is integral to the conduct of international sport.

Article 5 Legal Basis for Special Category Data

5.1. Special Category Data shall not be processed unless one or more of the following additional bases applies, in addition to a general lawful basis under Article 4:

- (a)** Explicit consent of the data subject for one or more specified purposes;
- (b)** Processing is necessary for the protection of vital interests where the data subject is physically or legally incapable of giving consent;
- (c)** Processing is necessary for the establishment, exercise, or defence of legal claims, including disciplinary and arbitration proceedings;



- (d) Processing is necessary for reasons of substantial public interest in connection with the integrity of sport, anti-doping, and safeguarding, on the basis of WAF's Statutes and regulatory framework;
- (e) Processing is necessary for the purposes of preventive or occupational medicine, medical diagnosis, or the provision of health care under the responsibility of a qualified medical professional bound by a duty of confidentiality.

5.2. Legal Basis Matrix — The DPO shall maintain a Legal Basis Matrix mapping each significant category of WAF processing activity to its operational lawful basis, the additional Special Category basis where applicable, and any necessary safeguards. The Matrix shall be updated annually and shall be available to data subjects upon request.

LEGAL BASIS MATRIX — INDICATIVE MAPPING

Athlete licensing → Contract · Anti-doping testing → Substantial public interest + Article 4.2 (international sporting administration) · TUE applications → Explicit consent + medical processing · Safeguarding records → Vital interests + substantial public interest · Whereabouts data → Article 4.2 (international sporting administration) + WADA ISPPPI · Disciplinary records → Establishment of legal claims + WAF Statutes · Medical emergencies → Vital interests.

Article 6 Data Classification Levels

6.1. WAF classifies all personal data processed within its systems into one of the following four levels of sensitivity, each carrying distinct security, access, and retention obligations:

Level	Category	Examples	Key Safeguards
L1	Public	Athlete name and nationality (with consent), competition results, public licence verification	Standard publication safeguards; Protected Persons excluded
L2	Internal	Member-organisation contact details, internal correspondence, training records	Role-based access; encrypted at rest
L3	Confidential	Athlete contact details, address, date of birth, licence applications, financial records	Restricted access; encryption in transit and at rest; audit logging
L4	Sensitive / Special Category	Medical records, TUE files, anti-doping records, safeguarding incidents, biometric data, criminal background data	Highest restriction; explicit consent or substantial public interest basis; separate storage; minimum-necessary access; mandatory DPO oversight



- 6.2.** Each WAF system, file, register, or processing activity shall be classified under one of the levels in Article 6.1. The DPO shall maintain the WAF Data Classification Register and shall ensure that classifications are reviewed annually.
- 6.3.** Where data of different classification levels is combined in a single record (for example, an athlete profile containing both contact data and medical data), the highest applicable classification shall apply to the record as a whole.
- 6.4.** Access to personal data shall be limited to those officers, employees, volunteers, and processors who have a documented need to access the data for the discharge of their functions, in accordance with the role-based access matrix maintained by the DPO under Article 8.



PART III

Governance & DPO

Data Protection Officer, role-based access, and accountability framework



PART III

Governance and the Data Protection Officer

Article 7 The Data Protection Officer (DPO)

- 7.1.** WAF shall designate a Data Protection Officer (DPO) responsible for overseeing compliance with this Policy and applicable data protection law.
- 7.2.** Strategic Designation — The DPO shall, at the strategic stage, be a person with established expertise in data protection law and practice, who shall be appointed by the Board of Directors for a renewable term of four (4) years and who shall not concurrently hold any operational line-management role within WAF that could compromise their independence.
- 7.3.** Transitional Designation — Until the strategic DPO designation under Article 7.2 takes effect, and for a period not exceeding twenty-four (24) months from the entry into force of this Policy, the WAF Safeguarding Officer shall act as interim DPO. The interim arrangement shall not diminish the independence obligations applicable to the DPO function under this Policy or under applicable law. The interim DPO shall, where necessary, retain external legal expertise to support the discharge of the DPO function in matters requiring specialist data protection competence.
- 7.4.** Independence — The DPO, whether strategic or interim, shall act independently in the discharge of the function. No officer or organ of the Federation shall instruct the DPO as to the substantive performance of the DPO's tasks, nor penalise the DPO for the proper performance of those tasks. The DPO shall report directly to the Board of Directors and may report directly to the General Assembly in matters of fundamental data protection concern.
- 7.5.** Tasks of the DPO — The DPO shall, at minimum:
- (a)** Inform and advise WAF and its officers of their obligations under this Policy and applicable data protection law;
 - (b)** Monitor compliance with this Policy, including the assignment of responsibilities, awareness-raising, training of staff, and related audits;
 - (c)** Provide advice on Data Protection Impact Assessments (DPIAs) under Article 12 and monitor their performance;
 - (d)** Maintain the WAF Data Classification Register, the Legal Basis Matrix, the Record of Processing Activities, the Retention Schedule, the Cross-Border Transfer Register, and the Breach Register;
 - (e)** Cooperate with supervisory authorities and act as the contact point for them on issues relating to processing;
 - (f)** Act as the contact point for data subjects in matters relating to the exercise of their rights under Part V;
 - (g)** Investigate and respond to data protection complaints from data subjects;



