Privacy Impact Assessment Summary

1. Name of the Program

Abuse-Free Sport Registry (the "**Registry**")

2. Background

Abuse-Free Sport is the program created by the Sport Dispute Resolution Centre of Canada ("**SDRCC**") according to the mandate it received from the Government of Canada, for preventing and addressing maltreatment in sport (the "**Mandate**"). This mandate is in addition to the SDRCC's existing mandate pursuant to the *Physical Activity and Sport Act* of "provid[ing] to the sport community a) a national alternative dispute resolution service for sport disputes; and b) expertise and assistance regarding alternative dispute resolution."

For its part, the objective of the Universal Code of Conduct to Prevent and Address Maltreatment in Sport (the "**UCCMS**") is to advance "a respectful sport culture that delivers quality, inclusive, welcoming and safe sport experiences" and, more specifically, to protect individuals participating in sport in Canada.

The UCCMS and related processes are implemented by the Office of the Sport Integrity Commissioner ("**OSIC**"), a functionally independent division of the SDRCC.

At present, the structure requires that each participating sport organization ("**Adopting Organizations**") implement the UCCMS with its individual members and identified participants ("**Participants**"), as set out in the service agreements entered into with the SDRCC (the "**Signatory Agreement**"). Participants sign a consent form, under which they agree to be subject to the UCCMS, its related processes, which may include the use and disclosure of their information, and the jurisdiction of the Abuse-Free Sport Program.

3. Description

The Registry is a searchable database of Participants whose eligibility to participate in sport has in some way been restricted due to provisional measures and/or sanctions imposed, for purposes of carrying out the objectives of the UCCMS, the Physical Activity and Sport Act, Abuse-Free Sport and the Mandate, in accordance with applicable laws (the "**Objectives**").

The OSIC is in charge of maintaining and updating the Registry.

The Registry aims to record and disclose key information relating to Participants whose eligibility to participate in sport has been restricted in line with matters under

the UCCMS. In other words, the objective of the Registry is to protect sport participants by making relevant information available. By making this information available, Adopting Organizations, organizations and the public can conduct background checks, due diligence or other verification on potential participants before deciding whether to permit their participation in sports, for instance.

The Registry includes three levels of access:

1) **Information accessible to the public as a whole ("Public Level"):** At this level, the Registry is accessible through a public website.

2) **Information accessible to Adopting Organizations ("Adopting Organization Level")**: Designated representatives of the Adopting Organization have access to this level of the Registry, using a unique individualized username and password with two-factor authentication. Consultation is limited to a need-to-know basis and subject to contractual obligations by the Adopting Organizations.

3) **Information accessible to the Abuse Free Sport ("AFS Level")**: This level is only accessible by authorized agents of Abuse-Free Sport, on a need-to-know basis, for the purpose of carrying out the Objectives.

The Registry represents a complete and effective response to the disclosure of information requirements under the UCCMS per its underlying principles to prevent and redress maltreatment. In so finding, the Registry represents the least restrictive impact on the privacy interests of Participants to achieve the Objectives, including the necessary and important mandate of the SDRCC in fostering safer sport environments in Canada. In short, the SDRCC asserts that the 'cost' of participating in sport Canada is the necessary term that if someone is alleged to have contravened or has contravened the UCCMS and their participation in sport is to be consequently restricted, their information may be publicly disclosed in order to protect other participants at every level and every context of sports.

4. Authority

- The Mandate
- *Physical Activity and Sport Act*
- UCCMS, in particular section 8.1
- Signatory Agreement and Participants' consent forms

5. Risks to Safety of Participants in Sport

There is a heightened risk of maltreatment in sport given the nature of the interactions that take place between individuals involved, for instance coaches,

volunteers and athletes, as well as given the involvement of minors and youth in sport roles. The Registry aims to address the following risks, among others:

- Exploitation of fiduciary relationships
- Forms of power imbalance
- Risk of re-offending

Regarding the latter, not only does sport present with heightened risk for maltreatment, but the segmentation of sport within Canada makes it so that individuals who have been sanctioned for maltreatment can move laterally to another jurisdiction or sport opportunity to evade sanctions and possibly victimize more individuals.

6. Risk Analysis by Privacy Principles

6.1. Limited and Direct Collection

The collection of personal information is limited to what is necessary to carry out the Objectives. This collection is primarily undertaken through the complaint management process of the OSIC ("**Complaint Management Process**"), which has a particular focus on procedural fairness.

As the case may be, when the information is obtained from an independent process of Adopting Organizations, specific requirements apply regarding due process, as specified in the Signatory Agreement.

6.2. Limiting Use, Retention and Disclosure of Information

Each access level of the Registry includes information limited to what is necessary for the purposes of the Objectives.

For instance, the Public Level includes information on Participants subject to some sanctions and provisional measures in relation to restrictions or ineligibility to participate in sport, for the duration such sanctions or provisional measures are in effect.

At the Adopting Organization Level of the Registry, the information may be more detailed or exhaustive to the extent necessary to implement the sanctions and provisional measures and are included for their period of application.

At the AFS Level of the Registry, to effectively carry out its mandate, the OSIC must retain records relating to a complaint and corresponding ruling

for a period that extends beyond the length of the sanction in question. The records are to be retained until the Participant is 80 years old. For example, the records may be relevant if the Participant in question re-offends but the sanction has expired. This is particularly important if there is continued re-offence.

Special considerations are applied regarding information of minors or vulnerable individuals.

6.3. Retention of Data and Disposal

The OSIC is responsible for ensuring timely data updates and data removal on the Registry. Such function is programmed, as well as a “purge” function when it is required to dispose of the data.

