Programme de soutien à la mise en œuvre du Code 2021

Lignes directrices pour le Standard international pour la protection des renseignements personnels

WORLD ANTI-DOPING AGENCY
play true

LIGNES DIRECTRICES POUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

Table des matières

LIGNES DIRECTRICES POUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS 2
BIENVENUE AUX LIGNES DIRECTRICES POUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS 5
Le contexte 5
Au-delà du SIPRP 5
Comment utiliser les Lignes directrices 6
RÉSUMÉ 8
SECTION 1 : ÉLABORATION D'UN PROGRAMME DE PROTECTION DES RENSEIGNEMENTS PERSONNELS 11
CHAPITRE 1 : COMMENT FAIRE DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS UNE PRIORITÉ 12
1. S'assurer que la protection des renseignements personnels fasse partie des objectifs clés de votre organisation 12
2. Création d'un rôle, d'une équipe ou d'un service de protection des renseignements personnels 13
CHAPITRE 2 : LES FONDEMENTS DE VOTRE PROGRAMME DE PROTECTION DES RENSEIGNEMENTS PERSONNELS 17
1. Comprendre les principes relatifs aux pratiques loyales en matière d'information 17
2. Comprendre le rôle du SIPRP dans votre programme de protection des renseignements personnels. 19
3. Intégrer les lois sur la protection des données et de la vie privée 20
CHAPITRE 3 : COMMENT STRUCTURER VOTRE PROGRAMME DE PROTECTION DES RENSEIGNEMENTS PERSONNELS 23
1. Identifier votre structure de gouvernance 23

2. Attribuer les rôles et les responsabilités 24

3. Définir les exigences auxquelles l'organisme doit répondre 25

4. Les documenter et les rendre obligatoires 25

SECTION 2 : MISE EN ŒUVRE DE VOTRE PROGRAMME DE PROTECTION DES RENSEIGNEMENTS PERSONNELS 27

CHAPITRE 4 : COMMENT IDENTIFIER CE QUE VOUS DÉTENEZ ET POURQUOI 28

1. Créer un registre des activités de traitement 29

2. Identifier les faits 30

3. Appliquer les exigences du SIPRP 32

4. Évaluer et atténuer les risques 36

CHAPITRE 5 : COMMENT EXPLIQUER VOS PRATIQUES DE TRAITEMENT 39

1. Préparer un avis de confidentialité 39

2. Communiquer votre avis de confidentialité aux bonnes personnes, au bon moment et de la bonne manière 42

3. Obtenir un consentement valable si vous en avez besoin 45

CHAPITRE 6 : COMMENT PROTÉGER LES RENSEIGNEMENTS PERSONNELS 48

1. Élaborer et mettre en œuvre un programme de sécurité de l'information 49

2. Mettre en œuvre des mesures de sécurité appropriées 51

CHAPITRE 7 : COMMENT SE PRÉPARER ET RÉAGIR À UNE ATTEINTE À LA SÉCURITÉ 55

1. Créer un plan d'intervention 55

2. Tester votre plan 59

3. Répondre à une atteinte à la sécurité 59

CHAPITRE 8 : COMMENT PARTAGER LES RENSEIGNEMENTS PERSONNELS DE MANIÈRE RESPONSABLE 63

1. Identifier et classifier les tiers 64

2. Appliquer les principes communs 65

3. Partager avec d'autres OAD 67

4. Partager avec les tiers mandataires 69

CHAPITRE 9 : QUELS RENSEIGNEMENTS PERSONNELS DOIVENT ÊTRE CONSERVÉS 76

1. Comprendre l'Annexe A du SIPRP 76

2. Mettre en œuvre l'Annexe A en dehors d'ADAMS 77

3. Définir des périodes de conservation pour d'autres données 79

4. Supprimer, détruire ou anonymiser à l'expiration des délais de conservation 79

CHAPITRE 10 : COMMENT RÉPONDRE AUX DEMANDES ET AUX PLAINTES 81

1. Comprendre les droits individuels en matière de renseignements personnels 81

2. Répondre à une demande ou à une plainte 83

SECTION 3 : SENSIBILISER LE PERSONNEL À VOTRE PROGRAMME DE PROTECTION DES RENSEIGNEMENTS PERSONNELS 90

CHAPITRE 11 : COMMENT CRÉER UNE CULTURE DE RESPECT DE LA VIE PRIVÉE 91

1. Former vos champions de la protection des renseignements personnels 92

2. Former votre personnel et accroître la sensibilisation 92

Bienvenue aux Lignes directrices pour la protection des renseignements personnels

Introduction

Bienvenue aux Lignes directrices pour la protection des renseignements personnels (Lignes directrices), un document de troisième niveau, non obligatoire, qui soutient le Standard international pour la protection des renseignements personnels (SIPRP). Ces Lignes directrices visent à mieux équiper les organisations antidopage (OAD) dans l'application de protections appropriées et efficaces aux renseignements personnels qu'elles traitent, comme décrites dans le SIPRP.

Là où le SIPRP indique les exigences minimales à rencontrer, les Lignes directrices vous aident à comprendre comment y arriver, en vous donnant des exemples et des suggestions, et en vous montrant comment aller encore plus loin lorsque c'est possible.

Le contexte

En vertu du Code mondial antidopage (le Code), les OAD s'engagent à protéger et à traiter les renseignements personnels de façon licite dans le cadre de leurs activités antidopage. Ceci est essentiel pour assurer la confiance continue des sportifs et des autres personnes soumises aux règles antidopage.

Grâce au SIPRP et aux Lignes directrices, les OAD peuvent élaborer des programmes de protection des renseignements personnels qui renforcent la confiance en aidant les sportifs à comprendre comment leurs renseignements personnels sont traités et protégés à chaque étape du processus antidopage, et en réduisant les risques de sécurité et de confidentialité pour les renseignements personnels.

Au-delà du SIPRP

La plupart des pays du monde ont adopté une loi sur la protection des données et de la vie privée. En fait, 66 % des pays l'ont déjà fait et un autre 10 % ont un projet de loi[1].

Le SIPRP fournit un ensemble d'exigences minimales et communes applicables aux traitements des renseignements personnels utilisés dans les activités antidopage. C'est une base sur laquelle les OAD

[1] Conférence des Nations unies sur le commerce et le développement, « Global Cyber Law Tracker » (législation sur la protection des données et de la vie privée dans le monde), https://unctad.org/page/data-protection-and-privacy-legislation-worldwide (dernier accès le 14 octobre 2020).

peuvent construire un programme de renseignements personnels qui respecte également les lois sur la protection des données et de la vie privée qui leur sont applicables.

Ces Lignes directrices fournissent des informations et des conseils pour vous aider à élaborer un programme de protection des renseignements personnels que vous pouvez adapter aux besoins et au contexte de votre OAD.

Comment utiliser les Lignes directrices

Alors, comment profiter au maximum des Lignes directrices ? Les Lignes directrices sont un outil de soutien pour les OAD de toutes tailles - grandes ou petites. Nous comprenons que des organisations différentes peuvent avoir des besoins différents, c'est pourquoi nous avons conçu les Lignes directrices sous forme de sections et de chapitres clairs pour vous aider à y naviguer d'une manière qui vous convienne. Nous avons également évité d'utiliser des termes et définitions définis pour cette dernière édition.

Si vous êtes novice en matière de protection des renseignements personnels ou de lutte contre le dopage, ou si vous commencez tout juste à élaborer un programme de protection des renseignements personnels, il peut être utile de lire les Lignes directrices du début à la fin et d'utiliser les exemples, les figures et les modèles pour votre propre travail. Vous serez ainsi guidé dans un processus logique d'élaboration et de mise en œuvre de votre programme de renseignements personnels.

Si vous cherchez un soutien pour un article ou une rubrique particulière du SIPRP, sélectionnez le chapitre qui vous convient et accédez directement à celui-ci. Si vous avez besoin de plus de contexte, vous pouvez passer en revue d'autres chapitres.

