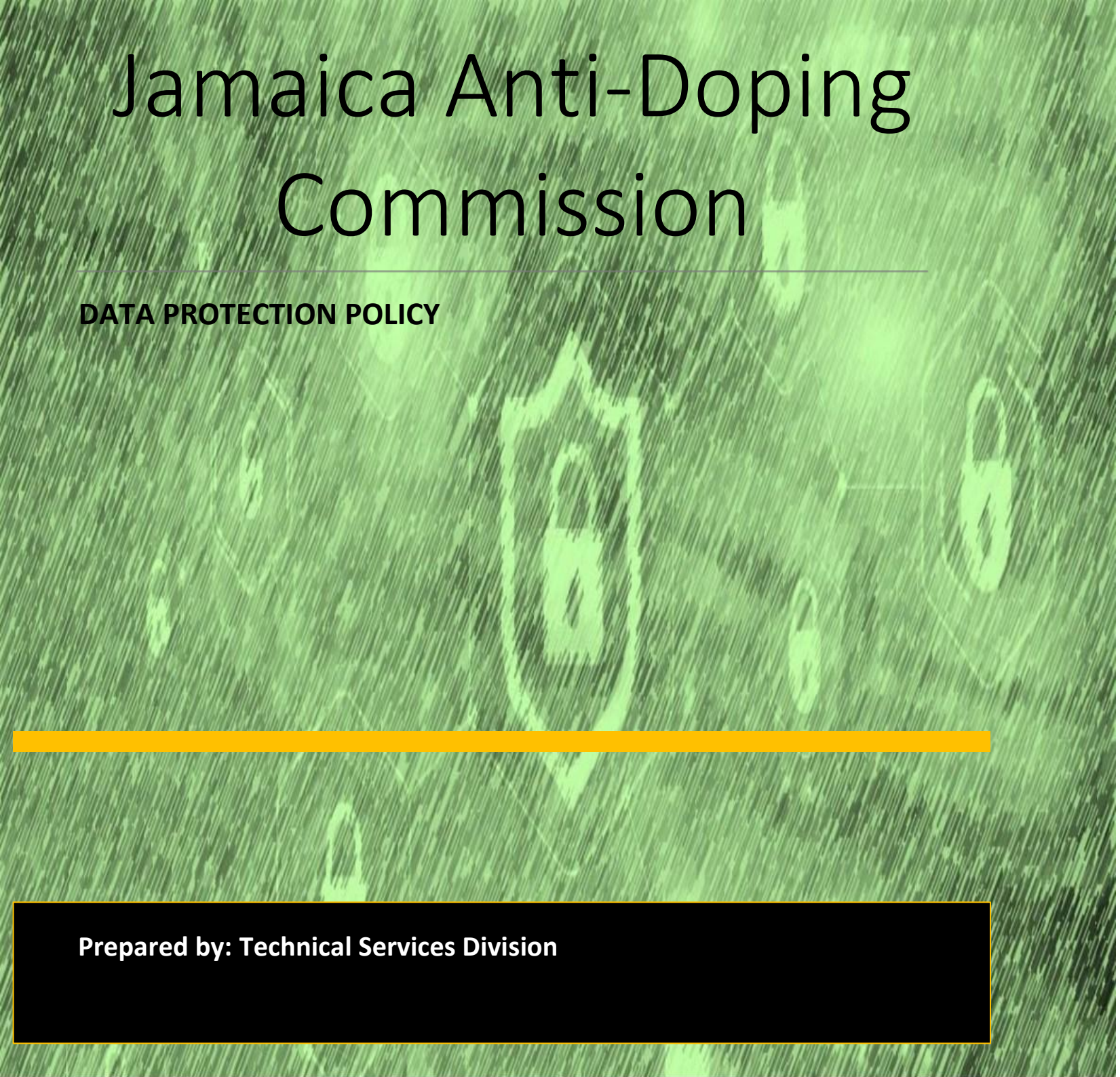
Jamaica Anti-Doping Commission

DATA PROTECTION POLICY



Prepared by: Technical Services Division

Contents

Data Protection Policy 4
The Scope....4
Parties Involved 5
Governance structure 6
Duties of JADCO as Data Controller....7
Responsibilities of Data Protection Officer 7
Consent 9
Minor....9
Reporting....9
Budget 9
Conflict of Interest 10
Records of Processing....10
Access to Personal Data 11
Data Processors/ Third Parties 14
Managing Third Parties 15
Types of Data Held 15
How data will be used....16
Technical Division 17
Intelligence & Investigations 17

Communication and Education Division 17
Protection of Data 18
General Protections 18
The Rights of the Athlete (Data Subject) 19
Responding to a Data Subject Request 21
Risk Assessment 22
Data Breach 23
Notifying other Organizations 24
Remediation Steps After Data Breach 24
Improvements for Future Response 25
Information Security Program 25
Information Security Policy 26
Protection of Data 26
Security Controls 27
Training of Staff 28
Retention Time 29
Legal Basis for Data Processing 40
Annex A 40
Annex B 42
Annex C 46

Contact 47

Data Protection Policy

- This policy is concerned with the use of personal data related to anti-doping, including past, present and future information. The information shall be collected from the athletes (or 'data subjects') and support personnel as defined in anti-doping rules.
- The Jamaica Anti-Doping Commission (JADCO) shall only use the information for the purpose of anti-doping. JADCO considers the protection of the athlete's personal data as our duty, and the process shall be in accordance with the International Standard for the Protection of Privacy and Personal Information (ISPPPI), 2021 set out by The World Anti-Doping Agency (WADA) and, when applicable, The Data Protection Act, Jamaica (2020).
- For the purposes of this policy JADCO shall be known as and referred to interchangeably as the 'data controller'.