6.4. Informed Consent

Consent is obtained through the consent form. Participants are now provided with context and an information session prior to signing. The objectives supporting the collection, use and disclosure of their personal information are described in a comprehensive and transparent manner.

The consent form fosters openness and transparency.

6.5. Accuracy and Individual Access

Accuracy is ensured through the application of a rigorous Complaint Management Process and procedural fairness.

The SDRCC and OSIC’s Protection of Privacy Policy, which is referred to in the consent form and publicly available, includes information regarding individual’s access to their record, possibility of requesting correction of such information (subject to the applicable processes) and contact information of the person responsible for receiving complaints regarding privacy matters, among other things.

6.6. Safeguards as to the Registry

Confidentiality safeguards are taken every step.

Technological, operational and physical safeguards are employed, including the following:

- Operational: employee training; appropriate policies and protocols regarding issues such as data mapping, defined uses and

disclosures, data retention, outsourcing, password policy, patch management.

- Technical and physical: please refer to Appendix A of this document for a summary of the technology risk/threat assessment carried out in relation to the Registry.

6.7. Direct Collection and Purpose Identification

Please refer to sections 2 to 4 of this document.

Information is obtained from Participants, witnesses (including victims), and any other relevant third parties mainly through the Complaint Management Process.

6.8. Openness

Openness is achieved through the implementation and disclosure of the consent form, the UCCMS and the Abuse-Free Sport Policies and Procedures.

All relevant documents are available online, in both official languages and respecting accessibility standards.

6.9. Accountability

As mentioned previously, SDRCC has a Protection of Privacy Policy, the latter being also applicable to the activities of the OSIC.

As per this Policy, the Privacy Officer must ensure that the policy is compliant with applicable privacy laws and regulations, monitor the SDRCC's compliance and respond to privacy complaints and breaches. His contact information is available in the policy, which is accessible online. An individual may request access to their information, as provided under the Protection of Privacy Policy.

The OSIC also has complementary Policies and Procedures.

Appendix A

Technology Risk/Threat Assessment (Summary)

For the purpose of this PIA summary, events or failures which may cause temporary unavailability of the Registry are not considered a threat. The focus of this analysis is to identify the following risks/threats:

1) Disclosure of personal data not intended for publication;
2) Error in personal data intended for publication;
3) Security breach of the servers hosting personal data.

1. Disclosure of personal data not intended for publication

Data showing on the Registry at the Public Level is pulled from a dataset containing some personal data that is not disclosed at the Public Level of the Registry. A need was identified to ensure that the portion of the dataset that is not to be disclosed publicly remains fully protected.

Mitigation measures include:

a) Only one authorized super-user account with two-factor authentication can make changes to the webpage hosting the Registry at the Public Level;

b) Access to the host server of the public page of the Registry is secure via the following means:
   - Technology:
     - Primary Firewall
     - IDS/IPS
     - NDR
     - SIEM
     - EDR
     - BOT Protection
     - Site not indexed by search engines.
   - Encryption:
     - Data is stored encrypted at rest and in transit.
   - Remote Access:
     - VPN for Management with 2FA
     - 2FA for all admin accounts
     - Application Firewall
     - Web Application Firewall
     - Access Restrictions.
   - Storage:
     - Database/Backups stored on non-public networks.

c) A maximum of three (3) specialized database administrators may mark a record for publication. No single administrator may alone make a record

public unless a specialized administrator approves its publication. A popup warning appears on the administrator screen, prompting a manual confirmation by the specialized administrator that the record is marked to be made public. A log is kept of who requested the record be made public and who approved it.

d) A single database administrator is able to remove a record from the public domain and a log is kept of who removed it.

2. Error in personal data intended for publication

Human errors may occur in data entry, causing inaccuracies in the personal information that is publicly disclosed on the Registry.

a) A maximum of three (3) specialized database administrators may mark a record for publication. No single administrator may alone make a record public unless a specialized administrator approves its publication. A popup warning appears on the administrator screen, prompting a manual confirmation by the specialized administrator that the record is marked to be made public. A log is kept of who requested the record be made public and who approved it.

b) Each administrator must verify the accuracy of the data entry prior to allowing the record to be made public.

c) At the Public Level, the Registry webpage and server have read-only access to the Registry database and cannot make changes to any of the information.

3. Security breach of the servers hosting personal data

The servers hosting the Registry data containing personal information may be targeted by viruses or malicious attacks. This could cause for information that is not intended to be public to be accessed by unauthorized users.

Mitigation measures include:

a) Service provider hired to develop, host and maintain the servers is a consultant specialized in data security who is a Certified Ethical Hacker, Computer Forensic Expert and Penetration Tester.

b) Night vulnerability scans are run with monthly penetration tests.

c) Access to the host server of the public page of the Registry is secure via the following means:
    - Technology:
        - Primary Firewall

        - IDS/IPS
        - NDR
        - SIEM
        - EDR
        - BOT Protection
        - Site not indexed by search engines.
    - Encryption:
        - Data is stored encrypted at rest and in transit.
    - Remote Access:
        - VPN for Management with 2FA
        - 2FA for all admin accounts
        - Application Firewall
        - Web Application Firewall
        - Access Restrictions.
    - Storage:
        - Database/Backups stored on non-public networks.
        - Network monitor tools (Ram, CPU, Patch, Load, etc.)
        - All content scanned with AV/AM software actively
        - Backup stored locally and offsite (all in Canada)
        - Card key access and biometrics required to access physical premises where servers and redundancy servers are located.

If any such threat is detected at any point in time, the immediate measure is to take down the public site until the full database is reviewed and assessed for accuracy and safety.