CONSTRUIRE

SECTION 1

- Faites de la protection des renseignements personnels une priorité
- Préparez le terrain
- Structurez votre programme

METTRE EN ŒUVRE

SECTION 2

A
- Identifiez ce que vous détenez et pourquoi
- Expliquez vos pratiques de traitement

B
- Protégez les renseignements personnels
- Préparez-vous à répondre à une atteinte

C
- Soyez responsable quand vous communiquez des renseignements personnels
- Définissez et appliquez les délais de conservation
- Répondez aux demandes et aux plaintes

ÉDUQUER

SECTION 3

- Créez une culture de respect de la vie privée

Résumé

- La lutte contre le dopage vous oblige à recueillir et à traiter des renseignements personnels.
- Vous pouvez renforcer la confiance des sportifs, réduire les risques de non-conformité et les risques juridiques, et améliorer la gouvernance globale de l'information en faisant de la protection des renseignements personnels une priorité stratégique.
- Désignez une personne responsable pour la protection des renseignements personnels chargée de veiller au respect du SIPRP. Veillez à ce que celle-ci puisse être contactée par les parties prenantes et soit soutenue par des ressources adéquates.
- Familiarisez-vous avec les principes relatifs aux pratiques loyales en matière d'information - ce sont les fondements du SIPRP.
- Comprenez que le SIPRP est un ensemble d'exigences minimales qui vise à garantir que toutes les OAD soient responsables de leur traitement des renseignements personnels.
- Examinez les lois relatives à la protection des données et de la vie privée, aux sports et à la lutte contre le dopage qui s'appliquent à vous. Elles doivent toutes être prises en compte dans le cadre de votre programme de protection des renseignements personnels.
- Définissez la structure de gouvernance de l'information au sein de votre organisation et veillez à ce que votre Responsable de la protection des renseignements personnels rende compte à la haute direction.
- Définissez les exigences du programme de protection des renseignements personnels que l'organisation doit respecter.
- Notez-les et rendez-les obligatoires.

METTRE EN ŒUVRE

A Évaluez — Expliquez

- Créez et maintenez un « registre de traitement » qui identifie (i) les activités qui impliquent des renseignements personnels ; (ii) la manière dont vous collectez, utilisez et partagez les renseignements personnels pour chaque activité ; et (iii) la manière dont les renseignements personnels sont protégés à chaque étape. Utilisez le modèle de l'AMA pour vous aider.
- Pour chaque activité, évaluez si (i) vous ne traitez que ce dont vous avez besoin ; (ii) les renseignements personnels sont exacts ; (iii) vous avez un fondement juridique valable pour le traitement ; et (iv) les personnes peuvent comprendre votre traitement.
- Utilisez le modèle de matrice d'évaluation des risques de l'AMA pour évaluer les activités à haut risque.
- Faites preuve de transparence en créant des avis de confidentialité qui expliquent le qui, quoi, pourquoi, comment et les droits et choix relatifs à vos activités de traitement des renseignements personnels. Utilisez le modèle d'avis de l'AMA pour vous aider.
- Veillez à ce que vos avis de confidentialité soient simples et adaptez-les au contexte dans lequel ils seront lus, c'est-à-dire avant ou au moment de la collecte des renseignements personnels. Vous vous retrouverez probablement avec plus d'un avis ou d'une politique de protection des renseignements personnels.
- Si nécessaire, assurez-vous d'inclure des mécanismes permettant aux personnes de confirmer leur consentement, en particulier pour les renseignements personnels sensibles, et révisez les conditions de validité du consentement dans le SIPRP.

B Protégez — Préparez-vous à répondre à une atteinte

- Mettez en place un programme de sécurité de l'information pour protéger les renseignements personnels. Vous devrez utiliser une combinaison de mesures physiques, environnementales, organisationnelles et techniques pour protéger les renseignements personnels.
- Répertoriez les systèmes, les applications et les logiciels que vous utilisez pour traiter les renseignements personnels ; comprenez comment les cyberrisques affecteraient ces actifs ; et attribuez des responsabilités pour les protéger.
- Établissez un plan d'intervention en cas d'atteinte à la sécurité qui comporte cinq étapes clés : la découverte, le confinement, l'évaluation, la notification et les mesures correctives. Testez-le.
- Attribuez des responsabilités à une équipe d'intervention en cas d'atteinte à la sécurité avec des compétences complémentaires.
- En cas d'atteinte à la sécurité, évaluez la gravité et l'impact de l'atteinte afin de déterminer si vous devez en informer les personnes concernées, d'autres organisations ou les autorités règlementaires.
- Conservez des registres appropriés. Utilisez le modèle de compte rendu ou de journal d'atteinte à la sécurité de l'AMA pour vous aider.

C

Communiquez de manière responsable

- Appliquez des principes communs avant de partager des renseignements personnels à l'extérieur de votre organisation : (i) identifiez un besoin de savoir ; (ii) minimisez ce qui est partagé ; et (iii) utilisez des contrôles techniques et contractuels pour protéger les informations.
- Appliquez des exigences supplémentaires selon le type de destinataire, qu'il s'agisse d'une OAD, d'un tiers mandataire ou d'un autre tiers. Plus le tiers est éloigné de vous, plus les exigences seront strictes.

Définissez et appliquez des délais de conservation

- Prenez le temps d'examiner et de comprendre l'Annexe A du SIPRP. Appliquez ces délais de conservation dans vos propres systèmes et à vos propres dossiers.
- Pour les données/les fins de traitement qui ne sont pas couvertes par l'Annexe A, examinez quels autres critères de conservation s'appliquent, y compris les exigences légales ou les délais de prescription.
- Lorsque les renseignements personnels ne sont plus nécessaires à une activité antidopage ou qu'ils ne doivent pas être conservés en vertu de la loi, ils doivent être supprimés, détruits ou rendus anonymes.

Répondez aux demandes et aux plaintes

- Pour répondre aux demandes d'exercice de droits en vertu du SIPRP ou à une plainte, il faut commencer par la classer (par exemple, une demande d'accès, de correction ou de limiter le traitement, ou de refus ou de retrait du consentement).
- Ensuite, accusez réception, rassemblez les informations dont vous avez besoin pour répondre et appliquez toute exception pertinente (par exemple, en supprimant les renseignements personnels d'un tiers).
- Assurez-vous que votre réponse est opportune, raisonnée et compréhensible pour le destinataire.

ÉDUQUER

Créer une culture de respect de la vie privée

- Fixez-vous comme objectif de créer une culture de respect de la vie privée, où chaque personne peut instinctivement appliquer les principes de protection des renseignements personnels à ses activités antidopage quotidiennes.
- Commencez par former vos champions de la protection des renseignements personnels afin qu'ils puissent diffuser leur expertise dans toute l'organisation. Ensuite, créez un programme de formation à la protection des renseignements personnels et rendez-le obligatoire pour qu'il touche tout le personnel.
- Le programme devrait couvrir des sujets tels que les exigences légales, les politiques internes, les cybermenaces et la manière de protéger les renseignements personnels. Utilisez des ressources prêtes à l'emploi ou des systèmes de gestion de l'apprentissage pour obtenir de l'aide.
- Mesurez les progrès et renforcez l'apprentissage par une formation supplémentaire, des simulateurs d'hameçonnage et des rappels de sensibilisation réguliers.

SECTION 1 :

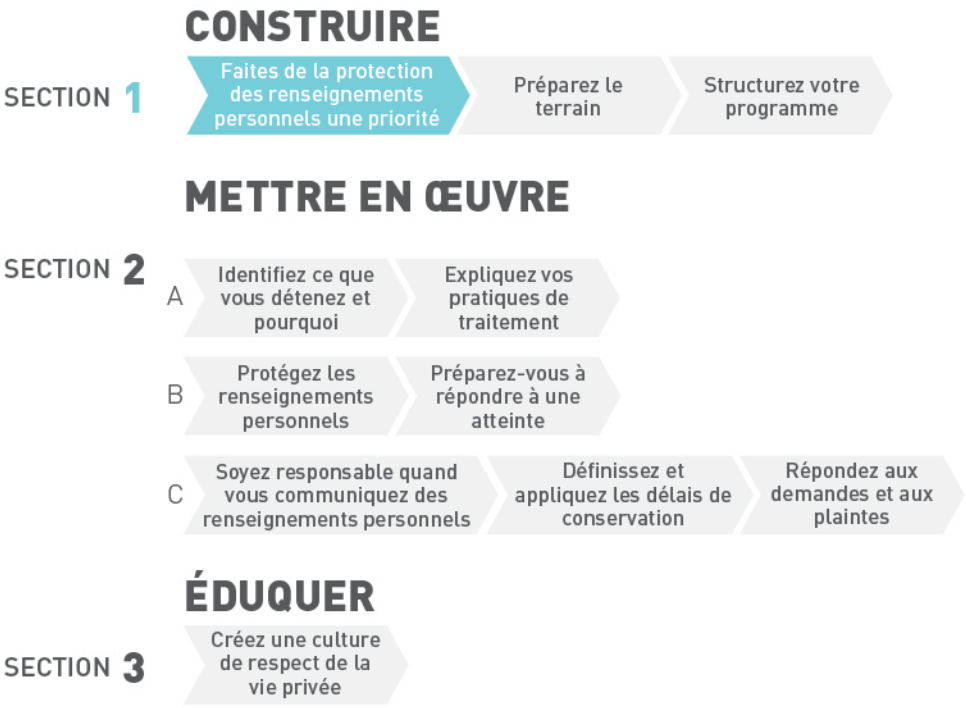
Élaboration d'un programme de protection des renseignement personnels

La section 1 comprend les Chapitres 1, 2 et 3. Cette section apportera un soutien à l'Article 4.0 du SIPRP - Traitement des renseignements personnels conformément au Standard international et au droit applicable - en vous aidant à faire de la protection des renseignements personnels une priorité au sein de votre organisation, à comprendre les principes clés du SIPRP, à établir un cadre pour votre programme de protection des renseignements personnels et à identifier les ressources qui peuvent vous aider en cours de route.

