# Table of Contents

1.0 **Introduction and Scope** ................................................................. 4  
  1.1 Definitions .................................................................................. 4  
  1.2 Key Provisions ........................................................................... 5  
    1.2.1 Key Code Provisions ............................................................... 5  
    1.2.2 Key ISTI Provisions ................................................................. 5  
    1.2.3 Key ISTUE Provisions ............................................................... 5  

2.0 **Processing Personal Information in Accordance with the ISPPI and Applicable Law** 5  
  2.1 Accountable Person ..................................................................... 5  
  2.2 Record of Processing ................................................................... 6  

3.0 **Processing Relevant and Proportionate Personal Information** .......................... 7  
  3.1 Relevant Purposes of Processing .................................................... 7  
  3.2 Accuracy ..................................................................................... 8  

4.0 **Processing Personal Information in Accordance with Law or with Consent / Ensuring Appropriate Information is Furnished to Participants and Other Persons** ................. 8  
  4.1 Consent and Notice ...................................................................... 8  
    4.1.1 Conditions for Valid Consent .................................................. 8  
    4.1.2 Required Notice ................................................................... 9  
    4.1.3 Form of Consent and Notice .................................................... 10  
  4.2 Sensitive Personal Information ....................................................... 11  
  4.3 Incapacity to Provide Consent ....................................................... 11  
  4.4 Other Valid Legal Grounds ............................................................ 11  
  4.5 Circumstances Where Notice May Be Withheld ............................ 12  

5.0 **Sharing Personal Information** .............................................................. 12  
  5.1 Third-Party Agents ...................................................................... 12  
  5.2 Anti-Doping Organizations ............................................................. 14  
  5.3 Other Third Parties ...................................................................... 15  

6.0 **Maintaining the Security of Personal Information** ........................................... 15  
  6.1 Physical and Environmental Measures .......................................... 15  
  6.2 Organizational Measures ............................................................... 16  
  6.3 Technical Measures ..................................................................... 17
6.4 Security Breach Preparedness and Response ................................................. 17
  6.4.1 Notify the Privacy Manager ................................................................. 17
  6.4.2 Assessment of Security Breach ............................................................ 18
  6.4.3 Notification to the Participant or other Persons .................................... 19
  6.4.4 Remediation ......................................................................................... 19
6.5 Risk Assessment ....................................................................................... 19

7.0 Storage and Retention ............................................................................... 20

8.0 Rights of Participants and other Persons .................................................. 21
  8.1 Notify Participants of Rights ..................................................................... 21
  8.2 Right to Access Information ..................................................................... 21
  8.3 Right to Correction or Limitation of Processing ....................................... 22
  8.4 Right to Refuse or Withdraw Consent ........................................................ 22
  8.5 Complaints ............................................................................................... 23

Template A: Form of Record of Processing ..................................................... 25
Template B: New Purpose Assessment ............................................................. 27
Template C: ADO Disclosure Request Form ................................................ 29
Template D: Sample Confidentiality Agreement ........................................... 31
Template E: Security Breach Reporting Form ............................................... 35
Template F: Security Breach Log.................................................................... 38
Template G: Risk Assessment Form ................................................................. 39
1.0 Introduction and Scope

WADA prepared these Privacy Protection Guidelines (Guidelines) to better equip Anti-Doping Organizations (ADOs) in applying appropriate and effective privacy protections to the Personal Information they Process in connection with their Anti-Doping Activities, as required by the International Standard for the Protection of Privacy and Personal Information (ISPPPI) and the World Anti-Doping Code (Code).

While not mandatory, these Guidelines set forth specific steps that ADOs can take to operationalize the rules and standards relating to the protection of Personal Information set out in the ISPPPI. The steps set out in these Guidelines map the requirements of Part Two of the ISPPPI, from Processing Personal Information in accordance with the ISPPPI and applicable law to Rights of Participants and other Persons with respect to Personal Information.

Consistent with the ISPPPI, these Guidelines aim to provide a minimum, common set of standards for the appropriate treatment of Personal Information Processed in the course of Anti-Doping Activities. In some cases, ADOs may be required by applicable laws to apply rules, standards or processes that exceed or differ from those set forth in the ISPPPI and these Guidelines.

ADOs remain responsible for ensuring that their Processing of Personal Information complies with applicable laws. Non-compliance with the ISPPPI, where such non-compliance is based on the incompatibility of applicable law and the ISPPPI, will not result in a determination of non-compliance with the Code.

These Guidelines were prepared and discussed with subject-matter experts and key stakeholders. However, as with all Guidelines issued under the Code, this document is subject to ongoing review and assessment to ensure it continues to reflect best practice, advances in technology, and emerging legal standards. WADA encourages feedback on this document and recommends that stakeholders consult WADA’s website (http://www.wada-ama.org) for the latest version.

1.1 Definitions

These Guidelines include defined terms from the Code, the International Standard for Testing and Investigations (ISTI), the International Standard for Therapeutic Use Exemptions (ISTUE), and the ISPPPI. For the purpose of these Guidelines, definitions
appearing in the Code shall be italicized and definitions appearing in an International Standard shall be underlined.

1.2 Key Provisions

Users of these Guidelines are advised to familiarize themselves with the ISPPPI, as well as key provisions of the Code and other International Standards listed below.

1.2.1 Key Code Provisions

- Article 5 Testing and Investigations
- Article 6 Analysis of Samples
- Article 7 Results Management
- Article 14 Confidentiality and Reporting

1.2.2 Key ISTI Provisions

- Article 4 Planning Effective Testing
- Article 11 Gathering, assessment, and use of intelligence
- Article 12 Investigations

1.2.3 Key ISTUE Provisions

- Article 9 Confidentiality of Information
- Annex B Template of TUE Application Form

2.0 Processing Personal Information in Accordance with the ISPPPI and Applicable Law

Article 4 of the ISPPPI sets forth a minimum set of requirements to ensure ADOs develop a basic internal governance structure and program for the appropriate treatment of Personal Information in accordance with the Code, the ISPPPI, and applicable laws.

2.1 Accountable Person

Pursuant to Article 4.5 of the ISPPPI, ADOs must designate a Person who is accountable for the ADOs’ compliance with the ISPPPI and all applicable data protection and privacy laws (for the purpose of these Guidelines, we will refer to the designated Person as the
Privacy Manager). The Anti-Doping Organization must also make the contact information for the Privacy Manager readily available to Participants.

