WSF ANTI-DOPING PROGRAMME DATA PROTECTION POLICY

The purpose of the International Standard for the Protection of Privacy and Personal Information (ISPPPI) is to ensure that all relevant parties involved in anti-doping in sport adhere to a set of core privacy protections when collecting and using athlete personal information.

The World Squash Federation (WSF) adheres to the WADA International Standard for the Protection of Privacy and Personal Information (ISPPPI).

Personal information collected by the WSF through whereabouts filings, updates, doping control forms, TUEs and other filings is retained indefinitely, used only for legitimate anti-doping purposes and shared with other anti-doping organizations and/or national governing body (or bodies) or as required by law or contract.

Public disclosure of personal information will generally only come about when permitted or required by the World Anti-Doping Code, the rules of National Anti-Doping Agencies or as required by law, law enforcement, or other governmental or agency processes. Personal information may also be viewed in connection with third party audits of the WSF. The WSF does not control how other organisations handle information shared with them by the WSF, but will include a statement requesting that such information be handled consistently with the WSF Data Protection Policy and/or the WADA ISPPI.

If an athlete, the athlete's representative(s), or others associated with the athlete make(s) public comments about any process involving the athlete, including any case, the WSF may respond publicly to such comments and rely upon any personal information provided to the WSF in such response. Also, the WSF may at any time release aggregate statistics of testing, TUE applications and permits, whereabouts filings, results management processes, and adjudication results.

Complaints or inquiries regarding the way the WSF is handling or has handled personal information should be submitted to wsf@worldsquash.org within three months of when you first learn of the facts giving rise to your complaint or inquiry. Within 30 days of receipt of your written complaint or inquiry, the WSF will provide a response.

Context & Overview

Introduction

WSF needs to gather and use certain information about individuals and organisations with respect to Anti-Doping. This policy describes how this personal data must be collected, handled and stored to meet the WSF's data protection standards — and to comply with the law.

Why this policy exists

This data protection policy ensures the World Squash Federation (WSF):

- Complies with data protection law and follows good practice
- Protects the rights of staff, customers, individuals and partners
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

Data protection law

The General Data Protection Regulations (GDPR), which apply from 25 May 2018, describes how organisations — including WSF — must collect, handle and store personal information. These rules apply regardless of whether data is stored electronically, on paper or on other materials. To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The GDPR is underpinned by important principles, which say that personal data must:

1. Be processed fairly and lawfully
2. Be obtained only for specific, lawful purposes
3. Be adequate, relevant and not excessive
4. Be accurate and kept up to date
5. Not be held for any longer than necessary
6. Processed in accordance with the rights of data subjects
7. Be protected in appropriate ways
8. Not be transferred to any country or territory without ensuring an adequate level of protection

People, Risks & Responsibilities

Policy scope

This policy applies to:

- The head office of WSF
- All branches of WSF
- All staff and volunteers of WSF
- All contractors, suppliers and other people working on behalf of WSF

It applies to all data that the WSF holds relating to identifiable individuals, even if that information technically falls outside of the Data GDPR. This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- Whereabouts Information
- Test Results
- …plus any other information relating to individuals

Data protection risks

This policy helps to protect WSF from some very real data security risks, including:

- **Breaches of confidentiality.** For instance, information being given out inappropriately.
- **Failing to offer choice.** For instance, all individuals should be free to choose how the WSF uses data relating to them.
- **Reputational damage.** For instance, the WSF could suffer if hackers successfully gained access to sensitive data.

Responsibilities

Everyone who works for or with WSF has some responsibility for ensuring data is collected, stored and handled appropriately. Each team or individual that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, these groups/people have key areas of responsibility:

- The **Executive Board** is ultimately responsible for ensuring that WSF meets its legal obligations.
- The **Data Protection Officer** is responsible for:
  - Keeping the Board updated about data protection responsibilities, risks and issues.
  - Reviewing all data protection procedures and related policies, in line with the agreed schedule. [Annually in January of each year]
  - Arranging data protection training and advice for the people covered by this policy.
  - Handling data protection questions from staff and anyone else covered by this policy.
  - Dealing with requests from individuals to see the data WSF holds about them (also called 'subject access requests').
  - Checking and approving any contracts or agreements with third parties that may handle the WSF's sensitive data.
  - Approving any data protection statements attached to communications such as emails and letters.
  - Addressing any data protection queries from journalists or media outlets like newspapers.
  - Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

- The **Operations Manager** is responsible for:
  - Ensuring all systems, services and equipment used for storing data meets acceptable security standards.
  - Performing regular checks and scans to ensure security hardware and software is functioning properly.
  - Evaluating any third-party services the WSF is considering using.

General staff guidelines

- The only people able to access data covered by this policy should be those who **need it for their work**.
- Data **should not be shared informally**. When access to confidential information is required, employees can request it from their line managers.
- **WSF will provide training** to all employees to help them understand their responsibilities when handling data.
- **Employees** should keep all data secure, by taking sensible precautions and following the guidelines below.
- In particular, **strong passwords must be used** and they should never be shared.
- Personal data **should not be disclosed** to unauthorised people, either within the WSF or externally.
- Data should be **regularly reviewed and updated** if it is found to be out of date and is no longer required, it should be deleted and disposed of.
- Employees **should request help** from their line manager or the Data Protection Officer if they are unsure about any aspect of data protection.