AGENCE MONDIALE ANTIDOPAGE
franc jeu

CHAPITRE 1 :

Comment faire de la protection des renseignements personnels une priorité



1. S'assurer que la protection des renseignements personnels fasse partie des objectifs clés de votre organisation

Chaque aspect de la lutte contre le dopage, de l'éducation passant par la gestion des résultats, exige des sportifs qu'ils fournissent certains renseignements personnels. Le Code affirme l'importance de veiller à ce que les droits à la vie privée des personnes soumises à des programmes antidopage soient pleinement protégés. De même, la Déclaration des droits antidopage des sportifs prévoit que les sportifs ont droit à un traitement équitable, licite et sécuritaire de leurs renseignements personnels.

Pour atteindre cet objectif, la protection des renseignements personnels doit être intégrée dans tout processus de lutte contre le dopage. Pour vous aider à déterminer si la protection des renseignements personnels est une priorité adéquate dans votre organisation, posez-vous les questions suivantes :

- Votre organisation a-t-elle des objectifs stratégiques ou opérationnels ou des buts pour l'avenir ?
- La protection des renseignements personnels, la gestion de l'information ou la sécurité de l'information figurent-elles dans ces priorités ?
- Existe-t-il des projets visant à consacrer des ressources humaines, informatiques, financières ou autres à la protection des renseignements personnels ?

Si vous avez répondu « non » à l'une des questions ci-dessus, vous devrez vous efforcer de faire de la protection des renseignements personnels une priorité au sein de votre organisation. Pour vous aider à y parvenir, réfléchissez aux moyens par lesquels une meilleure protection des renseignements personnels apportera une valeur ajoutée à votre organisation :

- De solides protections réduisent les risques associés au traitement des renseignements personnels des sportifs, ce qui renforce la confiance des sportifs dans les processus antidopage et dans votre organisation ;
- Intégrer le respect de la vie privée dans les processus quotidiens de lutte contre le dopage réduit le risque de non-conformité, ainsi que les risques juridiques et de réputation;
- Un programme de protection des renseignements personnels vous aidera à comprendre vos données et vos opérations, ce qui vous permettra de réaliser de nouvelles économies et d'améliorer la gouvernance de l'information ;
- La mise en œuvre de mesures de redevabilité dans votre programme de protection des renseignements personnels vous aidera à répondre à des attentes plus larges en matière d'éthique et de gouvernance dans toute l'organisation et fera de vous un partenaire plus fiable lorsque vous recevrez des informations d'autres OAD.

2. Création d'un rôle, d'une équipe ou d'un service de protection des renseignements personnels

Reconnaissant l'importance de faire de la protection des renseignements personnels une priorité, le SIPRP exige que les OAD désignent une personne responsable de la conformité de l'OAD avec le SIPRP. Aux fins de ces Lignes directrices, nous appellerons la personne désignée la Responsable de la protection des renseignements personnels. Les OAD sont libres de choisir un titre de leur choix, l'important étant que cette personne se concentre sur les questions de protection des renseignements personnels.

QUI PEUT ÊTRE UN RESPONSABLE DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ?

N'importe qui peut devenir un Responsable de la protection des renseignements personnels. L'idéal est de nommer des personnes qui ont une certaine connaissance des lois et des exigences en matière de protection des données, qui peuvent défendre l'importance de protéger la vie privée au sein de l'organisation et qui sont capables de surveiller la manière dont votre organisation traite les renseignements personnels. Des connaissances en matière de sécurité de l'information ou d'informatique et de lutte contre le dopage seraient également utiles pour remplir ce rôle.

Si des employés existants sont transférés à un poste de protection des renseignements personnels ou de nouveaux employés ne possèdent pas déjà cette expertise, envisagez d'investir dans leur développement professionnel. Demandez-vous également si des consultants ou des professionnels externes pourraient remplir ce rôle ou être engagés pour soutenir un responsable interne de la protection des renseignements personnels. En vertu du SIPRP, le Responsable de la protection des renseignements personnels n'a pas besoin de se consacrer exclusivement à la protection des renseignements personnels. Pour les grandes OAD, envisagez de soutenir le Responsable de la protection des renseignements personnels en lui adjoignant des membres d'équipe supplémentaires. Pour les petites OAD, vous pouvez également envisager de mettre en commun les ressources en partageant un Responsable de la protection des renseignements personnels avec d'autres OAD.

Dans certaines juridictions, des exigences d'indépendance peuvent être associées au rôle de Responsable de la protection des renseignements personnels (ou son équivalent) qui empêchent la personne d'exercer d'autres fonctions au sein de l'organisation. Il pourrait aussi être nécessaire de prendre en compte certaines exigences supplémentaires pour le rôle (par exemple, nécessité d'utiliser un titre particulier, comme celui de délégué à la protection des données, capacité à faire rapport directement à la haute direction ; protection contre les conséquences de l'exercice des fonctions, etc.)

QUELLES SONT LES RESPONSABILITÉS D'UN RESPONSABLE DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ?

Le Responsable de la protection des renseignements personnels devrait :

- Veiller à ce que l'OAD se conforme au SIPRP et aux lois applicables en matière de protection des données et de la vie privée ;
- Veiller à ce que l'OAD dispose de fondements juridiques valables pour traiter les renseignements personnels à des fins de lutte contre le dopage (voir 3. Appliquer les exigences du SIPRP dans Chapitre 4 :Comment identifier ce que vous détenez et pourquoi) ;
- Préparer, mettre en œuvre et revoir régulièrement les politiques et procédures internes de l'organisation en matière de protection des renseignements personnels ;
- Préparer les registres de traitement (voir 1. Créer un registre des activités de traitement dans Chapitre 4 : Comment identifier ce que vous détenez et pourquoi) ;

- Servir de contact principal au sein et en dehors de l'OAD pour les demandes, requêtes ou plaintes relatives à la protection des renseignements personnels (voir Chapitre 10 : Comment répondre aux demandes et aux plaintes) ;
- Veiller à ce que les délais de conservation des renseignements personnels fixés à l'Annexe A du SIPRP soient respectés (voir Chapitre 9 : Quels renseignements personnels doivent être conservées) ;
- Si nécessaire, informer les personnes concernées d'atteinte à la sécurité (voir Chapitre 7 : Comment se préparer et réagir à une atteinte à la sécurité) ; et
- Travailler avec les professionnels de l'informatique pour garantir la mise en œuvre de mesures de protection appropriées des renseignements personnels (voir Chapitre 6 : Comment protéger les renseignements personnels).

Notez que c'est l'OAD, et non le Responsable de la protection des renseignements personnels, qui est responsable en dernier ressort pour la conformité de l'OAD au Code et aux Standards internationaux.

Le Responsable de la protection des renseignements personnels aura besoin de ressources adéquates pour remplir son rôle. Envisagez de créer un budget annuel pour la protection des renseignements personnels ou de charger votre Responsable de la protection des renseignements personnels de préparer ce budget. Un budget de protection des renseignements personnels peut devoir tenir compte des éléments suivants :

- Ressources humaines (salaires des employés, coûts de formation, autres dépenses) ;
- Les coûts de conseillers juridiques, d'auditeurs ou de consultants externes ;
- Les coûts des logiciels de conformité en matière de protection des renseignements personnels ou d'autres outils (par exemple, les fournisseurs de logiciel de gestion de l'apprentissage ou les outils permettant de créer des registres de traitement ou de gérer les risques liés à la vie privée. Voir 1. Former vos champions de la protection des renseignements personnels dans Chapitre 11 : Comment créer une culture de respect de la vie privée) ;
- Frais de traduction si vous avez utilisé les ressources de l'AMA ou d'autres OAD qui doivent être traduites dans votre propre langue. Assurez-vous de faire appel à des traducteurs professionnels et de demander à votre responsable de la protection des renseignements personnels de vérifier l'exactitude des traductions, en veillant à ce que le langage du Code et des Standards internationaux et l'intégrité du travail soient intacts ;
- Coûts des matériaux et outils de formation du personnel (voir 2. Former votre personnel et accroître la sensibilisation dans Chapitre 11 : Comment créer une culture de respect de la vie privée)

Lorsque les ressources sont limitées, pensez au budget minimum nécessaire pour mettre en œuvre votre programme des renseignements personnels en tirant parti des ressources d'autres agences, comme les modèles SIPRP gratuits de l'AMA, les lignes directrices et les cours disponibles sur ADeL.