- (h) Report annually to the Board of Directors and to the General Assembly on the state of data protection within WAF.

7.6. Removal — The DPO may be removed from office only for cause, by reasoned written decision of the Board of Directors, and only after the DPO has been afforded a reasonable opportunity to respond to the grounds of removal. A removal decision shall be reported to the General Assembly at its next ordinary session.

7.7. Contact — The contact details of the DPO shall be published on the WAF official website (dpo@alpagutfederation.org) and shall be included in all data subject communications under Articles 16 and 17.

Article 8 Records of Processing and Role-Based Access

8.1. The DPO shall maintain, on behalf of WAF, a Record of Processing Activities (ROPA) that identifies, for each significant processing activity:

- (a) The name and purpose of the processing;
- (b) The categories of data subjects and personal data;
- (c) The data classification level under Article 6;
- (d) The lawful basis under Article 4 and, where applicable, Article 5;
- (e) The recipients to whom personal data is disclosed;
- (f) Where applicable, transfers to third countries and the safeguards in place under Article 13;
- (g) The retention period under Article 15;
- (h) The technical and organisational security measures under Article 11.

8.2. Role-Based Access Matrix — Access to personal data within WAF systems shall be controlled by a documented role-based access matrix maintained by the DPO. The matrix shall identify, for each role, the categories of data the role-holder is authorised to access and the purposes for which access is permitted. Access outside the matrix shall be granted only with the documented written authorisation of the DPO.

8.3. Training — All WAF officers, employees, volunteers, and member-organisation representatives who process personal data on behalf of WAF shall complete data protection training upon assuming their function and on a refresh cycle of no more than two (2) years.

Article 9 Data Protection Impact Assessment (DPIA)

9.1. Where a type of processing, in particular using new technologies, and taking into account the nature, scope, context, and purposes of the processing, is likely to result in a high risk to the rights and



freedoms of natural persons, WAF shall, prior to commencing the processing, carry out a Data Protection Impact Assessment.

9.2. A DPIA shall, in particular, be carried out in the case of:

- (a)** Systematic and extensive evaluation of athletes based on automated processing, including profiling for selection, ranking, or anti-doping risk assessment;
- (b)** Processing of Special Category Data on a large scale, including the establishment of an athlete medical or anti-doping database;
- (c)** Systematic monitoring of athletes, including whereabouts monitoring under the Anti-Doping Code;
- (d)** Processing involving Protected Persons on a significant scale;
- (e)** The introduction of new technologies, including biometric or AI-based systems.

9.3. The DPIA shall contain, at minimum: (a) a systematic description of the processing operations and the purposes; (b) an assessment of the necessity and proportionality of the operations; (c) an assessment of the risks to the rights and freedoms of data subjects; and (d) the measures envisaged to address the risks.



PART IV

Security & Risk Management

Technical and organisational measures, breach response, and special-category safeguards



PART IV

Security and Risk Management

Article 10 Technical and Organisational Measures

10.1. WAF shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk presented by the processing, including the risk of accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

10.2. Technical Measures — At minimum, WAF shall implement:

- (a) Encryption of Special Category Data in transit and at rest;
- (b) Pseudonymisation where the purpose of the processing can be achieved with pseudonymised data;
- (c) Multi-factor authentication for access to systems containing Confidential or Sensitive data;
- (d) Audit logging of all access to Sensitive data, with logs retained for the period set in the Retention Schedule;
- (e) Backup and disaster recovery procedures with documented Recovery Time Objectives;
- (f) Network segregation between systems holding data of different classification levels.