In practice, contact information for the Privacy Manager can be provided to Participants at the same time as other required information regarding the Processing of Personal Information by ADOs (see Section 4.1 of these Guidelines for further details). The Privacy Manager should, at a minimum: (i) ensure that the ADO complies with the ISPPPI and applicable data protection and privacy laws, including ensuring that the ADO has valid legal grounds to Process Personal Information (see Section 4.0 of these Guidelines); (ii) implement appropriate policies and procedures to enable such compliance; (iii) serve as the main contact within the ADO for data privacy-related inquiries, requests, or complaints (see Section 8.0 of these Guidelines); (iv) ensure the retention times for Personal Information set out in Annex A of the ISPPPI are adhered to (see Section 7.0 of these Guidelines); and (v) oversee the implementation of appropriate safeguards for Personal Information (see Section 6.0 of these Guidelines).

2.2 Record of Processing

Pursuant to Article 4.4 of the ISPPPI, ADOs shall maintain a record of the Processing of Personal Information for which they are responsible, which documents, at a minimum:

- The purposes of the Processing;
- A description of the types of Personal Information being Processed;
- The categories of potential recipients of the Personal Information;
- The safeguards used when Personal Information is disclosed to other ADOs or Third Parties;
- The period for which the Personal Information will be stored or the criteria used to determine the storage period; and
- A general description of the technical and organizational security measures applied to the Personal Information.

A form of a record of Processing can be found as Template A. As set out in the ISPPPI, WADA will maintain a record reflecting the Processing of Personal Information within

---

1 Other titles may be appropriate depending on applicable laws and the circumstances of an ADO. ADOs should also consider whether specific requirements attach to the role of Privacy Manager or its equivalent, and whether certain functions described above need to be divided into different roles under applicable laws. For instance, depending on the size of the ADO and requirements under applicable laws, the Privacy Manager may or may not need to be exclusively dedicated to data protection (i.e., in a small organization, the Privacy Manager may also have additional duties relating to Anti-Doping Activities), or may need to be assisted by additional staff. In certain jurisdictions, ADOs may also seek the assistance of external third parties to act as a Privacy Manager or to assist the ADO with Privacy Manager-related duties.
ADAMS. In certain jurisdictions, applicable laws may prescribe additional information that must be documented in a record of processing.

3.0 Processing Relevant and Proportionate Personal Information

3.1 Relevant Purposes of Processing

Except as otherwise required by applicable law, regulation or compulsory legal process, ADOs must only Process Personal Information in order to conduct Anti-Doping Activities under the Code and the International Standards.

Section 5.3 of the ISPPPI set outs the main purposes for which ADOs Process Personal Information, namely:

A. Making determinations in respect of TUEs in accordance with the ISTUE;
B. Performing Testing, including test distribution planning and Sample collection, handling, and transport in accordance with the ISTI; and
C. Engaging in investigations and results management.

In addition to the purposes set out in A to C, above, Section 5.3 of the ISPPPI provides that the Code or applicable law may prescribe additional purposes for which Personal Information may be Processed.

For instance, the Code provides that: Samples shall be analyzed to assist an ADO in profiling relevant parameters in an Athlete’s urine, blood or other matrix (Section 6.2 of the Code); and that Samples may be de-identified or anonymized for use in research or for use in the context of quality assurance or improvement or to establish reference populations (Section 6.3 of the Code).

Finally, the ISPPPI also provides a mechanism for the Processing of Personal Information for purposes not yet provided for in the Code or the International Standards: “Anti-Doping Organizations may Process Personal Information for other specified purposes where such purposes relate exclusively to the fight against doping and are found to be relevant to that fight following an appropriately documented assessment by the Anti-Doping Organization”.

Where ADOs wish to Process Personal Information for “other specified purposes”, i.e. purposes not provided for in the Code, the International Standards, or otherwise required by law, the ISPPPI provides that an appropriate assessment must be conducted and documented to ensure such purposes relate exclusively to the fight against doping. To
help ADOs conduct and document such an assessment, a new purpose assessment template can be found as Template B.

### 3.2 Accuracy

Section 5.4 of the ISPPPI provides that Personal Information Processed by ADOs shall be accurate, complete, and kept up-to-date.

In practice, ADOs generally collect information directly from Participants and other relevant Persons, and should inform such Persons of their obligation to ensure such information is accurate, complete, and up-to-date (in particular, taking into account the responsibilities of Participants to submit accurate whereabouts information). Where possible, ADOs should provide such Persons with readily accessible means to access their own Personal Information and make required updates. For example, certain information contained within ADAMS can be updated directly by Participants or other Persons at any time.

### 4.0 Processing Personal Information in Accordance with Law or with Consent / Ensuring Appropriate Information is Furnished to Participants and Other Persons

Prior to Processing a Person’s Personal Information, an ADO should ensure that they have valid legal grounds for such Processing, which may include consent, compliance with legal obligations, performance of a public interest task, reasons of substantial public interest, fulfilment of a contract, or to protect the vital interests of a Participant or other Person.

The Privacy Manager, as described in Section 2.1 above, should be responsible for identifying the valid legal ground(s) for an ADO’s Processing of Personal Information in accordance with applicable laws.

Principle responsibility for obtaining consent or establishing another valid legal ground to Process Personal Information rests with the ADO that places the relevant Athlete in its registered Testing Pool (i.e., the custodian organization) and/or that manages the relevant Athlete’s Passport (i.e., the Passport Custodian).

### 4.1 Consent and Notice

#### 4.1.1 Conditions for Valid Consent

Where permitted under applicable laws, ADOs should obtain consent prior to collecting and otherwise Processing Participants’ or other Persons’ Personal Information.

Section 6.1 of the ISPPPI provides that consent must be informed, freely given, specific and unambiguous. Section 6.2 of the ISPPPI provides the minimum
information that must be provided to a Participant or Person in order to ensure such consent is duly informed.

For example, consent and/or notice for Doping Control-related Processing of Personal Information may be obtained by using a Doping Control Form or an Athlete Event Consent Form, templates of which can be accessed at any time on WADA’s website. An Athlete Information Notice, which may be used to obtain consent to and/or provide notice regarding the Processing of Personal Information in ADAMS and/or to supplement ADOs’ Doping Control Form, is also accessible on WADA’s website.

4.1.2 Required Notice

ADOs creating their own consent and/or notice form should ensure the form includes the information set out at Sections 6.2 and 7 of the ISPPPI, namely:

- the types of Personal Information that may be Processed;
  - At a minimum, Participants should know that their name, contact information, birthdate, gender, sport nationality, medical information (including where relevant information reflected in any TUE application), and information derived from a Sample are being Processed when a Participant is subjected to a doping test.