COMMENT RENDRE LE RESPONSABLE DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ACCESSIBLE AUX PARTIES PRENANTES

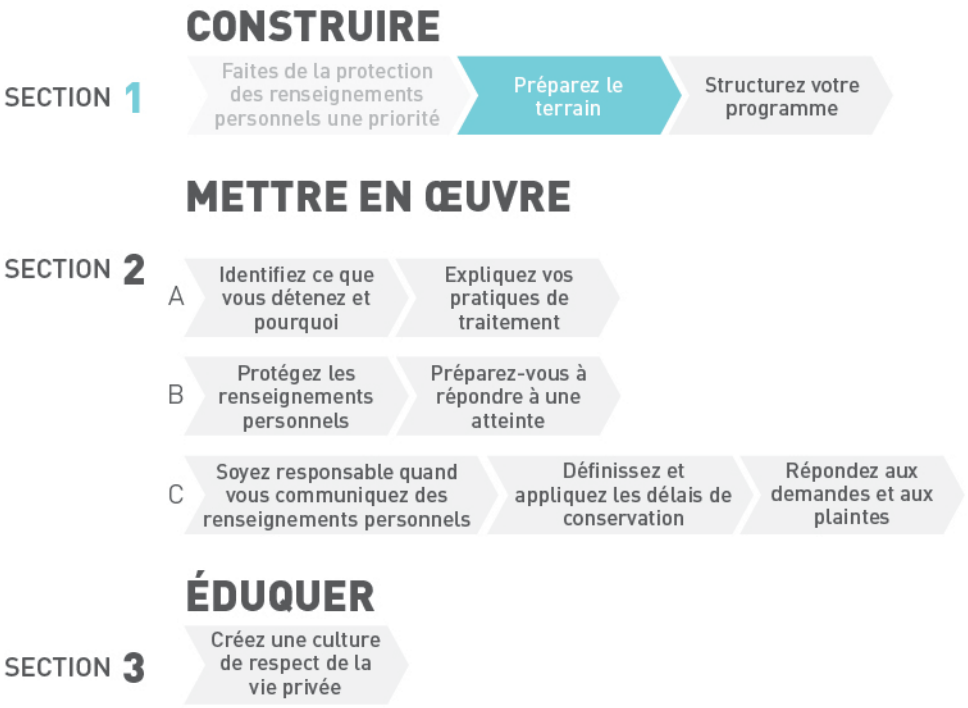
Chaque membre de votre organisation doit avoir accès au Responsable de la protection des renseignements personnels et être encouragé à lui soumettre toute question ou problème en matière de protection des renseignements personnels.

Le SIPRP exige que les coordonnées du Responsable de la protection des renseignements personnels soient facilement accessibles à l'externe. En pratique, les coordonnées du Responsable de la protection des renseignements personnels peuvent être fournies en même temps que les autres informations requises concernant le traitement des renseignements personnels (voir Chapitre 5 : Comment expliquer vos pratiques de traitement).

Vous n'êtes pas obligé de communiquer le nom de votre Responsable de la protection des renseignements personnels à l'externe, mais vous pouvez le faire si vous pensez que cela peut être utile. L'important est de fournir des coordonnées où il ou elle peut être facilement rejoint (par exemple, une adresse électronique, une adresse physique et/ou un numéro de téléphone).

CHAPITRE 2 :

Les fondements de votre programme de protection des renseignements personnels



1. Comprendre les principes relatifs aux pratiques loyales en matière d'information

Le SIPRP est explicitement basé sur les Lignes directrices de l'Organisation de coopération et de développement économiques (OCDE) de 1980 régissant la protection des renseignements personnels et les flux transfrontières de données de caractère personnel (Lignes directrices de l'OCDE[2]).

Les Lignes directrices de l'OCDE ont établi huit principes pour une gestion loyale de l'information qui ont jeté les bases des cadres juridiques de protection des données autour du monde et, de même, fournissent les bases du SIPRP.

[2] https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (dernier accès le 14 octobre 2020)

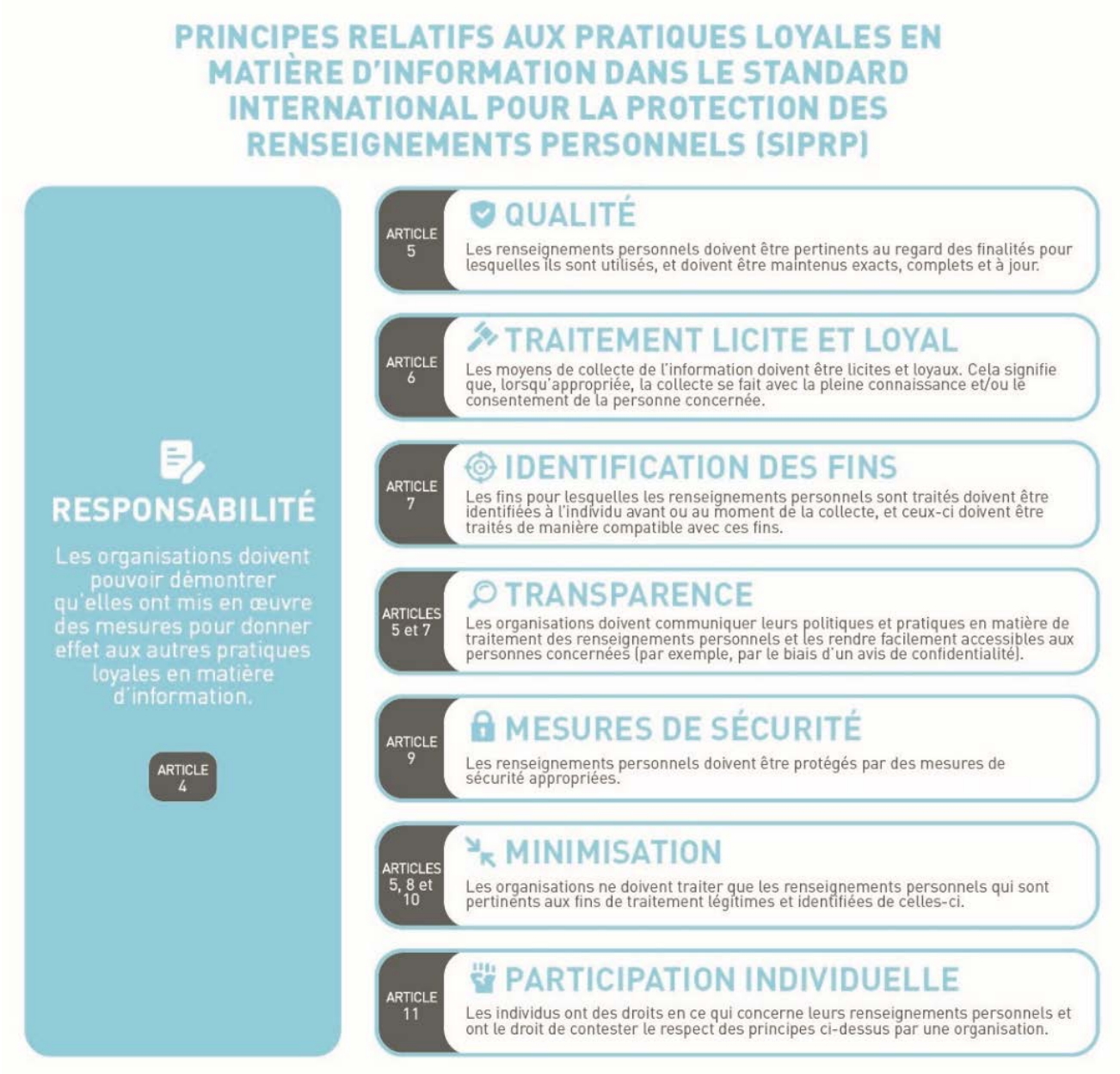


Figure 1 : Principes relatifs aux pratiques loyales en matière d'information dans le SIPRP[3]

[3] Les définitions et les noms des huit principes relatifs aux pratiques loyales en matière d'information ne sont pas toujours repris textuellement. Ils ont été adaptés à partir des Lignes directrices de l'OCDE et résumés par souci de simplicité et pour utiliser une terminologie plus actuelle.