10.3. Organisational Measures — At minimum, WAF shall implement:

- (a) Documented information security policies, reviewed annually;
- (b) Confidentiality undertakings signed by all officers, employees, and volunteers with access to personal data;
- (c) Vendor due diligence and written processor agreements (Article 11);
- (d) Incident response procedures and a documented Breach Protocol (Article 15);
- (e) Periodic data protection audits, no less frequently than every two (2) years;
- (f) Clean-desk and secure-disposal procedures for physical records.

Article 11 Processors and Sub-Processors

11.1. Where WAF engages a Processor to process personal data on its behalf, the engagement shall be governed by a written processor agreement that meets the requirements of GDPR Article 28.

11.2. The processor agreement shall, at minimum, set out: (a) the subject matter and duration of the processing; (b) the nature and purpose of the processing; (c) the type of personal data and categories of data subjects; (d) the obligations and rights of WAF as Controller; (e) the obligation of the Processor to process the data only on documented instructions from WAF; (f) confidentiality obligations of personnel; (g) security obligations consistent with Article 10; (h) the obligation to assist WAF in responding to data subject requests; (i) the obligation to assist WAF with breach



notification; (j) the obligation to delete or return data at the end of the engagement; (k) the right of WAF to audit; and (l) restrictions on the engagement of sub-processors.

11.3. Sub-processors may be engaged by a Processor only with the prior written authorisation of WAF and on substantially the same data protection terms as those agreed between WAF and the Processor.

11.4. Specific Processors — The processor obligations of this Article apply, without limitation, to: (a) WADA-accredited and WADA-approved laboratories under WAF Anti-Doping Code Article 10.7; (b) NADO partners under WAF Anti-Doping Code Article 10.6; (c) IT and cloud-service providers; (d) competition organisers and ticketing operators; and (e) external auditors and legal advisors processing personal data.

Article 12 Privacy by Design and by Default

12.1. WAF shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures designed to implement data protection principles in an effective manner and to integrate the necessary safeguards into the processing.

12.2. WAF shall implement appropriate technical and organisational measures to ensure that, by default, only personal data which is necessary for each specific purpose of the processing is processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage, and their accessibility.

Article 13 Public Registers and Minimum-Data Publication

13.1. WAF Public Registers — Where WAF maintains a public register (including the Licensing Register under the WAF Licensing System Article 3 and the Ineligibility Register under the WAF Anti-Doping Code Article 34.3), the data published shall be limited to the minimum necessary for the purpose of the register.

13.2. Minimum-Data Principle for Adults — Public registers concerning adult athletes, coaches, and referees shall publish, at maximum: full name; nationality; licence or grade level; year of award; current status (active, suspended, expired). No address, contact details, date of birth, medical data, or other Confidential or Sensitive data shall be published. This Article is without prejudice to the public Verify page, the content of which is governed by the WAF AID and Verification Specification, Articles 14 to 16.

13.3. Heightened Protection for Protected Persons — Where the public register concerns a Protected Person, the published data shall be limited to: initials and country of affiliation; licence or grade level; current status. The Protected Person's full name shall not be published in any open-access register without the explicit written consent of the Protected Person and their parent or guardian, given separately for the purpose of publication.



13.4. Verification API — WAF shall provide a verification interface enabling authorised third parties (such as competition organisers, member organisations, and other Code Signatories) to verify whether a specific person holds a current and valid WAF licence or grade, without exposing the underlying personal data file.