- the identity of the ADO collecting the Personal Information and the contact details for its Privacy Manager;

- which entities will Process the Personal Information, including other relevant ADOs located in other countries where the Participant may compete, train or travel;
  - This would be the ADO that is collecting the information, as well as any other ADO that would need the information for anti-doping purposes; WADA; Third-Party Agents to such ADOs or WADA; and, in exceptional cases, other third parties as permitted by the ISPPPI and applicable law.

  - For example, if a National Anti-Doping Organization is only the Sample Collection Authority, the Participant should know that this National Anti-Doping Organization, the Results Management Authority, the WADA-
accredited lab, the relevant National Federation and International Federation, as well as WADA may also Process his or her information.

- why the data is being Processed (i.e., the purposes of such Processing);
- the period for which the Personal Information will be retained or the criteria to determine such period;
  - At a minimum, Participants should be notified that their information will be stored by the Anti-Doping Organization in accordance with the timeframes set out in Annex A of the ISPPPI.
- the procedure to file a complaint and the possibility, if any, to submit a complaint to competent data protection authorities;
- the circumstances under which Personal Information may, where permitted by applicable law, be Publicly Disclosed;
- the Participant’s rights with respect to Personal Information under the ISPPPI and the means to exercise those rights;
- the negative Consequences (such as a violation of the Code, invalidation of Competition results, or prohibition from participating in organized sport) that could arise from a refusal to participate in Doping Controls, including Testing, and to consent, where consent is sought, to the Processing of Personal Information for Anti-Doping Activities;
- that regardless of a refusal to grant or a subsequent withdrawal of consent, the Processing of Personal Information by ADOs may be required where necessary for investigations or proceedings relating to anti-doping rule violations, or to establish, exercise or defend against legal claims relating to the ADO, the Participant, or both; and
- any other information necessary to ensure that the Processing of Personal Information remains fair.
  - This may include, for example, further detail regarding the transfer of Personal Information to other countries, including the fact that data protection and privacy laws may differ in such other countries.
  - By way of another example, this may include additional information that must be provided under applicable laws, such as information regarding cookies and other tracking technologies (where relevant to the ADO’s Processing activities).

4.1.3 Form of Consent and Notice

Written consent (and related notice) is to be preferred where practicable. However, ADOs should consider the specific circumstances of the Participant or other Person, as well as local practices, customs and the particular circumstances surrounding
the Processing of Personal Information when determining the appropriate manner of obtaining consent and providing related notices.

Where consent is not obtained in writing, ADOs should document the circumstances of the consent provided through other means. For example, an ADO that has obtained verbal consent from an Athlete to the Processing of Personal Information could create a record of the date the consent was obtained, the individual within the ADO that obtained the consent, and the information that was provided to the Athlete to ensure such consent was informed, freely given, specific and unambiguous, and that the requirements of Sections 6.2 and 7 of the ISPPPI were met.

4.2 Sensitive Personal Information

Where ADOs are relying upon consent to Process Personal Information, ADOs shall obtain explicit consent from the Participant or Person to whom the Personal Information relates where Sensitive Personal Information is Processed.

Sensitive Personal Information will include, for example, medical information supporting a TUE application, or an Athlete’s Samples and genetic information.

While the difference between an informed, specific, unambiguous consent and an explicit consent is narrow, an explicit consent requires an explicit and specific statement describing the relevant Processing of Personal Information, and an explicit action from the Person to whom the Personal Information relates consenting to such Processing. Given this heightened consent requirement, a written form of consent and related notice will be even more appropriate in the circumstances.

Where ADOs are relying on other valid legal grounds to Process Personal Information (see Section 4.4 below), there may likewise be distinct or additional requirements for the Processing of Sensitive Personal Information.

4.3 Incapacity to Provide Consent

Where ADOs are relying upon consent to Process Personal Information and a Participant is incapable of furnishing an informed consent by virtue of age, mental capacity or other legitimate reasons recognized in law, the Participant’s parent, guardian or other legal representative may furnish consent on the Participant’s behalf where permitted by applicable law. In such cases, the relationship between the Participant and the Participant’s legal representative should be verified through appropriate methods.

4.4 Other Valid Legal Grounds

In addition to consent, ADOs may Process Personal Information on the basis of other valid legal grounds under applicable anti-doping statutes, local data protection and privacy
laws, or other applicable laws, such as compliance with legal obligations, performance of a public interest task, reasons of substantial public interest, fulfillment of a contract or to protect the vital interests of the Participant or other Persons. ADOs will need to assess whether these alternative legal grounds are appropriate or necessary to rely upon based on their local laws.

Under the UNESCO *International Convention Against Doping in Sport*, State Parties to the Convention undertook to put in place appropriate measures to achieve the objectives of the Convention, including legislation, regulation, policies or administrative practices. Likewise, under the Code, ADOs set out their expectations that governments would implement such appropriate measures, including measures for cooperation and sharing of information among ADOs and WADA. ADOs may wish to consult with their local governments to discuss their legal authority to Process Personal Information in the course of their Anti-Doping Activities.

### 4.5 Circumstances Where Notice May Be Withheld

Section 7.2 of the ISPPPI provides that notice to Participants or other Persons may be delayed or suspended where providing such notice might reasonably be considered to jeopardize an anti-doping investigation or otherwise undermine the integrity of the anti-doping process.

Such measure should generally be limited to circumstances such as *No Advance Notice Testing*, investigations, and proceedings relating to anti-doping rule violations. Appropriate notice in accordance with the ISPPPI must then be provided to the Participant or other Person as soon as reasonably possible.

In the case of *Testing* or proceedings relating to anti-doping rule violations, Participants will generally receive notice as a matter of course when the *Testing* or proceedings have commenced, and should receive general notice regarding the practice of *No Advance Notice Testing* and investigations in accordance with the Code and the *International Standards*, and related anti-doping education efforts.

### 5.0 Sharing Personal Information

#### 5.1 Third-Party Agents

ADOs may share Personal Information with Third-Party Agents that Process such Personal Information for or on behalf of ADOs in the context of their Anti-Doping Activities. Common categories of Third-Party Agents include IT-service providers, laboratories, and external Doping Control Officers.

The ISPPPI requires that, prior to providing any Personal Information to such Third-Party Agents, ADOs ensure that such agents are subject to appropriate controls, including
contractual and technical controls, in order that Personal Information be appropriately protected while in the custody of the Third-Party Agent.