The Scope

- This policy covers personal information past, present and future which has been received from the athlete or about the athlete for the purpose of doping control. It also covers the processing of the athlete's information, including storing, analysing, updating, accessing, transferring and deleting of said data. This policy shall not be concerned with any scope outside doping control processes.
- JADCO shall update this policy when needed (when changes to anti-doping rules or internal policies occur). The update shall be made known to the athlete and JADCO's staff in advance.
- JADCO's staff shall strictly adhere to this policy and shall make sure any third party involved shall do the same. JADCO's staff shall be held accountable by law for the breach of this policy.

Parties Involved

The divisions identified will interact with the Data Protection Officer to ensure that the mandate of the data protection policy is observed and maintained.

Executive Director – The Data Protection Officer shall assist the Executive Director to ensure that all applicable rules, standards and procedures are observed and maintained throughout the data protection process.

Legal – The Data Protection Officer shall work with legal professionals to ensure that all applicable rules, standards and procedures are included in the internal policy.

Information and Communication Technology (ICT) – The Data Protection Officer shall work with ICT professionals to ensure appropriate safeguards for personal information are implemented.

Risk Management – The Data Protection Officer shall work with the Enterprise Risk Management Analyst to ensure that data protection standards are maintained throughout the processing of information.

Technical Services - Data Protection Officer shall work with the Technical Services Division to ensure that data protection standards are maintained throughout the processing of information during doping control processes.

Human Resource Management and Administration - Data Protection Officer shall work with the HRM&A Division to ensure that data protection standards are maintained for staff.

Communication and Education - Data Protection Officer shall work with the Communication and Education Division to ensure that data protection process is adhered to when collecting information from athletes and support personnel.

Finance & Accounts - Data Protection Officer shall work with the Finance & Accounts Division to ensure information relating to personal emoluments and deductions are kept confidential.

Governance structure

Data protection lead: Shaquiera Scott

Contact number: 876-322-2521

Email address: protectdata@jadco.gov.jm

Executive Director - the chief operating officer of the Jamaica Anti-Doping Commission is responsible for making key operational, budgetary decisions relating to JADCO.

Data Protection Officer – the responsible officer for collecting and maintaining all data provided by athletes. Data Protection Officer reports directly to the Executive Director.

The Director of Technical Services, Director of Communication and Education, Director of Human Resources Management and Administration, Director of Intelligence & Investigations – responsible for providing the Data Protection Officer with personal information and report to the Executive Director.

Information & Communication Technology Manager – responsible for responding to data breaches and protecting information systems that hold personal data and reports to the Executive Director.

Director of Finance – responsible for budgetary plans and reports directly to the Executive Director.

Executive Secretary – assists and reports directly to Executive Director.

Duties of JADCO as Data Controller

- JADCO shall determine the purpose for which and the manner in which any personal data should be collected and shall ensure that personal information being processed is accurate, complete, and kept up to date.
- JADCO shall inform athletes and/or athlete representatives of their obligation to ensure such information is accurate, complete, and up to date. Where possible, JADCO should provide athletes with readily accessible means to access their own personal information and make required updates.
- JADCO shall take all practicable steps to ensure that any personal information that is duplicated be removed as far as reasonably possible.

Responsibilities of Data Protection Officer
The Data Protection Officer shall:

1) Ensure that JADCO complies with the ISPPPI and applicable data protection and privacy laws and good practice;

2) Consult the Commissioner established under the Data Protection Act Jamaica, 2020 to resolve any doubt about how the provisions of the said Act and any regulations made under this Act are to be applied;

3) Ensure that JADCO has valid legal grounds to process personal information for anti-doping purposes;

4) Prepare, implement and regularly review the organization's internal privacy policies and procedures;

5) Prepare records of processing;

6) Serve as the main contact within and outside JADCO for privacy-related inquiries, requests, or complaints;

7) Ensure that the retention times for personal information set out in Annex A of the ISPPPI are adhered to;

8) Assist data subjects in the exercise of their rights under the Data Protection Act, ISPPPI and any other regulation related to privacy;

9) Provide notice to the data controller of any contravention of the data protection standard, or any of the provisions of the Data Protection Act or ISPPPI respectively;

10) Work with ICT professionals to ensure appropriate safeguards for personal information are implemented;

11) If necessary, provide notice of a security breach to the relevant individuals.