P A R T V

Data Subject Rights

Information, access, rectification, erasure, restriction, portability, and objection



PART V

Data Subject Rights

Article 14 Rights of the Data Subject

14.1. Data subjects whose personal data is processed by WAF shall have the following rights, exercisable by written request to the DPO:

- (a) Right to be informed (Articles 16–17);
- (b) Right of access — to obtain confirmation of whether their personal data is being processed and to obtain a copy of that data;
- (c) Right to rectification — to have inaccurate personal data corrected and incomplete data completed;
- (d) Right to erasure ("right to be forgotten") — subject to the limitations in Article 14.3;
- (e) Right to restriction of processing — in defined circumstances;
- (f) Right to data portability — to receive personal data in a structured, commonly used, and machine-readable format and to transmit it to another controller;
- (g) Right to object — to processing based on legitimate interests, including the operational basis under Article 4.2;
- (h) Right not to be subject to a decision based solely on automated processing, including profiling, that produces legal effects or significantly affects the data subject;
- (i) Right to withdraw consent — where processing is based on consent, the data subject may withdraw consent at any time, without affecting the lawfulness of processing carried out before withdrawal;
- (j) Right to lodge a complaint with a competent supervisory authority.

14.2. Response Timelines — WAF shall respond to a data subject request without undue delay and in any event within one (1) month of receipt of the request. Where the request is complex or where multiple requests have been received, this period may be extended by a further two (2) months, with notice to the data subject of the extension and the reasons within the original one-month period.

14.3. Limitations on Erasure — The right to erasure shall not apply to the extent that processing is necessary for: (a) compliance with a legal obligation; (b) the establishment, exercise, or defence of legal claims, including disciplinary, anti-doping, and safeguarding proceedings; (c) reasons of substantial public interest in the integrity of sport; or (d) archiving in the public interest. Anti-doping records, safeguarding files, and disciplinary records may be retained, in accordance with Article 15, despite an erasure request, where retention is justified under this Article.



14.4. Identification — Before fulfilling a request, the DPO may require the data subject to provide reasonable proof of identity. Where the request is made on behalf of a Protected Person by a parent or guardian, the DPO may require proof of parental responsibility.

14.5. No Charge — Requests under this Article shall be handled free of charge, save where requests are manifestly unfounded or excessive (in particular due to repetition), in which case WAF may either charge a reasonable fee taking into account administrative costs or refuse to act on the request, with reasons given.

Article 15 Retention Schedule

15.1. Personal data shall be retained for no longer than is necessary for the purposes for which it is processed, in accordance with the WAF Retention Schedule set out below. The DPO shall maintain and update the Retention Schedule annually, in consultation with the Anti-Doping Committee, the Safeguarding Officer, the Disciplinary Committee, and the Examination Commission.

Category	Retention Period	Rationale
Athlete licence records	Duration of licence + 5 years	Verification of past competition eligibility
Coach and referee records	Duration of licence + 5 years	Verification of qualifications
Competition results	Permanent (anonymised after 30 years)	Sport heritage and historical record
Anti-doping records (general)	10 years from violation date	WADA Code Article 17 alignment
Anti-doping — Whereabouts data	18 months from generation	WADA ISPPPI guidance
TUE files	Duration + 10 years	Anti-doping evidentiary alignment
Disciplinary records — minor	5 years from final decision	WAF Disciplinary Code Article 20
Disciplinary records — serious	Permanent	Public protection and ineligibility tracking
Safeguarding incident files	Until victim reaches age 25 + 7 years; minimum 30 years for serious cases	Child-protection best practice
Medical records (general)	Duration of licence + 10 years	Sports-medicine and liability standard
Minor athlete records	Until adulthood (18) + 10 years; longer if linked to safeguarding	UN CRC alignment
Whistleblower reports	10 years from closure of related case	Investigation evidentiary chain
Financial / membership data	10 years from termination	Audit and statutory accounting



Category	Retention Period	Rationale
Employment records	7 years from termination	Employment-law standard
Data breach records	Permanent	Regulatory reporting obligation
Marketing / consent-based data	Until consent withdrawal or 3 years of inactivity	Consent principle

15.2. Where personal data is to be retained beyond the retention period for archiving, statistical, or historical purposes, it shall be pseudonymised or anonymised wherever possible.

15.3. On expiry of the retention period, personal data shall be securely destroyed or permanently anonymised in accordance with the WAF Secure Disposal Procedure maintained by the DPO.