Appropriate contractual controls include provisions requiring that:

- Third-Party Agents comply with the ISPPPI and all applicable laws;
- Third-Party Agents only Process Personal Information on the documented instructions of the ADO and not for any other purpose;
- any staff handling Personal Information are subject to a duty of confidentiality;
- appropriate technical and organizational security measures are applied to the Personal Information Processed by the agent;
- other parties cannot be engaged by the Third-Party Agent to Process the Personal Information without prior authorization and appropriate contractual controls with those other parties being in place;
- Third-Party Agents provide prompt notification and assistance to ADO where Participants or other Persons assert rights under the ISPPPI or applicable law, or in the event of a Security Breach;
- all Personal Information be deleted or returned at the conclusion of the service or upon request; and
- Third-Party Agents make information available to the ADO to demonstrate compliance with such controls, or otherwise permit the ADO to verify such compliance through audits or other verifications.

Appropriate technical controls may include, depending on the nature of the Third-Party Agent’s access to the ADOs systems or information:
• Access restrictions (e.g. access by Doping Control Officers should be limited to the duration of an assigned Doping Control mission);
• Authentication requirements (i.e., logins, passwords, verification questions, etc.);
• Encryption, including with respect to any transmitted information; and
• Logging and monitoring of user access and activities.

5.2 Anti-Doping Organizations

The ISPPPI provides that ADOs shall not disclose Personal Information to other ADOs, except where necessary to allow the disclosing and recipient ADOs to fulfill their obligations under the Code.

Prior to sharing Personal Information with another ADO, the disclosing ADO must ensure that:

• the disclosure is in accordance with applicable data protection and privacy laws;
• the recipient ADO has established a right, authority, or need to obtain the requested Personal Information;
• the requested Personal Information is only being sent to the identified and relevant person at the recipient ADO, and that only Personal Information that is necessary to the right, authority or need established by the recipient ADO is shared; and
• the mode of communicating the Personal Information is secure.

The form provided at Template C provides a means of documenting any disclosure requests from ADOs, and better ensuring that the conditions set out above are met.

With respect to secure modes of communicating Personal Information, ADOs should consider using an encrypted or other secure file sharing system instead of email when transmitting information electronically. Secure file sharing systems typically include requirements that the recipient authenticate themselves (through a password or otherwise) and enables the disclosing party to set access limitations to the shared files.

Even where the above conditions for the disclosure of Personal Information are met, ADOs should not disclose Personal Information to other ADOs where such disclosure
would seriously compromise the status of an ongoing investigation, or where there is evidence that the recipient does not or cannot comply with the ISPPPI.

5.3 Other Third Parties

Disclosure to third parties other than Third Party Agents or ADOs is strictly limited under the ISPPPI to circumstances where such disclosures:

- are required by law, regulation or compulsory legal process;
- take place with the informed, express consent of the relevant Participant (in accordance with Section 4.1.1 of these Guidelines); or
- are necessary to assist law enforcement or governmental or other authorities in the detection, investigation or prosecution of a criminal offence or breach of the Code, provided that the Personal Information is reasonably relevant to the offence in question and cannot otherwise be reasonably obtained by the authorities.

As a matter of practice, ADOs should follow a process similar to that described in Section 5.2 above prior to disclosing Personal Information under such grounds, including ensuring that the recipient party has established a right, authority or need to receive the requested Personal Information, and that the mode of transmission of such Personal Information is secure.

6.0 Maintaining the Security of Personal Information

ADOs have a responsibility to protect the Personal Information in their possession by applying security safeguards appropriate to the sensitivity of the Personal Information, including physical, organizational, technical, environmental and other measures, to prevent a Security Breach.

6.1 Physical and Environmental Measures

Physical security measures include locked file cabinets; card access systems; physical keys; sign-in logs for visitor and other access to physical offices, data centres, or other locations where Personal Information is Processed or stored; and secure disposal of confidential physical files (e.g., shredding).

Environmental measures are measures to protect against accidental loss or destruction of Personal Information as a result of environmental factors or incidents, such as fire, flood
or power failure. For example, appropriate measures to protect against a fire may include smoke detectors and fire suppression systems.

6.2 Organizational Measures

Organizational measures include appropriate security policies and procedures; personnel training and awareness regarding such policies and procedures; ensuring personnel are bound by a contractual and/or statutory duty of confidentiality; and limiting access to Personal Information on a need-to-know basis.

With respect to limiting access, ADOs shall ensure that access to Personal Information by their own personnel occurs on a need-to-know basis consistent with their assigned role and responsibilities in the organization.

For example, an Education Manager should generally not have access to ADAMS, as he or she would not be involved in results management or investigations. A TUE manager would generally not need access to an Athlete’s whereabouts as this information is not relevant to determine if a TUE should be granted or not.

In addition, ADOs should implement processes to ensure that such access limitation occurs systematically. For example, ADOs should assign responsibility within the organization for authorizing, managing and monitoring access levels. Such authorized person(s) should ensure that whenever an individual changes job responsibilities, or an individual’s relationship with the ADO ends, any access credentials and access privileges of that individual are promptly reviewed and appropriately modified or revoked.

The ISPPPI also specifically requires that the personnel of an ADO that may have access to Personal Information be subject to an enforceable contractual or statutory duty of confidentiality. The contractual duty of confidentiality can be established by ensuring personnel sign a confidentiality agreement upon the start of any relationship between such personnel and the ADO. A template form of agreement has been provided as Template D. This template may also be used when engaging individual consultants or external TUE or other experts.

Internal policies and procedures, or applicable contractual agreements, should also contemplate disciplinary sanctions (up to and including termination) for any breach of confidentiality.

ADO personnel should receive regular training regarding internal security policies and procedures and their duties of confidentiality.
6.3 Technical Measures

Technical security measures help bolster an organization’s information security posture by protecting against human error and action. Technical security measures include:

- technical access restrictions (i.e., personnel will only have access to the electronic files, systems, or physical locations appropriate to their roles and responsibilities through technical access privilege management and authentication requirements);
- authentication requirements (e.g., unique logins and passwords which should be changed on a regular basis and appropriately complex – i.e., 8 digits or more, including letters and numbers);
- encryption, including with respect to any transmitted information;
- logging and monitoring of user access and activities to ensure access restrictions are respected and to help detect any unauthorized access or suspicious activity;
- anti-virus software and firewalls; and
- applying system upgrades and patches.

6.4 Security Breach Preparedness and Response

Security Breaches can vary in severity and impact depending on the Personal Information involved and the nature and circumstances of the breach.

For instance, the loss of a laptop by ADO personnel containing limited, non-sensitive Personal Information that was encrypted and is remotely wiped creates less risk of harm to individuals as compared to a ransomware attack by a malicious, motivated attacker affecting files containing a high volume of Sensitive Personal Information.

