Résumé de l'Évaluation des facteurs relatifs à la vie privée

1. Nom du programme

Registre de Sport Sans Abus (le « **Registre** »)

2. Contexte

Sport Sans Abus est le programme créé par le Centre de règlement des différends sportifs du Canada (le « **CRDSC** »), conformément au mandat qui lui a été conféré par le gouvernement du Canada, pour prévenir et contrer la maltraitance dans le sport (le « **Mandat** »). Ce mandat s'ajoute au mandat actuel du CRDSC en application de la *Loi sur l'activité physique et le sport* de « fournir à la communauté sportive un service pancanadien de règlement extrajudiciaire des différends sportifs ainsi qu'une expertise et une assistance en la matière. »

L'objectif du Code de conduite universel pour prévenir et contrer la maltraitance dans le sport (le « **CCUMS** ») est quant à lui de promouvoir « une culture sportive respectueuse qui offre des expériences sportives de qualité, inclusives, accueillantes et sécuritaires » et, plus particulièrement, de protéger les personnes qui font du sport au Canada.

Le CCUMS et les processus s'y rapportant sont mis en œuvre par le Bureau du Commissaire à l'intégrité dans le sport (« **BCIS** »), une division fonctionnellement indépendante du CRDSC.

À l'heure actuelle, la structure en place requiert que chaque organisation sportive participante (« **Organismes ayant adopté le CCUMS** ») mette en œuvre le CCUMS auprès de ses membres individuels et des participants identifiés (« **Participants** »), tel que prévu aux ententes de service conclues avec le CRDSC (l'« **Entente des Signataires** »). Les Participants signent un formulaire de consentement en vertu duquel ils acceptent d'être soumis au CCUMS, aux processus s'y rapportant, qui peuvent inclure l'utilisation et la divulgation de leurs renseignements, et à la juridiction du Programme Sport Sans Abus.

3. Description

Le Registre est une base de données consultable au sujet de Participants dont l'admissibilité à participer au sport a été restreinte d'une manière ou d'une autre en raison de mesures provisoires et/ou de sanctions imposées aux fins de la réalisation des objectifs du CCUMS, de la *Loi sur l'activité physique et le sport*, de Sport Sans Abus et du Mandat, conformément aux lois applicables (les « **Objectifs** »).

Le BCIS est responsable de maintenir et de mettre à jour le Registre.

Le Registre vise à contenir et à divulguer des informations clés au sujet de Participants dont l'admissibilité à participer au sport a été restreinte en lien avec l'application du CCUMS. En d'autres mots, l'objectif du Registre consiste à protéger les participants sportifs en rendant l'information pertinente disponible. En rendant cette information disponible, les Organismes ayant adopté le CCUMS, les organisations et le public peuvent faire des vérifications d'antécédents, des diligences appropriées ou d'autres vérifications sur des Participants potentiels avant de décider s'ils permettent leur participation au sport, par exemple.

Le Registre inclut trois niveaux d'accès :

1) **Information accessible au public (« Niveau public ») :** À ce niveau, le Registre est accessible par l'entremise d'un site Web public.

2) **Information accessible aux Organismes ayant adopté le CCUMS (« Niveau des Organismes ayant adopté le CCUMS ») :** Des représentants désignés des Organismes ayant adopté le CCUMS ont accès à ce niveau du Registre par l'entremise d'un nom d'usager individualisé et d'un mot de passe uniques, avec authentification à deux facteurs. La consultation est limitée selon le principe du besoin de savoir et fait l'objet d'obligations contractuelles auxquelles est soumise l'Organisation ayant adopté le CCUMS.

3) **Information accessible pour Sport Sans Abus (« Niveau de Sport Sans Abus ») :** Ce niveau est seulement accessible aux représentants autorisés de Sport Sans Abus, selon le principe du besoin de savoir, dans la mesure nécessaire pour la réalisation des Objectifs.