PART VI

Transparency & Communication

Privacy notices, data subject communications, and exercising of rights



PART VI

Transparency and Communication

Article 16 Privacy Notices

16.1. Where personal data is collected from the data subject, WAF shall, at the time of collection, provide the data subject with the following information:

- (a) The identity and contact details of WAF as Controller and the contact details of the DPO;
- (b) The purposes of the processing and the legal basis under Article 4 (and, where applicable, Article 5);
- (c) The categories of personal data concerned;
- (d) The recipients or categories of recipients of the personal data;
- (e) Where applicable, the fact that WAF intends to transfer personal data to a third country and the safeguards in place under Article 18;
- (f) The retention period under Article 15;
- (g) The data subject's rights under Article 14;
- (h) The right to lodge a complaint with a supervisory authority;
- (i) Whether the provision of personal data is a statutory or contractual requirement and the consequences of failure to provide the data.

16.2. Where personal data is not collected from the data subject, the same information shall be provided within a reasonable period after obtaining the data, and at the latest within one (1) month, unless an exception under GDPR Article 14(5) applies.

16.3. Privacy notices shall be drafted in clear and plain language, free of legal jargon, and shall be available in English. WAF shall make reasonable efforts to provide privacy notices in the languages of its principal member organisations.

16.4. Privacy Notices for Protected Persons shall be drafted in age-appropriate language, accompanied by parallel notice to the parent or guardian, and shall include explanation of the parent or guardian's right to exercise the data subject's rights on the Protected Person's behalf where applicable.

Article 17 Communication with Data Subjects

17.1. All communications with data subjects under this Policy shall be in writing, in clear and plain language, and shall be retained for the period set in the Retention Schedule.

17.2. WAF shall maintain a designated email address (privacy@alpagutfederation.org) for the receipt of data subject requests, complaints, and queries. The DPO shall acknowledge receipt of any such communication within five (5) working days.





P A R T V I I

International Transfers

Cross-border data flows, transfer mechanisms, and safeguards



PART VII

International Transfers

Article 18 Cross-Border Transfers

- 18.1.** WAF operates in 52 member countries, and the conduct of international sport necessarily involves cross-border transfers of personal data, including for the purposes of competition entry, anti-doping testing, safeguarding, licensing, and disciplinary proceedings.
- 18.2.** Permitted Transfer Mechanisms — Personal data shall be transferred outside the country of origin only where one of the following mechanisms applies:
- (a) Adequacy Decision — the destination country has been recognised by the European Commission, the Council of Europe, or another competent authority as providing an adequate level of protection;
 - (b) Standard Contractual Clauses (SCCs) — the transfer is governed by the European Commission's Standard Contractual Clauses, executed in writing between WAF and the recipient;
 - (c) Binding Corporate Rules (BCR) — for transfers within the WAF group of member organisations, internal binding rules adopted under Article 19;
 - (d) Necessity for International Sporting Administration — where the transfer is necessary for the conduct of international sport (in particular for competition entry, anti-doping testing, safeguarding, licensing, results processing, and disciplinary proceedings), supported by Article 4.2 of this Policy and recognised under GDPR Article 49(1)(d) (transfer necessary for important reasons of public interest);
 - (e) Explicit Consent — the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers in the absence of an adequacy decision and appropriate safeguards;
 - (f) Vital Interests — the transfer is necessary to protect the vital interests of the data subject or another natural person.
- 18.3.** Cross-Border Transfer Register — The DPO shall maintain a register of all systematic cross-border transfers of personal data, identifying for each: the categories of data, the recipients, the destination country, the transfer mechanism relied upon, and the safeguards in place.
- 18.4.** Special Considerations for Sensitive Data — Cross-border transfers of Special Category Data shall be subject to enhanced safeguards, including: (a) explicit prior consent of the data subject, save where another lawful basis under Article 5 applies; (b) encryption in transit and at rest; (c) restriction of access to the recipient's authorised personnel; (d) prohibition on onward transfer without WAF's authorisation; and (e) audit rights for WAF.



Article 19 Binding Internal Rules — Member Organisations

- 19.1.** WAF shall, within thirty-six (36) months of the entry into force of this Policy, adopt a set of Binding Internal Data Protection Rules (BIDPR) to govern intra-federation transfers of personal data between WAF and its member organisations and between member organisations themselves.
- 19.2.** Until the BIDPR is adopted, transfers between WAF and member organisations shall be governed by individual data sharing agreements based on Standard Contractual Clauses, executed in writing.
- 19.3.** The BIDPR shall, at minimum: (a) bind all member organisations to the principles of this Policy; (b) confer on data subjects enforceable rights against WAF and member organisations; (c) provide for mutual cooperation in responding to data subject requests; (d) establish a coordinated breach response under Article 20; and (e) provide for periodic audit and compliance review.