Consent

- Any consent required to be given, by a data subject, to the processing of personal data must be informed, specific, unequivocal, freely given, expression of will by which the data subject agrees to the processing of that data subject's personal data. This includes consent given by any individual to whom the data subject delegates, in writing, in such form and manner as may be prescribed, in the case of a minor, a parent or legal guardian of the minor.

Minor

- The rights conferred on athletes may be exercised by a parent or legal guardian of the minor, or by the minor in any case where the law recognizes the capacity of the minor to act in the matter to which the personal data relates.

Reporting

- The Data Protection Officer shall report to the Executive Director. The Executive Director shall have complete authority over the data protection process and shall be responsible for approving all decisions relating to the processing of data. The Data Protection Officer shall be accessible to all staff. All staff are encouraged to raise privacy questions and issues with this person.

Budget

- The Data Protection Officer will need adequate resources to fulfil their role. Data Protection Officer shall create an annual budget for the purposes of data protection.

The data protection budget may need to account for the following:

1) Human resources (employee salaries, training costs, other expenses);
2) Costs for external legal advisors, auditors, or consultants;
3) Costs for privacy compliance software or other tools (e.g., e-learning vendors, or tools to create records of processing or manage privacy risks);
4) Costs for staff training materials and tools. Other Resources - WADA's ISPPPI templates, guidance, and courses available on ADEL will also be utilised.

Conflict of Interest

- The person acting in the capacity of Data Protection Officer shall not be qualified to be appointed if there is or is likely to be any conflict of interest between the person's duties as Data Protection Officer and any other duties of that person.

Records of Processing

- The personal information will be used for the detection, deterrence and prevention of doping in sport, in accordance with the World Anti-Doping Code (Code), the International Standards (IS), the anti-doping rules of JADCO with authority to test the athlete.

This includes:

- Test planning and management;
- Sample analysis;

- The Athlete Biological Passport, which collates biological markers from multiple samples and multiple testing authorities;
- Results management, in the event of an adverse or atypical finding based on the athlete's sample (s) of the ABP. If the athlete has a therapeutic use exemption, it could be relevant to results management;
- Intelligence-gathering and investigations;
- Secondary purposes- anti-doping research or to improve and verify the quality of anti-doping detection methods if the conditions of Code Article 6.3 are met, namely: measures are adopted to ensure the athlete's personal information and sample cannot be linked to each other and cannot be traced back to the athlete.

Access to Personal Data

1) Athlete Profile

Basic demographic information is collected to appropriately identify athletes in ADAMS, and to contact them where necessary (for example, the athlete may need to be notified of an adverse analytical finding or whereabouts failure or to be contacted by a doping control officer seeking to locate him/her for doping control).

2) Test Planning

The test planning module in ADAMS enables Anti-Doping Organizations (ADOs) with testing authority over an athlete to plan, coordinate, order, monitor, and avoid duplication of doping controls for athletes under their authority. ADOs with testing authority can include National

Anti-Doping Organizations, International Federations, and Major Event Organizers. It is possible for multiple ADOs to have the authority to test you.

3) Lab results

The laboratory results module in ADAMS was specifically designed to preserve the confidentiality and integrity of laboratory results. Laboratories can only see and submit laboratory results associated with sample codes, not an athlete's name, and these results cannot be modified by any organization other than the laboratory that submitted the results.

4) Whereabouts

Whereabouts are used to plan, coordinate, and conduct doping controls (in particular, no advance notice and out of competition testing), to support the analysis of athlete biological passports or other analytical results, or to support the investigation of or proceedings regarding anti-doping rule violations.

Not all athletes are required to provide whereabouts. Athletes within JADCO Anti-Doping registered testing pool (high-level athletes) are required to provide complete whereabouts, as set out in the International Standard for Testing and Investigations. Other athletes may be placed in other whereabouts pools (Lower Testing Pool and Team Testing Pool) and asked to provide a subset of these whereabouts. These rules are set by JADCO and is reassessed on an ongoing basis.

5) Therapeutic Use Exemption

Therapeutic Use Exemptions (TUEs) allow athletes with a medical condition to use a prohibited substance or method where the conditions of the Code and the International Standard for Therapeutic Use Exemptions (ISTUE) are met. The TUE ADAMS module ensures TUE decisions are properly recorded to facilitate the mutual recognition of such decisions and to avoid the duplication of activities related to their review.

6) Athlete Biological Passport

The Athlete Biological Passport (ABP) module in ADAMS complements analytical methods to detect the use of prohibited methods or substances. It can be used to inform target testing or investigations, or to establish a prohibited use on its own. The ABP collates information on biological markers of blood and steroid doping from all samples collected for anti-doping purposes that meet the requirements of the ABP, regardless of the testing authority.

Passports are managed by athlete passport management units (APMUs), which are special units of WADA-accredited laboratories. Like laboratories, they can only see passport information associated with a passport ID, not the athlete name.

7) Results Management

The results management module is used to facilitate the coordinated management of positive test results and sanctioning of anti-doping rule violations (ADRVs) to avoid duplication of such activities and facilitate the mutual recognition of disciplinary decisions.