Data storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the Operations Manager. When data is **stored on paper,** it should be kept in a secure place where unauthorised people cannot see it. These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept **in a locked drawer or filing cabinet**.
- Employees should make sure paper and printouts are **not left where unauthorised people could see them**, like on a printer.
- **Data printouts should be shredded** and disposed of securely when no longer required.

When data is **stored electronically**, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data should be **protected by strong passwords** that are changed regularly and never shared between employees.
- If data is **stored on removable media** (like a CD or DVD), these should be kept locked away securely when not being used.
- Data should only be stored on **designated drives and servers**, and should only be uploaded to **approved cloud computing services**.
- Office based servers containing personal data should be **sited in a secure location**, away from general office space.
- Data should be **backed up frequently**. Those backups should be tested regularly, in line with the WSF's standard backup procedures.
- Data should **never be saved directly** to laptops or other mobile devices like tablets or smart phones.
- All servers and computers containing data should be protected by **approved security software and a firewall**.

Recommended Retention Times are detailed in Appendix A.

Basis for processing data

At least one of the following lawful bases for processing data must apply whenever personal data is processed:

- **Consent:** The individual given clear consent for you to process their personal data for a specific purpose [Privacy Policy]
- **Contract:** The processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps [SPIN etc.]
- **Legal obligation:** The processing is necessary for you to comply with the law (not including contractual obligations).

- **Vital interests:** The processing is necessary to protect someone's life.
- **Public task:** The processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
- **Legitimate interests:** The processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

Many of the lawful bases for processing depend on the processing being "necessary". This does not mean that processing always has to be essential. However, it must be a targeted and proportionate way of achieving the purpose. **The basis for the WSF to process the majority of its data is Consent and Contract.** Further information on the lawful basis for processing data can be found at: *z:/Data Protection/180131_Lawful Bases For Process Data.pdf*.

Consent and individuals' rights
Individuals have the right to:

- Ask the WSF not to process their personal data for marketing purposes
- Unsubscribe from WSF newsletters and other communications by clicking on the link provided in email communications
- Access and modify their data; where such data is non-editable they can request that the WSF does this on your behalf.
- To lodge a formal complaint with the Information Commissioner's Office (ICO).

Data use
Personal data is of no value to the WSF unless the business can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data, employees should ensure **the screens of their computers are always locked** when left unattended.
- Personal data **should not be shared informally**. In particular, it should never be sent by email, as this form of communication is not secure.
- Employees **should not save copies of personal data to their own computers.**

Always access and update the central copy of any data from the Z Drive.

Data accuracy
The law requires WSF to take reasonable steps to ensure data is kept accurate and up to date. The more important it is that the personal data is accurate, the greater the effort WSF should put into ensuring its accuracy. It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in **as few places as necessary**. Staff should not create any unnecessary additional data sets.
- Staff should **take every opportunity to ensure data is updated.** For instance, by confirming a customer's details when they call.
- WSF will make it **easy for data subjects to update the information** WSF holds about them. For instance, via the WSF website.
- Data should be **updated when inaccuracies are discovered**. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.
- It is the Data Protection Officer's responsibility to ensure **databases are checked against industry suppression files** every six months.

Data breaches
The WSF is not obliged to report data breaches to the Information Commissioner's Office as any such breach is unlikely to result in a risk to the rights and freedoms of individuals. However, in all instances the Data Breach Policy [found at: *z:/Data Protection/180131_Data Breach Policy.pdf* should be followed.

Subject Access Requests
All individuals who are the subject of personal data held by WSF are entitled to:

- Ask **what information** the WSF holds about them and why
- Ask **how to gain access** to it

- Be informed **how to keep it up to date**
- Be informed how the WSF is **meeting its data protection obligations**.

An individual contacts the WSF requesting access to their data, requesting deletion or correction of erroneous or incomplete data or to object to the use of data is called a **Subject Access Request** (SAR). SARs from individuals should be made by email, addressed to the Data Protection Officer at wsf@worldsquash.org.

The Data Protection Officer can supply a standard request form, although individuals do not have to use this. The Data Protection Officer will aim to provide the relevant data within 14 days (see *z:/Data Protection/180131_Subject Access Request Flowchart.pdf*.). The Data Protection Officer will always verify the identity of anyone making a subject access request before handing over any information.

APPENDIX A

RETENTION TIMES

ADRV: anti-doping rule violation
AAF: *adverse analytical finding*
ATF: *atypical finding*
NAF: non-analytical finding

I. Referenced data will be deleted no later than the end of the calendar quarter following the expiry of the stated retention period.
II. For practical reasons, retention times are submitted to two categories; 18 months and 10 years.
III. Retention times can be extended in case of pending anti-doping rule violations.