PART VIII

Data Breach Protocol

Detection, escalation, notification, and remediation of personal data breaches



PART VIII

Data Breach Protocol

Article 20 Breach Detection and Escalation

- 20.1.** All WAF officers, employees, volunteers, and processors are required to report any suspected or actual personal data breach to the DPO without undue delay, and in any event within twenty-four (24) hours of becoming aware of the breach.
- 20.2.** Reports shall be submitted to the DPO at dpo@alpagutfederation.org or through the dedicated breach-reporting channel published on the WAF website. Anonymous reports shall be accepted.
- 20.3.** Upon receipt of a report, the DPO shall:
- (a) Acknowledge the report within one (1) working day;
 - (b) Convene a Breach Response Team consisting of the DPO, the Legal Officer, the relevant operational head, and (where the breach involves Sensitive data) the Safeguarding Officer or Anti-Doping Committee Chair as appropriate;
 - (c) Conduct a preliminary assessment of the nature, scope, and severity of the breach;
 - (d) Initiate containment and remediation measures;
 - (e) Determine the notification obligations under Articles 21 and 22.

Article 21 Notification to Supervisory Authorities

- 21.1.** Where a personal data breach is likely to result in a risk to the rights and freedoms of natural persons, WAF shall notify the competent supervisory authority without undue delay and, where feasible, not later than seventy-two (72) hours after having become aware of the breach. Where the notification is not made within seventy-two (72) hours, it shall be accompanied by reasons for the delay.
- 21.2.** The notification shall, at minimum:
- (a) Describe the nature of the breach including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
 - (b) Communicate the name and contact details of the DPO;
 - (c) Describe the likely consequences of the breach;
 - (d) Describe the measures taken or proposed to be taken to address the breach, including, where appropriate, measures to mitigate its possible adverse effects.
- 21.3.** Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without further undue delay.



Article 22 Notification to Data Subjects

- 22.1.** When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, WAF shall communicate the breach to the data subject without undue delay.
- 22.2.** The communication to the data subject shall describe in clear and plain language the nature of the personal data breach and contain at least: (a) the name and contact details of the DPO; (b) the likely consequences of the breach; and (c) the measures taken or proposed to be taken to address the breach, including measures to mitigate its possible adverse effects.
- 22.3.** Communication to data subjects shall not be required where: (a) WAF has implemented appropriate technical and organisational protection measures (such as encryption) that render the data unintelligible to any person not authorised to access it; (b) WAF has taken subsequent measures that ensure that the high risk is no longer likely to materialise; or (c) it would involve disproportionate effort, in which case there shall instead be a public communication or similar measure.
- 22.4.** Communications concerning Protected Persons shall be made to the parent or guardian of the Protected Person, in addition to the Protected Person where age-appropriate.

Article 23 Breach Register and Lessons Learned

- 23.1.** The DPO shall maintain a Breach Register documenting all personal data breaches, regardless of whether they were notifiable. The Register shall record, for each breach: (a) the facts relating to the breach; (b) its effects; (c) the remedial action taken; (d) lessons learned; and (e) any changes to systems or procedures arising from the breach.
- 23.2.** The DPO shall report annually to the Board of Directors on the number, nature, and outcome of breaches recorded in the Register, with anonymisation as necessary to preserve confidentiality of ongoing matters.

72 - HOUR RULE

From the moment WAF becomes aware of a personal data breach likely to result in a risk to data subjects, the clock starts. Within 72 hours: notify the supervisory authority. If high risk: also notify affected data subjects without undue delay. Internal escalation must reach the DPO within 24 hours. Failure to comply may itself constitute a separate violation.