8) Intelligence & Investigations

JADCO is required to obtain, assess, and process anti-doping intelligence from all available sources to help deter and detect doping and to inform effective testing strategies. All analytical or non-analytical information or intelligence that provides reasonable cause to suspect that an

anti-doping rule violation may have been committed are investigated. ADAMS serves as one source of information to support these intelligence-gathering and investigatory functions.

Data Processors/ Third Parties

- **Jamaica Anti-Doping Commission (JADCO), International Federation (IF), Major Event Organizer (MEO)** - JADCO acting as testing authority (TA) and/or results management authority (RMA), international federation, or the organizer of an event the athlete participated in- and their sample collection authority and/or doping control coordinator, as identified on the DCF, or their other delegated third parties.

- **World Anti-Doping Agency (WADA), Delegated Third Parties, WADA Accredited Laboratories** - WADA (World Anti-Doping Agency) and its delegated third parties. WADA operates and manages ADAMS, a platform hosted in Canada based on the rules of the Code and IS, onto which your personal information will be uploaded by the Testing Authority. ADAMS will be used by the recipients described above to share the athlete's personal information as necessary for their anti-doping activities.

- **Athlete Passport Management Units** - Laboratories and Athlete Passport Management Units that are subject to the International Standard for Laboratories. They only have access to coded data (based on sample codes or passport IDs) that does not disclose the athlete's identity.

Managing Third Parties

- Third Parties will be required to sign the Data Protection Partnership Agreement with JADCO to indicate their commitment to keeping data stored, controlled, transferred by them.
- The Data Protection Agreement should detail the responsibilities that third parties will have to observe and their commitment to compliance with standards set by WADA through the ISPPPI, the Data Protection Act Jamaica, 2020 and any other regulations that relates to data protection in sports.

Types of Data Held

- Name of Athlete
- Athlete's Whereabouts Information
- Athlete's and Support Personnel identification information
- Athlete's sample analysis information (e.g., sample code number, sample type, altitude levels or exposure to extreme environmental conditions, and/or a list of recent medications/supplements or blood transfusions
- Athlete's Laboratory Test Results
- Athlete's Age/Date of birth
- Athlete's Address
- Athlete's and Support Personnel Contact number

- Athlete's and Support Personnel Email address
- Athlete's Doctor name
- Athlete's Coach's name
- Athlete's Sport
- Athlete's Discipline
- Country Athlete represent/s
- Athlete's Gender
- Athlete's Sample code
- Athlete's Biological Passport ID
- Medications ingested
- Athlete's Medical records
- Any other personal data collected from athlete and support personnel

How data will be used

- The data shall not be used for any commercial purposes, including direct marketing, sale of any goods and/or services. JADCO shall be assessing the processing of collected data every six (6) months to mitigate any risk to the athlete's data.
- The athlete's data may be shared with other anti-doping organisations (ADO) through the Anti-Doping Administration and Management system (ADAMS) in accordance with the International Standard for the Protection of Privacy and Personal Information (ISPPPI).

Technical Division
The athlete's data shall be used by JADCO for the following purposes:

1. To formulate our Testing Pools and Test Distribution Plan including whereabouts information.
2. To carry out Anti-Doping related research.
3. To communicate with you on Anti-Doping matters and processes.
4. To promote international cooperation in the fight against doping in sport.
5. To be used in the processing of a Therapeutic Use Exemption (TUE).
6. To be used in the process of Athlete Biological Passport.
7. To be used in the process of Result Management.

Intelligence & Investigations
The athlete's data shall be used by JADCO for the following purposes:

1. To investigate any potential Anti-Doping Rule Violation.
2. To be used in the process of compliance and enforcement of ADRVs.

Communication and Education Division
The athlete's data shall be used by JADCO for the following purposes:

1. To tailor and implement JADCO's education plan.
2. To conduct social research.

3. To conduct informational package distributions.

Protection of Data

- In accordance with this policy, and ISO9001:2015, JADCO shall establish a Document Control Centre (DCC) where the movement of each document containing the athlete's personal data shall be tracked both within JADCO and in the case where third party is involved. JADCO shall also set up a secure email and cloud server, and back-up system (on-site, off-site and cloud) to store your information electronically.
- Access shall only be granted to persons within JADCO's departments when required on a need-to-know basis.
- Physical copies of the athlete's document and information shall be stored in locked cabinets with access available only to the DCC.

General Protections

- **Access controls**: third parties have no access to the names of the Athletes on which data is maintained, authenticator code used to enter ADAMS, passwords to access computers assigned to staff, no sharing of passwords between/ among staff, three (3) tier back-up (on-site, off-site and cloud);

- **Physical controls**: The physical filing cabinet is locked and kept in a room; JADCO's office is only accessible with a key card by an authorized person;

- **Technical controls**: System containing personal information is hosted on international server, local personal information maintained on computers is protected by a firewall, anti-malware and protected perimeter (ie. Wifi), encryption of information in transit and at rest, IT must develop an incident response plan; Authentication requirements (e.g., unique logins, complex passwords, and second or multi factor authentication steps, such as TOTP or SMS codes, biometric authentication, etc.); Encryption, including for any transmitted information; Applying system upgrades and patches; Applying automatic screen locks and logoffs on all devices;

- **Organizational controls**: all personnel must sign written confidentiality agreements, all personnel must be trained on data privacy and protection; sign-in logs for visitor access to physical offices, doping control stations, records or other locations where personal information is processed or stored; camera surveillance of entry/exit points and areas where data will be processed; secure disposal of confidential physical files by shredding; implementing approval processes to limit access to personal information; and

- **Environmental controls**: Smoke detectors installed to alert when a fire occurs.