2. Comprendre le rôle du SIPRP dans votre programme de protection des renseignements personnels

Le SIPRP est aligné aux principes relatifs aux pratiques loyales en matière d'information, comme le montre l'image ci-dessus. Le but du SIPRP est d'assurer que les OAD prennent des mesures pour mettre en œuvre chacun de ces principes dans leurs activités antidopage.

En particulier, le SIPRP actuel, combiné au programme de supervision de la conformité au Code, vise à garantir que toutes les OAD puissent rendre compte de leur traitement des renseignements personnels à des fins de lutte contre le dopage. Cela s'aligne avec l'importance accrue accordée à ce principe dans les lois sur la protection des données et de la vie privée à travers le monde, de même que dans les principes relatifs aux pratiques loyales en matière d'information. En fait, la version actualisée des Lignes directrices de l'OCDE contient une nouvelle section décrivant ce qui est nécessaire pour mettre en œuvre le principe de responsabilité :

> « Tout maître de fichier devrait :
>
> 1) Avoir mis en place un programme de gestion de la vie privée qui :
> i) assure l'application des présentes Lignes directrices à l'ensemble des données de caractère personnel sous son contrôle ;
> ii) est adapté à la structure, à l'échelle, au volume et au caractère plus ou moins sensible de ses activités ;
> iii) prévoit des mesures de protection appropriées basées sur une évaluation des risques pour la vie privée ;
> iv) est intégré dans sa structure de gouvernance et établit des mécanismes internes de supervision ;
> v) comprend des plans pour répondre aux demandes et aux incidents ;
> vi) est actualisé sur la base d'un suivi permanent et d'évaluations périodiques ;
>
> 2) pouvoir faire la preuve de la mise en œuvre de son programme de gestion de la vie privée selon les besoins, et en particulier à la demande d'une autorité compétente chargée de protéger la vie privée compétente ou de toute autre entité chargée de promouvoir le respect d'un code de conduite ou d'arrangements similaires donnant un effet contraignant aux présentes Lignes directrices ; et
>
> *3)* Avertir, selon les besoins, les autorités chargées de protéger la vie privée ou autres autorités compétentes des cas d'atteintes significatives à la sécurité qui affectent des données de caractère personnel. Lorsque l'atteinte à la sécurité est susceptible de faire tort à des personnes concernées, le maître du fichier devrait en informer ces dernières ».[4]

Le SIPRP doit également être compris dans le contexte du Code et des autres Standards internationaux. Ces documents contiennent une série d'exigences qui informent et mettent en contexte les principes de protection des renseignements personnels énoncés dans le SIPRP.

[4] OCDE, Lignes directrices révisées sur la protection des renseignements personnels et les flux transfrontières d'informations (2013), page 16, https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf (dernier accès le 14 octobre 2020).

Par exemple, les renseignements personnels nécessaires à une OAD seront déterminés par ce que le Code et les Standards internationaux exigent que l'OAD recueille pour diverses activités antidopage.

Ces Lignes directrices visent à fournir aux OAD une compréhension de comment mettre en œuvre les principes du SIPRP, ainsi que des options et des outils pour atteindre cet objectif.

3. Intégrer les lois sur la protection des données et de la vie privée

Le SIPRP fait plusieurs références expresses à la nécessité pour les OAD de tenir compte des lois applicables en matière de protection des données et de la vie privée dans le cadre de leur mise en œuvre du SIPRP.

Comme mentionné ci-dessus, cela est dû au fait que, pour la plupart des OAD, il y aura des lois sur la protection des données et de la vie privée qui chevauchent le SIPRP. Étant donné que le SIPRP est basé sur les mêmes principes que les lois sur la protection des données et de la vie privée dans le monde entier, vous trouverez probablement de nombreuses similitudes entre le standard et les lois applicables à votre organisation. Les OAD doivent toujours tenir compte des lois applicables en matière de protection des données et de la vie privée lorsqu'elles élaborent leur programme de protection des renseignements personnels.

Les OAD doivent également prendre en compte les lois locales régissant le sport et la lutte contre le dopage et s'y référer. Dans certains cas, ces lois sur le sport et/ou la lutte contre le dopage règlementeront spécifiquement le traitement des renseignements personnels associés aux activités antidopage.

COMMENT SAVOIR QUELLES SONT LES LOIS QUI S'APPLIQUENT À VOUS ?

Tout d'abord, prenez en considération le(s) lieu(x) à partir duquel (ou desquels) vous exercez la plupart de vos activités (par exemple, votre siège social ou votre bureau principal). Dans la plupart des cas, cela déterminera les lois qui s'appliquent à vous.

Ensuite, déterminez si ce ou ces lieu(x) disposent d'une autorité de protection des données. Si c'est le cas, le site web de cette autorité est un excellent point de départ pour trouver des conseils et des informations sur les lois locales et leur application.

De même, s'il existe une loi ou une politique locale en matière de sport ou de lutte contre le dopage, consultez le site web de l'organisme gouvernemental responsable de cette loi ou politique.

Les organisations nationales antidopage (ONAD) et les fédérations internationales (FI) opérant au même endroit pourraient explorer des possibilités de collaboration et d'échange d'informations/d'expertise à cet égard.

Certaines lois cherchent à étendre leur application en dehors de leurs limites territoriales et utilisent d'autres critères, comme le fait que le traitement concerne des personnes sur un territoire donné et l'offre de biens ou de services sur ce territoire. En matière de lutte contre le dopage, chaque OAD avec laquelle vous collaborez sera soumise à ses propres lois, ce qui pourrait également vous concerner (par exemple, si vous fournissez des services antidopage à une autre OAD). Cela peut rendre complexe la tâche d'identifier les lois qui vous sont applicables.

En pratique, concentrez vos efforts sur la mise en place d'un programme de protection des renseignements personnels solide qui répond aux exigences minimales du SIPRP ainsi qu'aux exigences des lois du pays où vous vous trouvez. Dans la mesure du possible, suivez les meilleures pratiques décrites dans ces Lignes directrices et dans celles publiées par vos autorités règlementaires locales. Si vous disposez des ressources nécessaires, vous pouvez demander un avis juridique pour mieux comprendre votre cadre juridique.

Des outils gratuits, comme le « tracker » des lois relatives à la protection des données et de la vie privée dans le monde de la Conférence des Nations unies sur le commerce et le développement [5] peut également vous aider à identifier les lois pertinentes en matière de protection des données et de la vie privée.

Les cabinets d'avocats ou autres cabinets de consultants ainsi que les associations professionnelles de l'industrie[6] peuvent également offrir gratuitement des résumés, des webinaires et d'autres ressources dans leur domaine de compétence, qu'il s'agisse de la protection des renseignements personnels, du sport, ou même de la sécurité de l'information. Recherchez les entreprises locales ou les succursales locales d'entreprises internationales pour obtenir les informations qui vous seront les plus utiles.

[5] Voir note 1.
[6] Voir, par exemple, l'International Association of Privacy Professionals (https://iapp.org/).

QUE FAIRE SI VOUS PENSEZ QUE VOS LOIS SONT EN CONFLIT AVEC LE SIPRP ?

Le SIPRP est un document obligatoire, comme les autres Standards internationaux. Il fournit un plancher, et non un plafond, de standards pour la protection des renseignements personnels. Cela signifie que lorsqu'une OAD est soumise à des lois applicables qui fixent des standards inférieurs au SIPRP, l'OAD doit respecter les standards plus élevés du SIPRP. Lorsqu'une OAD est soumise à des lois applicables qui fixent des standards plus élevés que le SIPRP, elle doit compléter les standards du SIPRP par les exigences supplémentaires prévues par les lois applicables.

Le SIPRP contient une exception limitée. Dans le cas où la conformité avec le SIPRP mettrait une OAD en conflit avec d'autres lois applicables, l'OAD ne sera pas considérée comme non conforme au Standard dans la stricte mesure du conflit. Prenez bonne note que cela ne se produira que dans des circonstances exceptionnelles, car la loi applicable n'empêchera que très rarement une OAD de protéger les renseignements personnels avec les protections de base prévues par le Standard.

Les deux scénarios suivants illustrent la portée de l'exception :

PAS DE CONFLIT

Le SIPRP exige que les tiers mandataires soient soumis à des contrôles contractuels et techniques appropriés lorsqu'ils traitent des renseignements personnels pour mener des activités antidopage qui leur sont déléguées par une OAD. Le Règlement général sur la protection des données (RGPD) de l'UE exige que tout « sous-traitant » engagé par une OAD soit soumis à un ensemble spécifique de contrôles obligatoires.