PART IX

Protected Persons & Children

Heightened safeguards for Minors and Protected Persons in data processing



PART IX

Protected Persons and Children

Article 24 Heightened Protection for Protected Persons

- 24.1.** Personal data of Protected Persons (as defined in this Policy and in the WAF Anti-Doping Code Article 26.1, and including all Minors) shall be subject to the heightened safeguards established in this Part, in addition to the general protections of this Policy.
- 24.2.** Lawful Basis — Processing of personal data of a Protected Person on the basis of consent shall require the consent of the parent or guardian, in addition to the assent of the Protected Person where the Protected Person is of sufficient age and maturity to express a view. For Protected Persons aged sixteen (16) and above, the consent of the Protected Person may be sufficient where applicable national law so permits.
- 24.3.** Data Minimisation — The principle of data minimisation shall be applied with particular rigour in the case of Protected Persons. Information collected from or about a Protected Person shall be limited to the strict minimum necessary for the purpose.
- 24.4.** Public Disclosure — As provided in Article 13.3, the full name of a Protected Person shall not appear in any open-access WAF register without the explicit written consent of the parent or guardian, given specifically for that purpose.
- 24.5.** Profiling, Automated Decisions, and Emerging Technologies — Solely automated decision-making, including profiling, that produces legal or similarly significant effects shall not be applied to Protected Persons. Where any of the following technologies is contemplated for use in connection with WAF activities involving Protected Persons or any other data subjects, the use shall be preceded by a Data Protection Impact Assessment under Article 9 and shall comply with the Human Review Supremacy principle in Article 24.6: (a) facial recognition or other biometric identification systems; (b) biometric attendance, registration, or accreditation systems; (c) AI-assisted or algorithmic scoring, judging, or ranking of athletes; (d) AI-assisted or algorithmic anti-doping risk profiling; (e) automated talent identification or selection systems; (f) any other system that involves the systematic profiling, categorisation, or evaluation of natural persons.
- 24.6.** Human Review Supremacy — No fully automated decision involving the rights or interests of any data subject under WAF jurisdiction — and in particular no decision concerning eligibility, selection, sanction, ranking, licensing, or grading — shall produce legal or similarly significant effects without meaningful human review by an appropriately qualified WAF officer. Algorithmic and AI-assisted tools may inform, support, or recommend decisions, but the operative decision shall always rest with a natural person who has examined the matter and is accountable for the outcome. The data subject shall have the right to contest the decision, to obtain human intervention, and to express their point of view, in addition to the rights established in Article 14.



24.7. Marketing — Personal data of Protected Persons shall not be used for direct marketing purposes.

Article 25 Safeguarding-Linked Processing

- 25.1.** Personal data processed in connection with the WAF Safeguarding Policy is classified as Sensitive (L4) under Article 6 of this Policy and shall be processed in strict accordance with both this Policy and the Safeguarding Policy.
- 25.2.** Where the requirements of this Policy and the Safeguarding Policy diverge in respect of safeguarding records, the requirements providing higher protection for the welfare of the Protected Person shall prevail. In particular, retention of safeguarding records may exceed the periods set out in Article 15 where the welfare of the Protected Person so requires.
- 25.3.** Disclosure of safeguarding records to law enforcement or child protection authorities, where required for the welfare of the Protected Person, shall be made notwithstanding any restriction in this Policy.

HEIGHTENED SAFEGUARDS FOR PROTECTED PERSONS

Parental consent · Strict data minimisation · No public-name disclosure without specific written consent · No profiling for legal effects · No marketing · Safeguarding-record protection prevails · Communication to parents in plain age-appropriate language.



P A R T X

Final Provisions

Compliance, audit, training, amendments, and entry into force

**PART X****Final Provisions**

Article 26 Compliance and Audit

- 26.1.** WAF shall demonstrate compliance with this Policy through the maintenance of the records required by Articles 8, 15, 18, and 23, and through the periodic audit referred to in Article 10.3(e).
- 26.2.** The DPO shall report annually to the Board of Directors on the state of data protection compliance within WAF, including: (a) processing activities reviewed; (b) DPIAs conducted; (c) data subject requests received and handled; (d) breaches recorded; (e) cross-border transfers; and (f) recommendations for improvement.
- 26.3.** Significant non-compliance with this Policy by a WAF officer, employee, or volunteer may constitute a disciplinary offence under the WAF Disciplinary Code.