The Rights of the Athlete (Data Subject)
Under this policy, and in accordance with the ISPPPI and Data Protection Act, Jamaica (2020), the athlete shall have the rights to:

1. **Request to access own personal data** - the athlete may have the right to access or request a copy of the personal data that JADCO is collecting, using, or disclosing about you. The athlete must provide identification to prove identity, for their own privacy and security.
2. **Request to alter or update personal data** – the athlete may have the right to have incomplete, inaccurate, misleading, or not up-to-date Personal Data that JADCO collects, uses, or discloses rectified.

3. **Request the deletion of personal data** (subject to World Anti-Doping Code, International Standards, JADCO's anti-doping rules and applicable law) – the athlete may have the right to request that we delete or de-identity Personal Data that JADCO collects, uses, or discloses, except JADCO is not obligated to do so if it needs to retain such data in order to comply with a legal obligation or to establish, exercise, or defend legal claims.
4. **Request to terminate your consent** - For the purposes the athlete has consented to JADCO collecting, using, or disclosing of personal data, the athlete has the right to withdraw consent at any time. However, if the athlete so chooses to withdraw their consent they must be informed that this could also have consequences against them, such as triggering a non-compliance with the WADA Code and International Standard for Results Management as well as the JADCO Rules, thus producing an ADRV (Evasion, Refusal or Failure to Submit to Sample Collection); or preventing him or her from participating in sport events.
5. **Request the transfer of personal information to other anti-doping organisations** - the athlete may have the right to obtain personal data JADCO holds, in a structured, electronic format, and to send or transfer such data to another data controller, where this is (a) personal data which the athlete has provided to JADCO, and (b) in the case where JADCO is collecting, using, or disclosing such data on the basis of the athlete's consent or to perform a contract with you.
6. **Object to Personal Data being used for other purposes** – the athlete may have the right to object to certain collection, use or disclosure of personal data such as objecting to direct marketing.
7. **Restrict Personal Data being used in certain circumstances** – the athlete may have the right to restrict the use of personal data in certain circumstances.

8. **Lodge an official complaint with JADCO on the process of Personal Data Protection** – the athlete may have the right to lodge a complaint to the competent authority where it is believed that the collection, use or disclosure of personal data is unlawful or noncompliant with applicable data protection law.
9. **Informed Consent** - the athlete must be informed whether personal data of which that individual is the data subject are being processed by or on behalf of the JADCO and given the opportunity to expressly consent to that data being processed. This includes the personal data of which the individual is the data subject, the purposes for which the personal data are being or are to be processed, the recipients of classes of recipients to whom they are or may be disclosed.

Responding to a Data Subject Request

- When the athlete makes a requests in accordance with his rights as set out under the ISPPPI and the Data Protection Act, Jamaica(2020) JADCO, by way of the Executive Director, shall acknowledge the request of the data subject, in writing, stating that the request will be complied with or indicate the intention to comply.
- The Executive Director will liaise with the Data Protection Officer to ascertain whether the request can be fulfilled or not, and the reasons if not fulfilled.
- The Data Protection Officer shall respond to the Executive Director, giving reasons, for regarding the notice as, to any extent, unjustified and the extent (if any) to which the Data Protection Officer has complied or intends to comply with the request.
- If the Data Protection Officer intends to fulfil the request, in full or in part, it must be confirmed whether this is being done along with any relevant supporting documentation (for example, a copy of the requested personal information, or evidence that a requested correction has been completed); and if refusing to fulfil the request, in full or in part, the reasons for the refusal.

- The Data Protection Officer must ensure that the request is fulfilled, within 21 days, and in the event of a complaint being lodged that said complaint is resolved so that any unlawful or non-compliant practice remedied.

Please note: If JADCO cannot satisfactorily resolve the issue directly with the Person, JADCO will consult with WADA at privacy@wada-ama.org, who may issue recommendations to JADCO for resolving the issue.

The athlete's complaint may also be filed with the national regulator responsible for data protection in Jamaica; the Office of Information Commissioner.

Risk Assessment

- The Compliance and Risk Management Department shall conduct risk assessment for potential breaches using the Risk Assessment Matrix (**See Annex C**). This risk assessment shall be conducted routinely each quarter, at the start of each year and at the end or when required.
- Risk assessments should be completed in consultation with employees from other divisions. This will assist in identifying hazards which may normally go unnoticed.
- The Risk Assessment Matrix will assess consistent data protection, IT and/or cyber-security risks that may harm data collected, stored, shared, transferred. These risks may be amended as required or when new risks are identified.
- Once the hazards have been identified, the degree of risk they present needs to be determined. This entails pre-empting how these hazards can cause potential injury in different situations and conditions.