Il n'y a pas de conflit ici, car l'OAD peut se conformer à la fois au SIPRP et au droit applicable. De même, une OAD qui n'est soumise à aucune obligation de mettre en œuvre des contrôles spécifiques dans le cadre d'un accord avec un tiers mandataire en vertu des lois applicables serait tenue de respecter l'exigence du SIPRP pour ce faire. Il n'y a pas non plus de conflit dans ce scénario, car rien n'interdit à l'OAD de se conformer à l'exigence du SIPRP.

CONFLIT

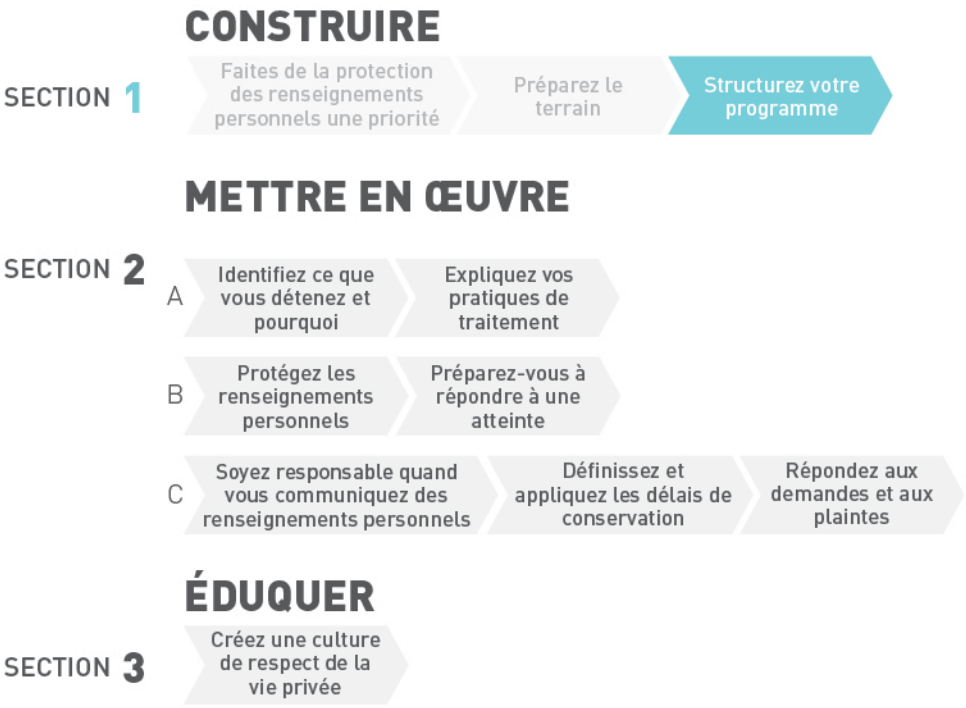
Une OAD est tenue de conserver certaines données antidopage pendant 20 ans en raison de leur pertinence pour certaines infractions pénales ou criminelles en matière de dopage pouvant faire l'objet d'une poursuite jusqu'à 20 ans après leur survenance. Le SIPRP prévoit une période de conservation maximale de 10 ans pour les mêmes données.

Dans ce scénario, il y a un conflit, car l'OAD ne respectera pas la période de conservation maximale prévue par le SIPRP en se conformant à la législation locale.

En cas de conflit réel entre le SIPRP et les lois applicables, vous devriez communiquer avec le département de conformité de l'AMA à l'adresse suivante compliance@wada-ama.org dès que raisonnablement possible et fournir à l'AMA la preuve de l'exigence spécifique conflictuelle (par exemple, la disposition légale spécifique imposant la période de conservation de 20 ans). Sur cette base, l'OAD ne serait pas considérée comme non conforme à la période de conservation maximale du SIPRP dans les cas spécifiques où une période de conservation plus longue est prescrite par une loi applicable à l'OAD. Dans la mesure du possible, l'OAD doit également informer les autres OAD concernées du conflit.

CHAPITRE 3 :

Comment structurer votre programme de protection des renseignements personnels



1. Identifier votre structure de gouvernance

Au Chapitre 1, nous avons examiné l'obligation de nommer un Responsable de la protection des renseignements personnels, les responsabilités de ce dernier, ainsi que les ressources humaines et financières à mettre à sa disposition.

Dans ce chapitre, nous allons au-delà de cette exigence de base pour vous aider à structurer votre programme de protection des renseignements personnels dans son ensemble. Tout d'abord, le Responsable de la protection des renseignements personnels doit être soutenu par les cadres supérieurs de l'OAD. Il s'agit généralement des personnes chargées de nommer le Responsable de la protection des renseignements personnels et d'approuver le budget consacré à la protection des renseignements personnels. Les décisions relatives à la protection des renseignements personnels peuvent également

nécessiter la participation d'autres personnes ou services, en fonction de la complexité et de la structure de votre organisation.

Pour vous aider à identifier la structure de gouvernance de votre organisation, posez-vous les questions suivantes :

- Qui est la personne ou l'organe de décision ultime de l'organisation ?
- Qui fait rapport à cette personne/cette entité ?
- Pouvez-vous tracer une ligne de communication de cette personne/cette entité jusqu'au Responsable de la protection des renseignements personnels ? Si ce n'est pas le cas, envisagez d'en établir une.
- Qui approuve les budgets de l'organisation ?
- Sur quelle base les décisions budgétaires sont-elles prises ? Qui est responsable de l'élaboration des plans budgétaires ?
- Qui d'autre participe à la prise de décisions clés pour l'organisation ? Sur le plan juridique ? Les responsables opérationnels ? Les agents financiers ? Examinez comment la fonction de protection des renseignements personnels interagit avec ces fonctions.
- Disposez-vous déjà de comités de gouvernance ou de comités axés sur le risque, la sécurité et/ou la gestion de l'information ? Envisagez d'inclure officiellement les questions de protection des renseignements personnels dans le mandat ou les responsabilités de ces comités.

2. Attribuer les rôles et les responsabilités

Maintenant que vous avez identifié la structure de gouvernance existante au sein de votre organisation, envisagez d'attribuer formellement les rôles et responsabilités en matière de protection des renseignements personnels, du sommet de l'organisation jusqu'au Responsable de la protection des renseignements personnels.

Par exemple, identifiez la personne ou l'organe de décision responsable en dernier ressort de l'organisation, et expliquez comment la responsabilité des questions de protection des renseignements personnels est déléguée au sein de l'organisation au Responsable de la protection des renseignements personnels (et à d'autres, le cas échéant).

Définir la manière dont le Responsable de la protection des renseignements personnels doit rendre compte à cette personne ou à cet organe décisionnel.

Pour les grandes organisations qui ont créé un comité ou un groupe chargé de discuter des questions de protection des renseignements personnels, il convient de réfléchir à la fréquence des réunions de ce comité, à la personne qui en fixe l'ordre du jour et aux questions qui doivent y être débattues.

Identifier les rôles qui sont complémentaires ou étroitement liés à la fonction de protection des renseignements personnels, tels que la sécurité de l'information, les technologies de l'information, les risques et/ou les fonctions juridiques. Envisagez d'exiger formellement que ces rôles se soutiennent et se complètent mutuellement.

3. Définir les exigences auxquelles l'organisme doit répondre

Au Chapitre 2, nous avons passé en revue les principes de protection des renseignements personnels et des données, les standards minimaux du SIPRP et les exigences légales qui devraient constituer la base de votre programme de protection des renseignements personnels.

Maintenant que vous avez identifié le cadre, il est temps de définir les exigences spécifiques que vous appliquerez au sein de votre organisation pour atteindre les objectifs de ce cadre. **Il s'agira « des politiques et procédures internes » requises par le SIPRP**.

Vous pouvez le décomposer par principe, par section du SIPRP ou par domaine opérationnel. Par exemple, vous pouvez établir une politique de protection des renseignements personnels dans laquelle chacun des principes relatifs aux pratiques loyales en matière d'information fait office de section, dans laquelle vous définissez ensuite les engagements et les actions concrètes que votre organisation doit prendre pour se conformer à chaque principe. Vous pouvez également utiliser les articles du SIPRP pour organiser votre document.

Si vous avez besoin d'aide, consultez la Liste de Vérification du SIPRP et le webinaire SIPRP en Pratique disponible sur ADEL. La section 2 des présentes Lignes directrices vous guidera également dans la mise en œuvre de tous les domaines clés de votre programme de protection des renseignements personnels.