Article 27 Relationship to Other WAF Documents

- 27.1.** This Policy operates as the federation-level data governance regulation of WAF. It is binding on all WAF activities involving personal data and shall be read in conjunction with: (a) the WAF Statutes; (b) the WAF Anti-Doping Code; (c) the WAF Safeguarding Policy; (d) the WAF Disciplinary Code; (e) the WAF Licensing System; and (f) the WAF Coach Framework.
- 27.2.** In the event of any conflict between this Policy and the WAF Statutes, the Statutes shall prevail. In the event of any conflict between this Policy and any other WAF regulatory document, this Policy shall prevail in respect of data protection matters, save where the other document provides higher protection for the data subject, in which case the higher protection shall apply.
- 27.3.** This Policy does not displace the specialised confidentiality, retention, and disclosure provisions of the WAF Anti-Doping Code, the WAF Safeguarding Policy, or the WAF Disciplinary Code; rather, this Policy provides the general framework within which those specialised provisions operate.

Article 28 Amendments

- 28.1.** This Policy may be amended upon recommendation of the DPO and the Board of Directors and approval of the General Assembly, in accordance with the Statutes. Amendments to bring this Policy into alignment with developments in applicable data protection law may be adopted by the Board of Directors on the recommendation of the DPO, with subsequent ratification by the General Assembly.
- 28.2.** Proposed amendments shall be circulated to all member organisations no less than sixty (60) days before adoption, save in cases where urgent amendment is required to address a material risk to data subjects.



Article 29 Transitional Provisions

29.1. Phased Implementation — Recognising the operational reality of WAF at the date of adoption of this Policy, the following provisions shall enter into operational force on a phased basis:

- (a) Articles 1–6 and Articles 14–17 (general principles, classification, and data subject rights) shall enter into force on the effective date of this Policy;
- (b) Article 7 (DPO) shall enter into force immediately, with the interim arrangement under Article 7.3 applying for up to twenty-four (24) months;
- (c) Article 8 (Records of Processing and Role-Based Access) shall be implemented progressively, with full implementation no later than twelve (12) months after the entry into force of this Policy;
- (d) Article 9 (DPIA) shall be applied to all new processing activities from the effective date and to existing processing activities of high-risk nature within twelve (12) months;
- (e) Article 10 (Technical and Organisational Measures) shall be implemented progressively, with the minimum technical safeguards under Article 10.2 in place no later than eighteen (18) months;
- (f) Article 19 (Binding Internal Rules) shall be adopted within thirty-six (36) months as provided in Article 19.1;
- (g) Articles 20–23 (Breach Protocol) shall enter into force on the effective date of this Policy.

29.2. The DPO shall report to the Board of Directors quarterly on the progress of phased implementation.

Article 30 Entry into Force

30.1. This Policy shall enter into force on the date of its adoption by the WAF Board of Directors at the meeting held on 19 May 2026 in Baku, pursuant to Board Resolution WAF-BOD-2026-001; subject to ratification by the General Assembly in December 2026, with subsequent ratification by the General Assembly at its next ordinary session.

30.2. All WAF officers, employees, volunteers, member organisations, and processors shall, within ninety (90) days of the entry into force of this Policy, sign an acknowledgment of acceptance of this Policy.

**OFFICIAL**

Adoption & Signatures

This WAF Data Protection Policy has been adopted by the WAF Board of Directors at the meeting held on 19 May 2026 in Baku, pursuant to Board Resolution WAF-BOD-2026-001; subject to ratification by the General Assembly in December 2026, in accordance with the WAF Statutes, Article 26. By signature below, the undersigned officers confirm the adoption of this Policy on behalf of the Federation, and affirm WAF's commitment to the highest international standards of personal data protection.

Adopted by	WAF Board of Directors, with subsequent ratification by the General Assembly
Date of Adoption	19 May 2026
Version	1.0
Effective Date	19 May 2026
Official Language	English (authoritative text)

SIGNATURES

Authorised Signatories

Vasif Namazov

Chairman of the Board

Signature

Date

**EMIL RAHIMOV****Interim President — BAŞAD**

World Alpaut Federation

Signature

Date

DATA PROTECTION OFFICER*To be appointed at the General Assembly, December 2026*

Signature

Date



WORLD ALPAGUT FEDERATION

The International Governing Body for the Sport of
Alpabut

AZ1010 Mikayil Rafili str. 32,
Nasimi dist., Baku, Azerbaijan

office@alpabut federation.org · alpabut federation.org

© 2026 World Alpabut Federation · All rights reserved