- After conducting a thorough assessment of the risk, JADCO should then look at processes to eliminate or reduce the risk as much as possible. JADCO should use the hierarchy of control measures provided on the Risk Assessment Matrix to do this.
- Review is an ongoing process, in the event something new is introduced into the environment JADCO may need to consider if their control measure is the most effective for their business.

Data Breach

- In the event of a data breach communication of said breach shall be sent to Compliance and Risk Management Department as soon as possible. There shall be an explanation by the officer who identified the data breach of the effects of said breach to the Risk and Compliance Officer.
- Communication of a data breach shall be sent to the athlete/s and or athlete representative as soon as possible. The communication shall be sent and shall detail the circumstances in which the breach may affect the rights and interests of the athlete in a significant way.
- There shall be a record (**See Annex A**) of any breach that has occurred that affects or is likely to affect in a significant way the rights and interests of the persons concerned. The record shall include the following:

1. Facts of breach
2. Effects of breach
3. Remedial action taken

All internal data breaches identified by JADCO must be reported on the Internal Security Breach Reporting Form and sent to the Executive Director for processing (**See Annex B**).

Notifying other Organizations

- JADCO must communicate and collaborate with WADA, other ADOs, International Federation and National Federation that may be affected by the breach or that have a relationship with the affected individuals. Where a security breach affects personal information processed via ADAMS, JADCO is required to promptly notify WADA of the breach.
- JADCO may be required to notify a regulatory authority for privacy or data protection (Information Commissioner, see: Data Protection Act (2020), Jamaica).
- JADCO may also be required to notify cyber security centres or threat intelligence networks in the event of a malicious attack, or law enforcement (Counter Terrorism and Organized Crime Investigation Branch of the Jamaica Constabulary Force) in the event illegal activity is suspected.
- Under the ISPPPI, there are no mandatory timing or content requirements for notification to other organizations.

Remediation Steps After Data Breach

- In addition to notifying affected individuals and organizations, there are many steps you can take to remediate a breach. The specific measures will depend on the nature of the breach you suffered. They could include:

1. Re-training or providing more training to staff;
2. Isolating or disabling compromised systems;
3. Changing all passwords on compromised systems;
4. Remote wiping lost or stolen devices;
5. Monitoring logs, systems and networks for signs of suspicious activity; or

6. Restoring lost information from a backup (off-site cloud server).

Improvements for Future Response

- To improve the management of future breaches, the stipulated time stated in the policy guideline should be adhered to. All breaches and lessons learned should be documented throughout the process.
- JADCO should document these lessons in a record/log of the breach or another document, and update the breach response plan as needed.

Information Security Program

- Information security program will be implemented, controlled and monitored by the Information and Communication Technology Division. This includes policy settings that prevent unauthorized people from accessing business or personal information. Information and Communication Technology Division shall be responsible for developing policies and procedures to manage and monitor network and infrastructure security, testing and auditing.

- Information and Communication Technology Division will be responsible for research, and will consult with the Executive Director on new technology that can be used to protect sensitive information from unauthorized activities, including inspection, modification, recording, and any disruption or destruction.

- JADCO must provide adequate budget allocation for security to the Information and Communication Technology Division, and ensure that they are ready to detect, respond to, and proactively prevent, attacks such as phishing, malware, viruses, malicious insiders, and ransomware.

Information Security Policy

- Information and Communication Technology Division shall be responsible for creating and implementing an Information Security Policy (ISP) to guide individuals when using IT assets.

- The ISP must be updated frequently based on company changes, new threats, conclusions drawn from previous breaches, and changes to security systems and tools.

Protection of Data

- The privacy of data that is collected and stored by JADCO is of paramount importance and is a requirement under the Data Protection Act of Jamaica.
- JADCO will ensure that the necessary controls are in place to protect and limit access to personal data unless authorized to do so.
- Data must be secured from unauthorized access in transit and at rest and the following controls have been implemented as part of the strategy to achieve this goal.

Security Controls

- Security controls are mechanism that are employed to restrict access to information, to prevent the manipulation or changing of information without the proper authorization or to prevent from viewing information that is not meant for public scrutiny.

Encryption

- Data transmitted over the Internet is encrypted using the Transport Layer Security (TLS) protocol. TLS encrypts data to ensure that eavesdroppers and hackers are unable to see what is being transmitted which is useful for private and sensitive information such as passwords, personal correspondence and credit card information.

Group Policy

- Group Policy is a hierarchical infrastructure that allows a network administrator in charge of Microsoft's Active Directory to implement specific configurations for users and computers. Group Policy is primarily a security tool, and can be used to apply security settings to users and computers. With the use of group policies, access to files and folders containing specific data is restricted to all users except those authorized to interact with the data.

Microsoft Intune

- Microsoft Intune is a cloud-based endpoint management solution that is used to manage user access and simplifies app and device management across devices, including mobile devices, desktop computers, and virtual endpoints. Access to data on organization-owned devices can be protected from malicious individuals. JADCO uses the cloud-based Microsoft Business 365 and has Intune implemented on its mobile devices and desktop computers.