Considérez des questions comme :

- Quelles mesures devons-nous prendre pour répondre à la demande d'une personne concernée ?
- Comment vérifions-nous les pratiques en matière de protection des renseignements personnels et de sécurité des informations des tiers avec lesquels nous travaillons ?
- Que faisons-nous pour maintenir des garanties de sécurité pour les renseignements personnels que nous traitons ?
- Comment expliquons-nous aux sportifs et aux autres personnes la manière dont nous allons traiter leurs renseignements personnels ?

Il est important que vos politiques et procédures internes reflètent les pratiques réelles de votre organisation (ou les pratiques que vous êtes sûr de pouvoir mettre en œuvre au sein de votre organisation).

4. Les documenter et les rendre obligatoires

Documentez les exigences que vous avez identifiées dans des politiques et procédures internes pour vous conformer aux exigences de documentation du SIPRP. Vous devriez également envisager de documenter le cadre de gouvernance que vous avez mis en place pour soutenir votre Responsable de la protection des renseignements personnels et votre programme de protection des renseignements personnels.

Vous pouvez créer et formater ces documents de la manière qui convient le mieux à votre organisation et à ses politiques et procédures existantes dans d'autres domaines. Généralement, les politiques servent à définir des exigences de plus haut niveau, comme l'obligation de ne traiter que les renseignements personnels nécessaires à une activité particulière. Des procédures peuvent être ajoutées si vous devez définir un processus détaillé à respecter, par exemple une procédure d'évaluation des nouvelles activités pour garantir que seuls les renseignements personnels nécessaires seront traités. Ces exigences pourraient également être intégrées dans un code de conduite ou un manuel pour employés ou autres types de documents existants.

Pour ce qui est de rendre ces exigences obligatoires au sein de votre organisation, **le SIPRP exige que le personnel soit soumis à des obligations de confidentialité exécutoires**. Une obligation exécutoire est une obligation qui peut entraîner des sanctions disciplinaires ou d'autres conséquences si elle est violée par un individu.

Pour s'assurer que la responsabilité en matière de protection des renseignements personnels circule de haut en bas au sein de l'organisation, il est bon d'aller au-delà de cette exigence du SIPRP et de demander au personnel d'examiner et de formellement reconnaître vos politiques et procédures internes en matière de protection des renseignements personnels, éventuellement de manière annuelle (voir Chapitre 11 : Comment créer une culture de respect de la vie privée). De même, la violation de vos politiques et procédures internes doit faire l'objet de sanctions disciplinaires appropriées.

SECTION 2 :

Mise en œuvre de votre programme de protection des renseignements personnels

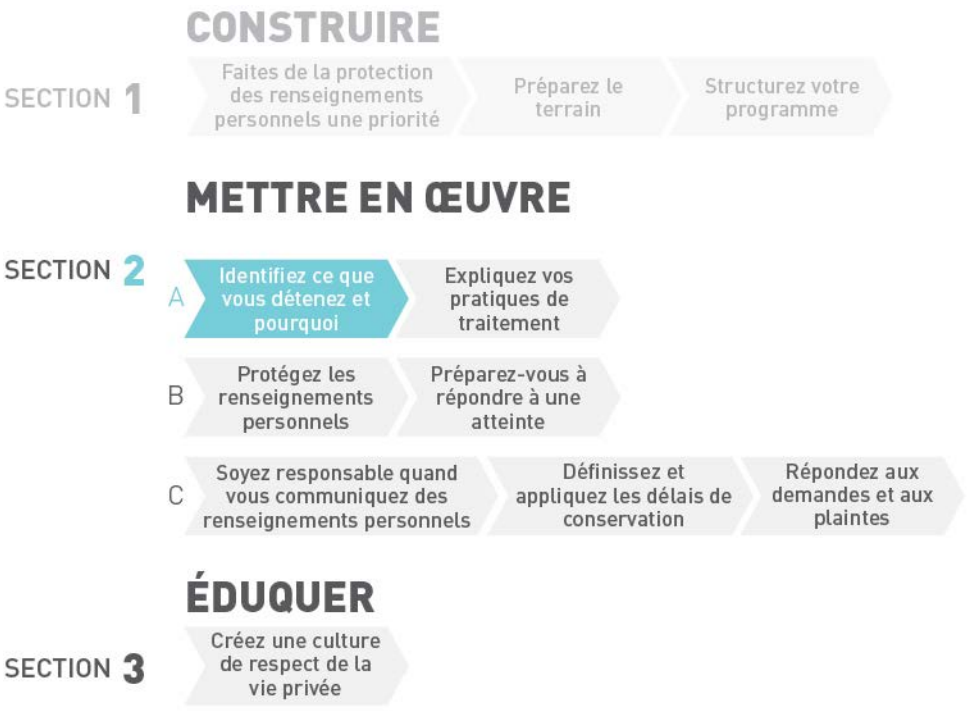
La Section 2 comprend les Chapitres 4 à 10. Cette section apportera un soutien aux Articles 5.0 à 11.0 du SIPRP en vous aidant à comprendre les renseignements personnels que vous détenez et à expliquer aux autres ce que vous en faites (Partie A) ; à protéger les renseignements personnels que vous traitez et à vous préparer à une éventuelle atteinte (Partie B) ; et à rendre opérationnelle la protection des renseignements personnels dans les actions quotidiennes comme le partage des renseignements personnels, la suppression des renseignements personnels dont vous n'avez plus besoin et la réponse aux demandes et aux plaintes (Partie C).

PARTIE A : ÉVALUER ET EXPLIQUER VOTRE TRAITEMENT DES RENSEIGNEMENTS PERSONNELS

La Partie A comprend les Chapitres 4 et 5 et apportera un soutien à l'Article 5.0 du SIPRP - Traitement des renseignements personnels pertinents et proportionnés ; à l'Article 6.0 - Traitement des renseignements personnels conformément à un fondement juridique valable ; et à l'Article 7.0 - Fourniture d'informations appropriées aux participants aux autres personnes. Elle vous guidera à travers un processus visant à identifier les renseignements personnels que vous détenez et à expliquer à d'autres ce que vous en faites.

CHAPITRE 4 :

Comment identifier ce que vous détenez et pourquoi



1. Créer un registre des activités de traitement

Les OAD doivent créer et maintenir ce qu'on appelle un « registre du traitement » pour chacune de leurs activités qui impliquent des renseignements personnels. C'est ce que l'on appelle parfois un « inventaire des données » ou une « carte des données ». Ce registre documente les renseignements personnels traités pour une activité spécifique dont une organisation est responsable.

L'objectif de ces registres, ou inventaires de données, est de renforcer la responsabilité d'une organisation et de s'assurer qu'elle a une bonne compréhension des renseignements personnels qu'elle traite. Dans le cas contraire, il peut être difficile, voire impossible, de respecter les normes et exigences applicables en matière de protection des renseignements personnels. De nombreuses activités de conformité en matière de protection des renseignements personnels sont facilitées lorsque vous disposez d'un registre de toutes vos activités de traitement. Par exemple:

Dans certaines juridictions, les OAD peuvent être tenues par la loi de conserver un « registre traitement » ou un document similaire. C'est le cas des OAD soumises au RGDP. Si cela vous concerne, assurez-vous que votre registre de traitement contient toutes les informations supplémentaires que vous êtes tenu d'inclure en vertu de la loi.

- Vous pouvez utiliser votre registre de traitement pour rédiger un avis de confidentialité décrivant ce traitement ;
- Si vous devez procéder à une évaluation des risques liés à votre traitement, le travail de compréhension de votre traitement aura déjà été effectué ;
- Si vous êtes victime d'une atteinte à la sécurité, vous pouvez rapidement identifier les systèmes et les données informatiques concernés ;
- Si vous êtes soumis à des exigences juridiques complexes en matière de transfert de données ou de motifs légaux de traitement, une vue détaillée de toutes vos activités vous aidera à appliquer ces exigences.

Avant de commencer, choisissez le format ou l'outil que vous utiliserez pour créer et gérer ces registres. Vous pouvez utiliser un simple document Word ou un fichier Excel comme le modèle de registre de traitement de l'AMA. Vous pouvez également utiliser un logiciel de conformité disponible sur le marché disposant de modèles ou de systèmes prêts à l'emploi que vous pourrez remplir. Étant donné que la création de « registres de traitement » est devenue une exigence obligatoire dans le cadre du RGPD en 2018, de nombreuses autorités de protection des données de l'UE ont également créé des modèles de fichiers Excel et des guides pour vous aider à remplir ces registres.