To help better prepare for a Security Breach, ADOs should implement an incident preparedness and response plan. This plan should address, and assign responsibility for, containment, recovery, assessment of risk, notification, and remediation measures. The incident response plan should indicate which stakeholders within the ADO, and which external advisers, as appropriate, should be notified and involved in the response to a Security Breach.

This plan should also be tailored to reflect notification and other obligations under applicable data protection and privacy laws.

6.4.1 Notify the Privacy Manager

A Security Breach, whether confirmed or suspected, should be promptly reported to the Privacy Manager. The ADO, as per the ISPPPI, must maintain appropriate
records for all Security Breaches, including the facts related to the breach, its effects and remedial actions taken.

A template Security Breach reporting form has been provided as Template E to assist ADOs and Privacy Managers in their record-keeping and notification obligations.

The reporting form or its equivalent should be completed by the Privacy Manager and/or the individual who discovers or suspects a Security Breach (in which case it should be provided to the Privacy Manager as soon as possible).

### 6.4.2 Assessment of Security Breach

Once an incident has been reported to the Privacy Manager, he or she should assess the Security Breach to determine its severity and to implement appropriate containment, notification, and remediation measures in accordance with the incident response plan.

In particular, Privacy Managers and other relevant stakeholders and advisors of the ADO will need to assess the Security Breach to determine whether it is required to notify other organizations, individuals or governmental authorities.\(^2\)

The ISPPPI provides that the ADO is required to inform the individuals concerned where the breach is likely to affect their rights and interests in a significant way.

Factors to determine whether the breach meets this trigger include:

- whether there is a risk of the individuals concerned suffering emotional or psychological distress as a result of the breach;
- whether the individuals concerned might be exposed to a risk of discrimination, identity theft, or related harms; or
- whether the individuals concerned might suffer damage to reputation or economic harm.

---

\(^2\) As mentioned in the ISPPPI, security breach notification obligations are becoming increasingly common throughout the world, and ADOs may well be required to comply with obligations that go beyond the ISPPPI in respect of Security Breach notification obligations.
6.4.3 Notification to the Participant or other Persons

Where an ADO has determined that it must notify affected Participants or other natural Persons about a Security Breach in accordance with the assessment referred to above, the notification should include the following information:

- nature of the breach;
- possible negative consequences for the Persons concerned; and
- remediation measures taken or to be taken by the ADO.

WADA also encourages ADOs to communicate and collaborate with WADA and other ADOs that may be affected by the breach or that have a relationship with the affected Persons. Where a Security Breach affects an ADO’s ADAMS account or access, ADOs are required to promptly notify WADA of the breach.

6.4.4 Remediation

Remediation measures following a Security Breach will vary depending on the cause, nature and circumstances of a Security Breach. They may involve enhanced security safeguards, disciplinary sanctions for Persons found to be the cause of the Security Breach, and increased training and awareness for personnel.

The Privacy Manager should continually monitor the enforcement and effectiveness of the incident management plan and remediation efforts, and should use lessons learned from a Security Breach to review and improve the ADO’s incident preparedness and incident response plan.

One means to enhance an ADO's incident preparedness is to maintain records regarding each Security Breach. Many data protection and privacy laws also require records to be kept in this respect. We have provided a template Security Breach log as Template F by way of an example. Note that completing an incident reporting form as described in Section 6.4.1 above will be also be helpful in maintaining records regarding a breach and completing a Security Breach log.

6.5 Risk Assessment

ADOs should regularly review and assess the risks to Personal Information in their custody and control, and should adapt their security safeguards in accordance with such risk
assessments. Where relevant, ADOs should also consider any privacy-by-design measures that could be taken to reduce risks for Participants.3

In particular, the ISPPPI requires that ADOs assess their Processing of Sensitive Personal Information and whereabouts information every three years to identify applicable risks and any measures that could be taken to reduce risks to the Participants concerned.

For example, ADOs have the discretion under the ISTI to collect different types and amounts of whereabouts information from different tiers of Athletes (see Article 4.8 of the ISTI). By way of another example, ADOs have the discretion to apply anti-doping rules to Athletes other than international or national-level Athletes, which may result in the collection of Sensitive Personal Information in respect of such Athletes. Under the ISPPPI, ADOs are required to revisit the decisions made in these respects on a regular basis to ensure the information collected is relevant and proportionate to the anti-doping objectives for such collection, and that risks for affected Athletes have been identified and mitigated to the extent possible.

A basic risk assessment form has been provided as Template G to guide ADOs in their assessments.4

7.0 Storage and Retention

ADOs must abide by the retention schedule found in Annex A of the ISPPPI. While Personal Information maintained in ADAMS is automatically deleted in accordance with this retention schedule by WADA, ADOs should implement processes to ensure that these retention times are enforced with respect to hard-copy information or information stored on other systems.

The designated Privacy Manager may do this, for example, by confirming that different departments within the ADO have complied with scheduled deletion dates, regularly reviewing such dates, and maintaining a deletion log.

---

3 Privacy-by-design considerations will be particularly relevant for ADOs developing or assessing new systems or applications to be used in the course of Anti-Doping Activities. Privacy-by-design measures would include granular control over access privileges to ensure access on a need-to-know basis; automated data deletion processes; ensuring any such system or application only requires users to input relevant and proportionate information, etc.

4 ADOs should consider whether specific requirements attach to such risk assessments, or whether additional assessments are required under applicable laws. For instance, an ADO may be required to complete a Data Protection Impact Assessment, and regulatory authorities may have issued guidance setting out the information to be included in such an assessment.
8.0 Rights of Participants and other Persons

All natural Persons have rights concerning the Processing of their Personal Information under the ISPPPI.

8.1 Notify Participants of Rights

Persons whose Personal Information is Processed by an ADO have a right to be informed of such Processing and of their rights in respect of such Processing. The information that must be provided to such Persons under the ISPPPI is set out at Section 7.1 of the ISPPPI and Section 4.1 above. As part of their notice obligations, ADOs must be responsive to questions or concerns they receive from Participants or other Persons relating to the Processing of their Personal Information.

Where Persons have rights under applicable data protection and privacy laws that are not provided for under the ISPPPI, ADOs should inform relevant Persons of such additional rights and the means of exercising such rights.

8.2 Right to Access Information

Persons have the right to receive from ADOs: (a) confirmation of whether or not the ADO Processes Personal Information relating to them; (b) the information referred to in Section 4.1 above; and (c) a copy of their Personal Information in the possession of the ADO.