- JADCO has also put in place next-generation firewall system to monitor and block unauthorized traffic from accessing its network from external entities.

Training of Staff

- JADCO will ensure at all times that those with specific responsibilities under this policy will have access to the relevant training. In the event of any changes to the International Stanm or statute will be required to and be able to evidence that appropriate training has been undertaken.
- Training shall take place once each quarter or when required after changes to any policies, procedures and/or regulations.
- Training shall be conducted by the Data Protection Officer in conjunction with the Information and Communication Technology Division on the following areas:

1. Privacy rules for personal identifiable information (PII)
2. Secure data processing
3. Safe data handling
4. Third-party data handling
5. Data protection laws
6. Compliance regulations
7. Cybersecurity awareness
8. Physical access to the data centre
9. Data handling practices
10. Documenting, monitoring, and reviewing data assets
11. Network security

12. Hardware and software updates and patches
13. Backup and restore procedures
14. Requirements for setting and changing passwords
15. Credential sharing
16. Single sign-on (SSO)
17. Use of multi-factor authentication (MFA) or password-less login
18. Security codes
19. Breach reporting protocols
20. Internal protocols after data breach
21. Phishing
22. Smishing
23. Secure password use and multi-factor authentication

Training shall take the form of any of the following or a combination of the following:

1. Simulations
2. Presentations – Auditory/Visual
3. Discussions
4. Direct Instruction

Retention Time

- The personal information shall be retained by JADCO and WADA in accordance with the criteria and retention periods in Article 10 and Annex A of the ISPPPI.

Retention times can be extended in case of pending or reasonably anticipated anti-doping rule violations, investigations, or other legal proceedings.

Module	Data	Retention Periods	Remarks	Criteria
1 – Athlete			**Athlete data relevant for practical purposes and for notification purposes in the event of an ADRV. These data are not particularly sensitive.**	
Athlete (general)	Name, Date of birth, Sport Discipline and Gender	10 years as of time when Athlete is excluded from ADO's Testing program or as of time other data categories have been deleted (see, e.g. Section 6 - ADRV), whichever is later	Necessary to notify of ADRV and to keep a record of Athletes included in an ADO's Testing program. Same as above.	Necessity

	Contact information (phone number (s), email address, mailing address)	10 years as of time when Athlete is excluded from ADO's Testing program		Necessity
2 – Whereabouts* *(except for city, country, and In-Competition whereabouts information, which are needed for the Athlete				

Biological Passport - see section 7) **Whereabouts**	Whereabouts (other than city, country and In-Competition whereabouts)	12 months as of end of the whereabouts quarter for which the data was submitted	Relevant to count 3 whereabouts failures in 12 months' time.	Necessity
	Whereabouts failures (filing failures and missed tests)	10 years as of date of whereabouts failure	Relevant to count 3 whereabouts failures in 12 months' time and to other possible ADRVs. If ADRV, will also be kept as part of results management file (see section 6)	Necessity
3 – TUEs			**Destroying medical information makes it impossible for WADA/ADOs to review TUEs retrospectively after TUE has lost its validity.**	

			TUE information is largely medical and therefore sensitive. Can be relevant in case of re-Testing or other investigations Loses relevance after expiration of TUE except in case of reapplication.	
TUE	TUE certificates and rejected TUE decision forms TUE application forms and supp. med information and any other TUE info not otherwise	10 years as of date of TUE expiry/date of rejection decision 12 months from date of TUE expiry	Can be relevant in case of re-application.	Proportionality/ Necessity Proportionality/ Necessity

	expressly mentioned herein. Incomplete TUEs	12 months from date of creation		Proportionality
4 – Testing **Testing**	Doping Control Forms (DCFs)	10 years as of Sample collection date	DCFs, associated mission/Testing orders, and chain of custody documents are relevant for Athlete Biological Passport and in case of re-Testing of Samples. If ADRV, will also be kept as part of results management file (see section 6). Same as above.	Proportionality/Necessity

	Mission/Testing orders	Retained until all associated DCFs have been deleted	Same as above.	Proportionality/Necessity
	Chain of custody	10 years as of document creation date	Documentation that is incomplete or not matched to a Sample typically results from a data entry error and is discarded after a short delay for data integrity purposes.	Proportionality/Necessity Proportionality
	Incomplete Testing documentation or documentation not matched to a Sample	12 months as of document creation date		

5 – Test results/Results Management		As of Sample collection date / date of creation of relevant documents:		
	Analytical test results (incl. AAF/ATF), laboratory reports, and other associated documentation	10 years*	Necessary because of multiple violations and retrospective analysis. If ADRV, will also be kept as part of results management file (see section 6). *Subject to the criteria and requirements of the Code/International Standards, analytical data resulting from Sample analysis and other Doping Control information may, in certain circumstances, be kept beyond the applicable retention period for research and other purposes permitted by Article 6.3 of the Code. Samples and data must be processed to ensure they cannot be traced back to an athlete before being used for	Necessity Proportionality/Necessity

			such secondary purposes. 10 years is the maximum retention time for identifiable data and Samples. See the International Standard for Laboratories for details.	
6- Proceedings and Decisions (ADRV) **Decisions and Proceedings**	Sanctions and Decisions under the Code	As of date of final decision: Longer of 10 years or duration of sanction*	**Managed by disciplinary body / sports federation / ADO**. Necessary because of multiple violations and possible duration of sanctions. * Decisions (e.g. CAS decisions) can be important legal precedents and part of the public record; in such cases, ADOs may decide to retain a decision beyond the applicable retention period. Necessary because of multiple violations and possible duration of sanctions.	Necessity Proportionality/Necessity