Le Registre représente une solution complète et efficace en lien avec les exigences en matière de divulgation de renseignements en vertu du CCUMS, à la lumière des principes sous-jacents nécessaires pour prévenir et contrer la maltraitance. Par conséquent, le Registre représente la mesure la moins restrictive sur les intérêts des Participants en matière de vie privée pour l'atteinte des Objectifs, y compris le mandat nécessaire et important du CRDSC de favoriser des milieux sportifs plus sécuritaires au Canada. En résumé, le CRDSC soutient que le « coût » de participer aux sports au Canada implique nécessairement que si on allègue qu'une personne a contrevenu au CCUMS ou si elle y a contrevenu et que sa participation au sport est conséquemment limitée, ses renseignements peuvent être divulgués publiquement afin de protéger les autres participants à tous les niveaux et dans tous les contextes du sport.

4. Autorité

- Le Mandat
- La *Loi sur l'activité physique et le sport*
- Le CCUMS, en particulier l'article 8.1
- L'Entente des Signataires et les formulaires de consentement des Participants

5. Risques à la sécurité des Participants dans le sport

Il existe un risque accru de maltraitance dans le sport en raison de la nature des interactions qui ont lieu entre les individus qui y participent, par exemple, les entraîneurs, les bénévoles et les athlètes, de même que compte tenu de la participation de mineurs et de jeunes dans des rôles sportifs. Le Registre vise, entre autres, à contrer les risques suivants :

- Exploitation d'un rapport de fiduciaires
- Formes de déséquilibre des pouvoirs
- Risque de récidive

En ce qui a trait à ce dernier élément, non seulement le sport présente-t-il un risque accru de maltraitance, mais la segmentation du sport au Canada fait en sorte que les individus qui ont été sanctionnés pour maltraitance peuvent se déplacer latéralement vers une autre juridiction ou une autre opportunité en matière de sports afin d'échapper aux sanctions et potentiellement victimiser d'autres individus.

6. Analyse du risque selon les facteurs relatifs à la vie privée

6.1. Collecte limitée et directe

La collecte de renseignements personnels se limite à ce qui est nécessaire pour la réalisation des Objectifs. Cette collecte s'effectue principalement par l'entremise du Processus de gestion des plaintes du BCIS (le « **Processus de gestion des plaintes** »), qui met particulièrement l'accent sur l'équité procédurale.

S'il y a lieu, lorsque l'information est obtenue dans le cadre d'un processus indépendant d'une Organisation ayant adopté le CCUMS, des exigences particulières s'appliquent en ce qui a trait à la procédure équitable, telles que spécifiées dans l'Entente des Signataires.

6.2. Utilisation, rétention et divulgation des renseignements limités

Chaque niveau d'accès du Registre comprend les renseignements limités à ce qui est nécessaire pour les fins des Objectifs.

Par exemple, le Niveau public comprend des renseignements sur les Participants qui sont sujets à certaines sanctions et mesures provisoires en relation avec des restrictions ou une inadmissibilité à participer au sport, pour la durée pendant laquelle ces sanctions et mesures provisoires sont en vigueur.

Au Niveau des Organismes ayant adopté le CCUMS, l'information peut être plus détaillée ou exhaustive dans la mesure nécessaire pour mettre en œuvre les sanctions et les mesures provisoires et elle est incluse pour leur période d'application.

Au Niveau de Sport Sans Abus, dans le but d'exécuter son mandat de manière efficace, le BCIS doit conserver les dossiers qui se rapportent aux plaintes et aux décisions correspondantes pour une période qui va au-delà de la durée de la sanction en question. Les dossiers doivent être conservés jusqu'à ce que le Participant ait 80 ans. Par exemple, les dossiers peuvent être pertinents si le Participant en question commet une nouvelle violation, mais que la sanction a pris fin. Ceci est particulièrement important pour les cas de récidive.

Des considérations spéciales sont appliquées en ce qui concerne les renseignements des mineurs ou de personnes vulnérables.

6.3. Conservation et suppression des données

Le BCIS est responsable d'assurer la mise à jour opportune des données et la suppression des données sur le Registre. Une telle fonction est programmée, de même qu'une fonction de « purge » lorsqu'elle est nécessaire pour supprimer les données.

6.4. Consentement éclairé

Le consentement est obtenu par l'entremise du formulaire de consentement. Les Participants ont désormais accès au contexte et à une séance d'information avant de signer. Les objectifs au soutien de la collecte, de l'utilisation et de la divulgation de leurs renseignements personnels sont décrits de manière détaillée et transparente.