Module	Data	Retention periods	Remarks	Criteria
1 – *Athlete*		as of time when *Athlete* is excluded from ADO's *Testing* pool:	***Athlete* data relevant for practical purposes and because of multiple violations.** **These data are not particularly sensitive.** **Managed by ADO.**	
Athlete (general)	Name	Indefinitely	This can be retained indefinitely. ADOs should be allowed to keep a record of *Athletes* that have been part of their *Testing* pool. For elite *Athletes*, this information is public information anyway.	
	Date of birth	Indefinitely		
	Sport discipline	Indefinitely		
	Gender	Indefinitely		
	Phone number(s)	10 yrs	10 years because of possible ADRV: AAF/ATF (stored *Sample*) or NAF	Necessity
	Email address	10 yrs	10 years because of possible ADRV: AAF/ATF (stored *Sample*) or NAF	Necessity
	Home address	10yrs	10 years because of possible ADRV: AAF/ATF (stored *Sample*) or NAF	Necessity
2 – Whereabouts (except for the *Athlete* Passport program see section 8)		as of date to which the data relate:	**Only small amount of Whereabouts is relevant to retain, but it is impossible to establish which part.**	
Whereabouts	Whereabouts	18 months	Can be relevant to establish ADRV retrospectively	Necessity
	Failures	18 months	Relevant to count three Strikes in 12 months time	Necessity
	Missed tests	18 months	Relevant to count three Strikes in 12 months time	Necessity
			If ADRV, will be kept as part of disciplinary file indefinitely (see section 7).	
3 – *TUE*			**Destroying medical information makes it impossible for WADA to review *TUE*s retrospectively after *TUE* has lost its validity** ***TUE* information is largely medical and therefore specifically sensitive.** **Managed by ADO / TUEC.**	

Module	Data	Retention periods	Remarks	Criteria
TUE	*TUE* approval forms *TUE* supp. med information *TUE* info not included: (i) on the approval form; or (ii) in the supporting medical information	10 yrs as of approval date 18 month from end of validity of *TUE*	Can be relevant in case of re-*testing*. Loses relevance after expiration of *TUE* except in case of re-application (and sensitive information).	Proportionality / Necessity Proportionality
4 – *Testing*		as of document creation date / as of first indication of AAF, ATF, ADRV or *Sample* collection	**Long retention only relevant in case of AAF, ATF, ADRV or stored *Sample*(s).** **Managed by ADO.**	
Testing	Mission orders *Doping Control* Form Chain of Custody	18 months / 10 yrs 18 months / 10 yrs 18 months/ 10 yrs	18 months if there is no indication of an ADRV/ 10 yrs if there is an indication of a possible ADRV, if the *Sample* is stored for possible re-*testing* or if it is part of a passport program. 18 months if there is no indication of an ADRV/ 10 yrs if there is an indication of a possible ADRV, if the *Sample* is stored for possible re-*testing* or if is part of a passport program. 18 months if there is no indication of an ADRV/ 10 yrs if there is an indication of a possible ADRV, if the *Sample* is stored for possible re-*testing* or if it is part of a passport program.	Proportionality /Necessity Proportionality /Necessity Proportionality /Necessity
5 – *Samples* (lab)			**Only positive *Samples* are a possible privacy issue** **Managed by Laboratory**	
Samples	A *Sample* B *Sample*	Indefinitely / 10 yrs Indefinitely / 10 yrs	These *Samples* are anonymous, and may be retained indefinitely for scientific purposes. In case of an AAF, and if the *Sample* is identifiable, 10 yrs should be the maximum retention time.	Proportionality Proportionality
6 – Test results/Results management (forms/ documentation)		as of creation of relevant documents:	**Relevant because of multiple violations and retrospective analysis** **Managed by ADO**	
Results	Negative findings AAF ATF	10 yrs 10 yrs 10 yrs	Negative results have an historical value and keeping them could be in the interest of the *Athlete*. Necessary because of multiple violations. Necessary because of multiple violations.	Proportionality /Necessity Necessity Necessity

Module	Data	Retention periods	Remarks	Criteria
7 – Disciplinary Rulings (ADRV)			**Relevant because of multiple violations.** **Managed by disciplinary body / sports federation / ADO.**	
Disciplinary rulings	Sanctions under the *Code* Arbitral awards Relevant supporting documentation/files	Indefinitely Indefinitely Indefinitely	Should be kept indefinitely for legal and precedential value.	Necessity Proportionality
8 – *Athlete Biological Passport** * Differentiation between *Samples* and results. As *Samples* are not used for directly establishing ADRV, *Samples* will not be stored, only results. * For blood there are no A or B *Samples*. * Only positive *Samples* are a possible privacy issue. Biological passport *Samples* are not positive *Samples*.				
Results	Results	10 yrs as of date results were obtained	For the biological passport (blood module), the endocrinological/steroidal urine modules or longitudinal profiling, the retention time for results is 10 yrs.	Necessity
Whereabouts	Whereabouts	10 yrs as of date the data relates to	10 yrs when needed to support atypical/abnormal results/to refute *Athlete*'s claims. For cases where circumstances warrant for negative results to be stored for future inclusion in the biological passport (blood module/endocrinological/steroidal urine modules): 10 yrs (only needed for limited amount of *Athletes*).	Necessity