The ADO should normally provide a copy of the Personal Information, and otherwise respond to an access request, within thirty (30) days of receiving a properly formulated request. The Personal Information should be provided in a readily intelligible format, and without excessive cost to the requester. Where the ADO is unable to respond to a request within such period, the ADO should supply the Person with an explanation for the delay and an estimated timeframe for its response, which should be as soon as practicable under the circumstances.

Prior to responding to an access request, the ADO should confirm the identity of the requester. The manner of conducting such verification may depend on the circumstances of the request and the ADO’s relationship with the requester. For example, an ADO may require a requester to present themselves in person in order to confirm their identity.

In other circumstances, an ADO may be able to confirm the requester’s identity through electronic means (i.e., by confirming the requester’s login credentials), or by requesting that the requester confirm certain Personal Information by phone or other means.

ADOs shall also ensure that only Personal Information regarding the requester is provided in response to the access request, and not of any other Person (i.e., by redacting Personal
Information relating to third parties within the copy of Personal Information to be provided to the requester, as appropriate).

The right of access is subject to certain exceptions under the ISPPPI. Additional exceptions may also exist under applicable data protection and privacy laws.

Under the ISPPPI, an ADO may refuse to respond favourably to an access request if doing so would conflict with other Anti-Doping Activities, such as No Advance Notice Testing or the investigation and establishment of anti-doping rule violations.

ADOs must provide reasons for refusing to provide access to the relevant Person in writing within the same thirty (30) day period.

8.3 Right to Correction or Limitation of Processing

Where a Person demonstrates that an ADO’s Processing of Personal Information is inaccurate, incomplete, or excessive, such Person may request that his or her Personal Information be rectified, amended, or deleted, or that the ADO no longer Process such Personal Information. For clarity, Processing of an excessive nature would include any Processing that is not necessary to the performance of Anti-Doping Activities by the ADO.

The ADO must comply with such a request without undue delay once the Person demonstrates the inaccuracy, incompleteness, or excessive nature of the ADO’s Processing of Personal Information. The ADO must also inform any ADOs to whom it has disclosed the Personal Information in question of any relevant correction, deletion or restriction, unless this proves impossible or involves a disproportionate effort on the part of the ADO.

8.4 Right to Refuse or Withdraw Consent

Where ADOs are relying upon consent to Process Personal Information, a Person may refuse to grant or withdraw consent to the Processing of his or her Personal Information at any time.

Participants must be notified that in these circumstances, and despite their objection, the ADO may still Process their Personal Information to fulfill obligations and responsibilities arising under the Code. Participants should also be notified that objecting to the
Processing of Personal Information can result in an anti-doping rule violation under the Code.

8.5 Complaints

Any Person may file a complaint if he or she believes that his or her Personal Information is not being Processed in accordance with the ISPPPI or applicable data protection and privacy laws.

A Person's complaint should be directed to the custodian ADO's Privacy Manager in the first instance, using the contact information made available to Participants as discussed in Section 4.1 above. If the ADO cannot satisfactorily resolve the issue directly with the Person, the ADO should then consult with WADA at privacy@wada-ama.org, who may issue recommendations to the ADO for resolving the issue.

The Person should also be notified that a complaint may be filed with a national regulator responsible for data protection in the Person's country.
List of Templates

1. Template A: Form of Record of Processing
2. Template B: New Purpose Assessment
3. Template C: ADO Disclosure Request Form
4. Template D: Sample Confidentiality Agreement
5. Template E: Security Breach Reporting Form
7. Template G: Risk Assessment Form
**TEMPLATE A: FORM OF RECORD OF PROCESSING**

The chart below may be used by ADOs to document their Processing of Personal Information in accordance with the requirements of Article 4.4 of the ISPPPI. Additional guidance and examples have been provided within the chart to assist ADOs with the completion of their records. In certain jurisdictions, applicable law may prescribe additional information that must be documented in a record of processing.

Name of individual completing form:
Date of creation:
Date of last update:

CONFIDENTIAL

<table>
<thead>
<tr>
<th>Anti-Doping Activity</th>
<th>Processing Activity</th>
<th>Types of Personal Information Collected</th>
<th>Manner/Medium of Collection and Source</th>
<th>Purposes of Collection and Use</th>
<th>Recipients of Personal Information (Internal)</th>
</tr>
</thead>
<tbody>
<tr>
<td>e.g.: Therapeutic Use Exemptions</td>
<td>e.g.: Application for TUE</td>
<td>[Provide details of all possible types of personal information, e.g. name, contact information, medical condition, medication, etc.]</td>
<td>[Provide details of manner/medium of collection, and of the source of information, for all types of personal information, e.g. online application form completed by Athlete; supporting medical information obtained from Athlete doctor, etc.]</td>
<td>[Provide details of purposes of processing for each type of data]</td>
<td>[Describe all internal recipients, e.g. administrative staff, TUE managers, etc.]</td>
</tr>
<tr>
<td>Transfers/Disclosures (external)</td>
<td>Storage Media and Location of Data</td>
<td>Retention/Destruction</td>
<td>Technical/Organizational Safeguards</td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-----------------------------------</td>
<td>-----------------------</td>
<td>-----------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Purpose of Transfer/Disclosure</td>
<td>[Insert details regarding the storage media and location of data]</td>
<td>[Insert details of the applicable retention periods and means of destruction]</td>
<td>[Provide a general description of safeguarding measures. This may include pseudonymisation, encryption, methods to ensure the ongoing confidentiality, integrity, and availability of processing, methods to restore data, etc. ADOs may also reference applicable portions of information security policies or procedures.]</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Types of Personal Information transferred/disclosed

Mechanism for Transfer/Disclosure

[Describe how information is transferred/disclosed, e.g. secure fire sharing system, disclosure via ADAMS, etc.]

Safeguards applied to Transfer/Disclosure

[Describe applicable safeguards for each mechanism of transfer, e.g. encryption, confidentiality agreements with external experts, etc.]
**TEMPLATE B: NEW PURPOSE ASSESSMENT**

The form below allows ADOs to collect relevant information in order to assess whether a proposed new purpose for the Processing of Personal Information meets the requirements of Section 5.3(d) of the ISPPPI, and may be used as a record to document such assessment. Section 5.3(d) provides that such new purpose(s) must be found to relate exclusively to the fight against doping following an appropriately documented assessment.