Le formulaire de consentement favorise l'ouverture et la transparence.

6.5. Exactitude et accès

L'exactitude est assurée par l'application d'un Processus de gestion des plaintes rigoureux et de l'équité procédurale.

La Politique de protection des renseignements personnels du CRDSC et du BCIS à laquelle on réfère dans le formulaire de consentement et mise à la disposition du public, comprend de l'information au sujet des droits d'accès d'une personne à son dossier, de la possibilité de demander la correction des renseignements (sous réserve des processus applicables) et des coordonnées de la personne responsable de recevoir les plaintes en ce qui concerne les renseignements personnels, entre autres choses.

6.6. Mesures de protection relatives au Registre

Des mesures de protection en matière de confidentialité sont prises à chaque étape.

Des mesures de protection sur les plans technique, opérationnel et physique sont mises en œuvre, notamment les suivantes :

- Sur le plan opérationnel : formation des employés, politiques et protocoles appropriés relativement aux enjeux tels que le mappage des données, utilisations et divulgations définies, rétention des données, sous-traitance, politique en matière de mots de passe et gestion des correctifs.

- Sur les plans technique et physique : veuillez vous reporter à l'Annexe A de ce document pour un résumé de l'évaluation de la technologie et des risques qui a été réalisée en lien avec le Registre.

6.7. Collecte directe et définition des objectifs

Veuillez vous référer aux sections 2 et 4 de ce document.

Les renseignements sont obtenus auprès des Participants, des témoins (y compris les victimes) et de tout autre tiers concerné, principalement dans le cadre du Processus de gestion des plaintes.

6.8. Transparence

La transparence est réalisée par la mise en œuvre et la communication du formulaire de consentement, du CCUMS et des politiques et procédures de Sport Sans Abus.

Tous les documents pertinents sont disponibles en ligne, dans les deux langues officielles et respectent les normes d'accessibilité.

6.9. Responsabilité

Comme mentionné précédemment, le CRDSC possède une politique de protection des renseignements personnels qui s'applique également aux activités du BCIS.

En vertu de cette politique, l'agent de la protection de la vie privée doit s'assurer que la politique respecte les lois et règlements applicables en matière de vie privée, surveiller la conformité du CRDSC et répondre aux plaintes ou violations en matière de vie privée. Ses coordonnées sont disponibles dans la politique, qui est accessible en ligne. Une personne peut demander l'accès à ses renseignements dans la mesure prévue dans la Politique de protection des renseignements personnels.

Le BCIS possède également des politiques et procédures complémentaires.

Annexe A

Évaluation des risques/menaces technologiques (Résumé)

Aux fins de ce résumé de l'EFVP, les événements ou défaillances susceptibles de provoquer une indisponibilité temporaire du Registre ne sont pas considérés comme une menace. L'objectif de cette analyse est d'identifier les risques/menaces suivants :

1) Divulgation de données personnelles non destinées à la publication;
2) Erreur dans les données personnelles destinées à la publication;
3) Faille de sécurité des serveurs hébergeant les données personnelles.

1. Divulgation de données personnelles non destinées à la publication

Les données affichées dans le Registre au Niveau public sont extraites d'un ensemble de données contenant certaines informations personnelles qui ne sont pas divulguées au Niveau public du Registre. Un besoin a été identifié de protéger les données qui ne doivent pas être divulguées publiquement.

Les mesures d'atténuation comprennent :

a) Un seul compte super-utilisateur autorisé, avec une authentification à deux facteurs, peut apporter des modifications à la page hébergeant le Registre au Niveau public ;

b) L'accès au serveur hôte de la page publique du Registre est sécurisé par les moyens suivants :
   - Technologie :
     - Pare-feu principal
     - IDS/IPS (systèmes de détection et de prévention contre les intrusions)
     - NDR (détection de réseaux et réponse)
     - SIEM (gestion des informations et des événements de sécurité)
     - EDR (détection et réponse aux terminaux)
     - Protection contre les robots (ou bots)
     - Site non indexé par les moteurs de recherche.
   - Cryptage :
     - Les données sont cryptées au repos et en transit.
   - Accès à distance :
     - VPN pour la gestion avec authentification à 2 facteurs
     - Authentification à 2 facteurs pour tous les comptes administrateurs
     - Pare-feu d'application
     - Pare-feu d'application Web
     - Restrictions d'accès.