	Relevant documentation/files (incl. AAF or whereabouts failure record, case files, laboratory and ABP documentation packages, etc.)	Longer of 10 years or duration of sanction		Necessity
7 – Athlete Biological Passport **Results**	Biological variables,	10 years as of date of match between results	Necessary because of multiple violations and to analyse or review biological variables, APMU	Necessity

	ATPF, APF, APMU reports, expert reviews, ABP documentation packages and associated laboratory documentation.	and Doping Control Form/ date of creation of relevant documents	reports, expert reviews, etc., over time. If ADRV, will also be kept as part of results management file (see section 6). Needed to support atypical/abnormal results, or to refute Athletes' claims.	
Whereabouts	Whereabouts (only city, country and In-Competition whereabouts)	10 years as of end of the whereabouts quarter for which the data was submitted		Proportionality/Necessity

Legal Basis for Data Processing

JADCO shall indicate the purpose for which personal information will be collected when receiving personal information from an athlete of athlete representative. The purposes can include one or more of the following reasons:

- Compliance with legal obligations;
- Performance of functions of a public nature in the public interest;
- Processing necessary for public health purposes;
- Fulfilment of a contract;
- Processing needed for the legitimate purposes of an organization; or
- Dealing with legal claims or processes.

Annex A

SECURITY BREACH LOG

Confidential

Details of Breach						Assessment		Notifications			
Date of Breach	No. of People Affected	Nature of Breach (availability, confidentiality, integrity)	Description of Breach	Description of Data/ Data Categories	How was breach discovered	Potential Consequences for Affected Individuals and Known Risk Factors	Remedial Action Taken/To Be Taken	Individuals Informed? If not, brief description of why not	Data Protection Authority Informed? If not,, brief description of why not.	WADA ADOs Informed?	Other governmental authorities/ organizations informed?

Annex B

INTERNAL SECURITY BREACH REPORTING FORM

Confidential

Report Date: **Security Breach Report #:**

Contact Information of Reporting Individual	
Name:	
Title and Department:	
Phone:	
Email:	

Description of Security Breach	
Date or time period during which breach occurred:	
Date and time breach discovered:	
Location of breach:	
Estimate number of individuals directly affected by the breach:	
Type(s) of individuals affected (i.e. Athlete, Athlete Support Personnel, etc.):	
Describe the systems or assets (laptop, mobile device, storage locker) affected or involved by or in the breach:	
Describe the nature and cause of the incident (provide sufficient detail):	
Describe any other details related to the breach (e.g., is this an isolated incident or the result of a systemic problem):	

Personal Information and Safeguards	
Describe what types of Personal Information are affected by the breach (i.e. name, contact information, medical history, etc):	
What was the format of the Personal Information (i.e., hard copy, electronic, etc.)?	
Describe any physical (locked cabinets, etc.), technical (i.e. encryption and encryption level, password protections, remote wiping capabilities, etc.), and legal (confidentiality agreement, etc.) safeguards in place at the time of breach:	

Containment of the Security Breach	
Describe the steps taken, if any, to contain and remediate the breach and possible harm(s) that may result from the breach:	
Describe any other proposed steps that should be taken to further mitigate and remediate the harm or adverse consequences from the breach:	

Harm/Consequences of the Breach	
Describe the possible harm(s) that may result from the breach (i.e. identify theft, breach of contractual obligations, risk of physical harm, reputational harm, etc.):	

Internal Notifications	
Who did you notify when the breach was discovered?	
Have you notified the person responsible for data protection/privacy? If yes, when?	
Have you notified any other relevant party? If yes, when?	

Annex C

Risk Assessment Matrix

Risk Assessment Matrix									
Date	Data Type	Risk	Severity	Likelihood	Risk No.	Corrective and Preventative Action	Monitoring		
							Action Taken	Severity	Occurrence

Risk Level		Identified Risks		Corrective and Preventative Action
Low Risk	1	Data Risk	Breach	Limit access
Medium Low Risk	2	Hacking	Internal	Firewall
Medium Risk	3	Data Change	External	Implement Access policy
Medium High Risk	4	Data Loss - Flood, Fire, Earthquake		Password protection
High Risk	5	Data Theft		Encryption of data - secured socket layer
		Data Interception		Tiered back-up system
				Multi-factor authenticator

Contact

Jamaica Anti-Doping Commission
Ballater Multiplex, 1 Ballater Avenue,
Kingston 10
Tel: 876-960 2416/ 876-929 3500
Toll-free: 888 429 5232
Hours: Mon- Thurs: 8:30am – 5pm
Fri: 8:30am – 4pm
Saturday: Closed
Sunday: Closed