ADO Name: New Purpose Assessment

<table>
<thead>
<tr>
<th>1. <strong>Details of Processing</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1.1. Types of Personal Information</strong></td>
</tr>
<tr>
<td><strong>1.2. Purpose(s) of Processing</strong></td>
</tr>
<tr>
<td><strong>1.3 Categories of recipients of Personal Information (internal and external)</strong></td>
</tr>
<tr>
<td><strong>1.4 Description of safeguards</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>2. <strong>Assessment of Relevance to Fight Against Doping</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>2.1 Relevance to fight against doping</strong></td>
</tr>
<tr>
<td>2.2 Relevant Code and International Standard references</td>
</tr>
<tr>
<td>--------------------------------------------------------</td>
</tr>
<tr>
<td>2.3 Organizations or individuals consulted</td>
</tr>
</tbody>
</table>
### TEMPLATE C: ADO DISCLOSURE REQUEST FORM

The form below may be used by ADOs to evaluate disclosure requests, which it receives from other ADOs. This form allows ADO to collect relevant information in order to assess whether to grant or deny a disclosure request and it may also be used as a record to document the decision to grant or deny a request.

<table>
<thead>
<tr>
<th><strong>1. Organization Requesting Disclosure</strong></th>
<th><strong>2. Disclosure Request</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1.1. Organization</strong></td>
<td><strong>2.1. Athlete(s)/Participant(s) concerned:</strong> Name: Gender: Nationality: Sports Discipline: ADAMS ID:</td>
</tr>
<tr>
<td></td>
<td><strong>2.2. Type of information requested</strong> Brief description:</td>
</tr>
<tr>
<td><strong>1.2. Status of organization</strong></td>
<td><strong>2.3. Purpose of disclosure</strong> Related Code and International Standards: Brief description:</td>
</tr>
<tr>
<td><strong>1.3. Responsible person</strong></td>
<td><strong>2.4. Intended onward disclosures</strong> Brief description of intended disclosures (organizations/persons to which the information will be disclosed and purpose of disclosures):</td>
</tr>
</tbody>
</table>

The organization requesting disclosure hereby warrants that any information on Athletes or other Participants received from [ADO] will only be used for anti-doping purposes as described in this form, and will be returned or destroyed when no longer needed for such purposes. The requesting
organization agrees to use the information in compliance with applicable laws and regulations; the *WADA Code*; and the *International Standards*.

Date:
Name:
Title:
Organization:

Signature:
TEMPLATE D: SAMPLE CONFIDENTIALITY AGREEMENT

The ISPPPI requires that the personnel of an ADO that may have access to Personal Information be subject to an enforceable contractual or statutory duty of confidentiality. We have provided a sample confidentiality agreement, which may be used by an ADO for the purpose of complying with this requirement. This template may also be used when engaging individual consultants or other external experts. However, when Personal Information is shared with Third-Party Agents, this template is to be used in conjunction with other appropriate contractual and technical controls as set out in Section 5.1 of the Privacy Protection Guidelines. ADOs will need to review and modify this template as necessary, including to ensure it complies with applicable laws.

THIS AGREEMENT is made on [date].

BETWEEN:

1. [ADO] [provide description, including the jurisdiction where the organisation is incorporated, a registered number (if any), and business address] ("[ADO]"); and

2. [Name] of [Address] (an individual, referred to throughout as “I”).

As [employee of]/[consultant to]/[other relationship to] [ADO],

I, ____________________________________________ declare and accept that by executing this Confidentiality Agreement (the “Declaration”) I am bound by its terms.

Confidential Information

I understand that the nature of my involvement as [employee]/[consultant]/[other relationship] is such that I will have knowledge of, or become aware of, sensitive and Confidential Information (as defined below), including personal information, regarding other individuals.

I do swear or solemnly affirm that as [employee]/[consultant]/[other relationship] for [ADO], I will comply with all the requirements pertaining to the confidentiality of the information received by me or that comes to my knowledge, in any other way, in the course of my duties and tasks during and after the term of my involvement.

Except as required or permitted by law or by any competent court, regulator or governmental body having jurisdiction over [ADO]; as authorized in the course of my duties; or as expressly authorized by [ADO] in writing, I will not disclose or give to any person whatsoever, including in particular members of the media, any Confidential Information or document that comes to my knowledge or possession either directly or indirectly through the performance of my duties.

If disclosure is required or permitted by law or by any competent court, regulator or governmental body having jurisdiction over [ADO], I will consult with [ADO] reasonably in advance of such disclosure so as to permit [ADO] reasonable opportunity to review and comment on such
disclosure and, if so desired, for [ADO] to take any reasonable action to prevent or restrict such disclosure or use.

I hereby acknowledge that [ADO] has all rights to possession of and title to all Confidential Information and any copies, extracts and summaries and other Confidential Information originating during the course of my involvement as [employee]/[consultant]/[other relationship] for [ADO].

For the purpose of this Declaration, “Confidential Information” means information of a confidential nature (regardless of whether or not such information is recorded in any physical, electronic or other media and including all copies, extracts and derivations of confidential information) that is received by me or otherwise generated by me pursuant to or in connection with my involvement as [employee]/[consultant]/[other relationship] for [ADO] and that concerns the business, affairs, assets and/or interests of [ADO] or any of its affiliates, including technical data; know-how; designs; plans; specifications; methods; processes; controls; systems; trade secrets; recipes; formulae; research and development data; product complaint and testing information; computer source and object code; lists of customers and suppliers; personal information; information relating to development, engineering, manufacturing, marketing, distribution, sale or purchase of goods and/or services; accounts; financial statements; financial forecasts; business plans; budgets, estimates, sales information or other financial information; and any other information concerning the business, affairs, assets and/or interests of [ADO] or any of its affiliates which is marked as being confidential or would reasonably be expected to be kept confidential.

Injunctive Relief

I understand that breach of my obligation of confidentiality may result in possible legal action against me and in immediate termination of my involvement with [ADO]. I acknowledge, consent and agree that in the event of any such breach, [ADO] shall be entitled, in addition to any other legal remedies and damages available, to specific performance thereof and to temporary and permanent injunctive relief to restrain the violation or threatened violation of such obligations by me and persons acting for or in connection with me.

Acknowledgments

I acknowledge that this Declaration is a term and condition of my contract of [employment] OR [consultancy] OR [other] with [ADO] and therefore forms a material part of that contract. I certify and acknowledge that I have carefully read all of the provisions of this Declaration and I understand and shall fully and faithfully comply with this Declaration.

With respect to any Confidential Information covered by this Declaration, if any provision in this Declaration conflicts with any of my existing obligations with respect to such Confidential Information under my existing [employment] OR [consultancy] OR [other] agreement with
[ADO], such provision in this Declaration shall prevail to the extent of such conflict with respect to such Confidential Information.