- Stockage :
  - Base de données/sauvegardes stockées sur des réseaux non publics.

c) Un maximum de trois (3) administrateurs spécialisés de bases de données peut marquer une fiche pour publication. Aucun administrateur ne peut à lui seul rendre une fiche publique à moins qu'un administrateur spécialisé n'approuve sa publication. Une fenêtre apparaît sur l'écran de l'administrateur, invitant l'administrateur à confirmer manuellement que la fiche est bien marquée pour être rendue publique. Un journal est tenu indiquant qui a demandé que la fiche soit rendue publique et qui l'a approuvée.

d) Un seul administrateur de la base de données peut retirer une fiche du domaine public et un journal est tenu indiquant qui l'a retirée.

2. Erreur dans les données personnelles destinées à la publication

Des erreurs humaines peuvent survenir lors de la saisie de données, entraînant des inexactitudes dans les informations personnelles divulguées publiquement sur le Registre.

Les mesures d'atténuation comprennent :

a) Un maximum de trois (3) administrateurs spécialisés de bases de données peut marquer une fiche pour publication. Aucun administrateur ne peut à lui seul rendre une fiche publique à moins qu'un administrateur spécialisé n'approuve sa publication. Une fenêtre apparaît sur l'écran de l'administrateur, invitant l'administrateur à confirmer manuellement que la fiche est bien marquée pour être rendue publique. Un journal est tenu indiquant qui a demandé que la fiche soit rendue publique et qui l'a approuvée.

b) Chaque administrateur doit vérifier l'exactitude des données saisies avant d'autoriser que la fiche soit rendue publique.

c) Au Niveau public, la page Web et le serveur du Registre n'ont un accès à la base de données du Registre qu'en lecture seule et ne peuvent modifier aucune des informations.

3. Faille de sécurité des serveurs hébergeant des données personnelles

Les serveurs hébergeant les données du Registre contenant des informations personnelles peuvent être la cible de virus ou d'attaques malveillantes. Des utilisateurs non autorisés pourraient ainsi avoir accès à des informations qui ne sont pas destinées à être rendues publiques.

Les mesures d'atténuation comprennent :

a) Le consultant engagé pour développer, héberger et entretenir les serveurs est un spécialiste en sécurité informatique qui est un pirate éthique certifié, un expert en criminalistique informatique et un testeur d'intrusion.

b) Des analyses de vulnérabilité nocturnes sont effectuées avec des tests d'intrusion mensuels.

c) L'accès au serveur hôte de la page publique du registre est sécurisé par les moyens suivants :
    - Technologie :
        - Pare-feu principal
        - IDS/IPS (systèmes de détection et de prévention contre les intrusions)
        - NDR (détection de réseaux et réponse)
        - SIEM (gestion des informations et des événements de sécurité)
        - EDR (détection et réponse aux terminaux)
        - Protection contre les robots (ou bots)
        - Site non indexé par les moteurs de recherche.
    - Cryptage :
        - Les données sont cryptées au repos et en transit.
    - Accès à distance :
        - VPN pour la gestion avec authentification à 2 facteurs
        - Authentification à 2 facteurs pour tous les comptes administrateurs
        - Pare-feu d'application
        - Pare-feu d'application Web
        - Restrictions d'accès.
    - Stockage :
        - Base de données/sauvegardes stockées sur des réseaux non publics
        - Outils de surveillance réseau (Ram, CPU, Patch, Load, etc.)
        - Tout le contenu analysé activement avec le logiciel AV/AM
        - Sauvegarde stockée localement et hors site (entièrement au Canada)
        - Accès par carte-clé et données biométriques requis pour accéder aux locaux physiques où se trouvent les serveurs et les serveurs de redondance.

Si une telle menace est détectée à un moment ou à un autre, la mesure immédiate consiste à fermer le site public jusqu'à ce que la base de données complète soit examinée et évaluée du point de vue de l'exactitude et de la sécurité.