For the avoidance of doubt, I acknowledge that the provisions of this Declaration shall survive the termination of my [employment with] OR [engagement by] OR [relationship with] [ADO].

This Declaration and the documents referred to herein, together with the existing [employment] OR [consultancy] OR [other] agreement between [ADO] and I, constitute the entire agreement and understanding of the parties with respect to the subject matter of this Declaration, and supersede all prior understandings and agreements, whether oral or written, between the parties hereto with respect to such subject matter.

**Governing Law and Jurisdiction**

This Declaration and any dispute or claim (including non-contractual disputes or claims) arising out of it or in connection with it or its subject matter or formation, shall be governed by and construed in accordance with the law of [laws of the country where the Declaration would likely need to have effect]. I irrevocably agree that the courts of [jurisdiction of country where the Declaration would likely need to have effect] shall have exclusive jurisdiction to settle any dispute or claim (including non-contractual disputes or claims) arising out of or in connection with this Declaration or its subject matter or formation. I agree that service upon me at the last address notified to [ADO] by me as my home address of any proceedings relating to this Declaration shall constitute good service upon me.

**Severability**

If any provision of this Declaration is invalid, illegal or unenforceable in any respect, such provision shall be enforced to the maximum extent possible, given the fundamental intentions of the parties when entering into this Declaration. To the extent such provision cannot be so enforced, it shall
be stricken from this Declaration and the remainder of this Declaration shall be enforced as if such invalid, illegal or unenforceable provision had never been contained in this Declaration.

Signed by:

………………………………………………………

[Director/Secretary]
For and on behalf of [ADO]

………………………………………………………

Date:

………………………………………………………

Name:

………………………………………………………

[Individual's name]

Date:

………………………………………………………
## TEMPLATE E: SECURITY BREACH REPORTING FORM

The form below may be integrated into ADOs Security Breach preparedness and response plan. The form will assist ADOs in the collection of relevant information to: (i) determine whether a Security Breach triggers notification requirements under the ISPPPI and/or applicable laws; (ii) complete any such notification with the details required to be provided under Article 9.5 of the ISPPPI; and (iii) maintain appropriate records regarding a Security Breach, as required by Article 9.5 of the ISPPPI.

### ADO Name

Security Breach Report

**CONFIDENTIAL**

**Report Date:**

<table>
<thead>
<tr>
<th><strong>Contact Information of Reporting Individual</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Name:</td>
</tr>
<tr>
<td>Title and Department:</td>
</tr>
<tr>
<td>Phone:</td>
</tr>
<tr>
<td>Email:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Description of Security Breach</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Date or time period during which breach occurred:</td>
</tr>
<tr>
<td>Date and time breach discovered:</td>
</tr>
<tr>
<td>Location of breach:</td>
</tr>
<tr>
<td>Estimate number of individuals directly affected by the breach:</td>
</tr>
<tr>
<td>Type(s) of individuals affected (i.e. Athlete, Athlete Support Personnel, etc.):</td>
</tr>
<tr>
<td>Describe the systems or assets (laptop, mobile device, storage locker) affected or involved by or in the breach:</td>
</tr>
</tbody>
</table>
Describe the nature and cause of the incident (provide sufficient detail):

<table>
<thead>
<tr>
<th>Describe any other details related to the breach (e.g., is this an isolated incident or the result of a systemic problem):</th>
</tr>
</thead>
</table>

### 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:
<table>
<thead>
<tr>
<th>Containment of the Security Breach</th>
</tr>
</thead>
<tbody>
<tr>
<td>Describe the steps taken, if any, to contain and remediate the breach and possible harm(s) that may result from the breach:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Harm/Consequences of the Breach</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Internal Notifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Who did you notify when the breach was discovered?</td>
</tr>
<tr>
<td>Have you notified the person responsible for data protection/privacy? If yes, when?</td>
</tr>
<tr>
<td>Have you notified IT? If yes, when?</td>
</tr>
<tr>
<td>Have you notified any other relevant party? If yes, when?</td>
</tr>
</tbody>
</table>
The chart below may be integrated into ADOs Security Breach preparedness and response plan. The chart will assist ADOs (and specifically, persons designated as accountable for ADOs' compliance with ISPPPI and applicable data protection and privacy laws) in the collection of relevant information to maintain appropriate records regarding a Security Breach, as required by Article 9.5 of the ISPPPI.

**CONFIDENTIAL**

<table>
<thead>
<tr>
<th>ADO name:</th>
<th>Date:</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Details of breach</strong></td>
<td><strong>Assessment</strong></td>
</tr>
<tr>
<td>Date of breach</td>
<td>No. people affected</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## TEMPLATE G: RISK ASSESSMENT FORM

The form below allows ADOs to collect relevant information in order to assess the proportionality and risks of their Processing of whereabouts information and Sensitive Personal Information, and to determine whether any measures could be taken to reduce any such risks to the Participants concerned.

ADO name

CONFIDENTIAL

<table>
<thead>
<tr>
<th><strong>Contact Information of Individual Completing Form</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Name:</td>
</tr>
<tr>
<td>Title and Department:</td>
</tr>
<tr>
<td>Phone:</td>
</tr>
<tr>
<td>Email:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Description/Proportionality of the Processing</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Describe the nature and purposes for the Processing (describe what the benefits of the processing for ADO or anti-doping programs more broadly will be; what the intended effects on individuals is; and include any relevant references to the Code, International Standards, guidelines or other documentation)</td>
</tr>
</tbody>
</table>

| Describe the specific types of whereabouts or Sensitive Personal Information involved: |

| Describe how the Processing achieves the purposes of the Processing (include an assessment of any specific factors to consider in determining whether to collect whereabouts information or Sensitive Personal Information under the Code or International Standards) |
## Identify and Assess Risks

<table>
<thead>
<tr>
<th>Describe the source and nature of risks/potential impact on individuals</th>
<th>Likelihood of harm (e.g., remote, possible, probable)</th>
<th>Severity of harm (e.g. minimal, significant or severe)</th>
<th>Overall risk (e.g. low, medium or high)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## Mitigation Measures

<table>
<thead>
<tr>
<th>Risk</th>
<th>Options to mitigate risk(^5)</th>
<th>Residual risk (e.g., low, medium or high)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## Consultations with relevant stakeholders

Describe any stakeholder consultations conducted:

---

\(^5\) List any safeguards applied to the Personal Information; measures to ensure only necessary Personal Information is Processed; type of notice provided or consent obtained to demonstrate acceptance of risk; access controls, etc.)