Une fois qu'un format est choisi, assurez-vous qu'il permettra de saisir toutes les informations nécessaires sur votre traitement de renseignements personnels. **Selon le SIPRP, les informations minimales que vous devez inclure dans le registre pour chaque activité de traitement sont**:

- Pourquoi vous effectuez cette activité (c'est-à-dire les fins du traitement) ;
- Une description des types de renseignements personnels concernés ;
- La durée de conservation des renseignements personnels (ou les critères sur lesquels repose la période de conservation) ;
- Qui aura accès à ces renseignements personnels ou les recevra (c'est-à-dire les catégories de destinataires potentiels) ;

- Les mesures prises pour protéger les renseignements personnels lorsque ces destinataires sont d'autres OAD, des tiers mandataires ou des tiers
- La manière dont les renseignements personnels sont protégés de manière plus générale (c'est-à-dire une description des mesures de sécurité techniques et organisationnelles).

Le SIPRP ne fixe pas d'autres exigences quant au format du registre ou aux types d'informations qu'il doit contenir. Pour un exemple d'un registre de traitement moins conventionnel qui contient tout de même toutes les informations décrites ci-dessus, consultez la FAQ sur la confidentialité et la sécurité d'ADAMS, sous l'entête, « Quelles informations sont recueillies dans ADAMS et comment sont-elles utilisées et communiquées ?. » Cette section de la FAQ, ainsi que la description des mesures de sécurité dans ADAMS (sous l'entête « Comment vos informations sont-elles protégées dans ADAMS ») répond à l'exigence du SIPRP selon laquelle l'AMA doit tenir un registre des traitements qui reflète les types d'activités de traitement qui ont lieu dans ADAMS. Ce registre est conçu comme un document convivial et accessible qui peut être facilement compris par les sportifs, les autres OAD ou toute personne qui souhaite comprendre le fonctionnement d'ADAMS. Comme les activités antidopage sont harmonisées dans le monde entier, vous pouvez également utiliser cette page web pour vous aider à créer vos propres registres, en gardant à l'esprit que vos registres doivent également refléter les éléments de vos activités de traitement qui se produisent en dehors d'ADAMS.

2. Identifier les faits

Maintenant que vous disposez du cadre de base de votre registre de traitement, vous devez le remplir avec les informations pertinentes. Tout au long de ce processus, votre meilleur guide sera la personne qui est effectivement responsable de chaque activité que vous souhaitez documenter. Par exemple, si vous souhaitez vous renseigner sur un traitement des renseignements personnels qui se produit dans le cadre de votre programme d'éducation, adressez-vous à votre responsable de l'éducation. Il peut être utile d'impliquer également le personnel responsable de tout système informatique ou base de données associée.

QUELLES ACTIVITÉS IMPLIQUENT DES RENSEIGNEMENTS PERSONNELS ?

Tout d'abord, identifiez les activités qui impliquent des renseignements personnels. Si vous êtes une grande organisation, commencez au niveau d'un département et répartissez les tâches quotidiennes de chaque département. Si vous êtes une petite organisation, réfléchissez à ce que chaque personne fait au quotidien.

Par exemple, si l'on prend la personne ou le service responsable de la gestion des autorisations d'usage à des fins thérapeutiques (AUT), il est probable qu'il soit responsable de certaines ou de toutes ces tâches :

- Créer et améliorer les processus de l'organisation pour la gestion des AUT;
- Recevoir et examiner les demandes d'AUT ;
- Recevoir et examiner les demandes de reconnaissance d'une AUT ;
- Répondre aux questions des sportifs sur la procédure d'AUT ;
- Répondre aux questions des autres OAD concernant une AUT accordée/refusée ;

- Saisir les données relatives aux AUT dans ADAMS ;
- Suivre le nombre et les types de demandes d'AUT reçues au cours d'une période donnée ; et
- Assurer la liaison avec le comité AUT de l'organisation (CAUT).

Maintenant que vous disposez d'une liste complète de tâches, réfléchissez à celles qui peuvent être regroupées en différentes étapes d'une même activité globale. Par exemple, la saisie des données d'AUT dans ADAMS est une étape du processus d'examen d'une demande d'AUT. Considérez également quelles tâches n'impliquent pas des renseignements personnels - nous avons mis en évidence certaines tâches en bleu qui peuvent nécessiter une enquête plus approfondie pour déterminer si elles impliquent ou non des renseignements personnels.

Vous pouvez choisir de regrouper toutes les tâches ci-dessus dans un seul registre de traitement pour la « gestion des AUT ». Vous pouvez diviser la gestion des AUT en plusieurs registres différents. Cela est à votre discrétion et dépend de la complexité des différentes tâches. Gardez à l'esprit que la création et la maintenance de ces registres de traitement peuvent prendre beaucoup de temps, et que vous ne voulez pas être détaillé au point de rendre ces registres non durables dans le temps.

COMMENT LES RENSEIGNEMENTS PERSONNELS SONT-ILS RECUEILLIS, UTILISÉS ET PARTAGÉS POUR CHAQUE ACTIVITÉ ?

Pour chaque activité que vous avez identifiée à l'étape précédente, vous devrez documenter les types de renseignements personnels qui sont recueillis, comment ils sont utilisés et avec qui ils sont partagés.

Pour ce faire, conformément à notre exemple d'AUT, examinez les questions suivantes :

- Quels sont les renseignements personnels que les personnes doivent fournir pour demander une AUT ?
- Comment ces informations sont-elles recueillies, et auprès de qui ou de quoi sont-elles recueillies ?
- À quoi servent ces renseignements personnels ? Certains des renseignements personnels recueillis sont-ils inutilisés ?
- Avec qui les renseignements personnels sont-ils partagés ?
- Comment sont-ils partagés ?
- Où et comment les renseignements personnels sont-ils stockés ?
- Quand et comment les renseignements personnels sont-ils supprimés lorsqu'ils ne sont plus nécessaires ?
- Tout au long du processus, quels sont les systèmes ou les outils utilisés pour recueillir, utiliser et partager les renseignements personnels ?

Notez vos réponses dans votre registre. Il est toujours préférable de commencer par plus de détails et d'informations, puis d'affiner votre document lors d'un deuxième examen.

COMMENT SONT-ILS PROTÉGÉS ?

Aux fins du SIPRP, vous devez vous concentrer sur deux types de protection des renseignements personnels :

- Les protections générales ; et
- Les protections spécifiques appliquées au moment de l'échange de renseignements personnels dans le cadre d'une activité de traitement.

Pour les protections générales, tenez compte des protections que vous avez mises en place grâce à votre programme global de sécurité de l'information (voir Chapitre 6 : Comment protéger les renseignements personnels pour obtenir des conseils). Reprenant l'exemple des AUT :

- Contrôles d'accès : Seuls les gestionnaires des AUT ont accès aux demandes d'AUT dans le classeur physique que nous utilisons et/ou dans ADAMS ;
- Contrôles physiques : Le classeur physique est verrouillé ; notre bureau n'est accessible qu'avec une carte-clé ;
- Contrôles techniques : Les ordinateurs que nous utilisons pour traiter les demandes d'AUT sont protégés par un pare-feu ;
- Contrôles organisationnels : Les responsables des AUT ont signé des obligations écrites de confidentialité.

Pour faciliter votre travail, vous pouvez toujours faire référence à une description de votre programme de sécurité de l'information et des mesures de sécurité qui sont appliquées pour répondre à l'exigence liée à la description des mesures techniques et organisationnelles qui sont en place.

Pour les protections appliquées au moment du partage de renseignements personnels, examinez chaque type de partage impliqué dans votre activité, et les types de protection appliqués pour chacun d'entre eux. Reprenant l'exemple des AUT :

- Partage via ADAMS : il existe dans ADAMS un certain nombre de mesures de sécurité qui s'appliqueront à ce partage (par exemple, cryptage au repos et en transit, contrôles d'accès, traçabilité des actions).
- Partage avec votre CAUT : par exemple, un canal de communication crypté, s'assurer que les membres du CAUT soient soumis à une obligation de confidentialité comme l'exige le SIAUT, supprimer les identifiants lorsque ceux-ci ne sont pas nécessaires à l'examen d'une demande par le CAUT.

3. Appliquer les exigences du SIPRP

L'étape suivante, après avoir documenté les faits de votre activité de traitement, consiste à examiner si votre activité de traitement répond à certaines exigences. Posez-vous les questions suivantes :

- Ne traitez-vous que ce dont vous avez besoin ?
- L'information est-elle exacte ? Prenez-vous des mesures pour vous assurer qu'elles le sont ?
- Quel est votre fondement juridique de traitement ?
- Les personnes concernées sont-elles correctement informées de l'activité de traitement ?
- Les personnes concernées comprennent-elles l'activité de traitement ?
- Traitez-vous des renseignements personnels à des fins qui ne sont pas des activités antidopage ?

TRAITEZ-VOUS UNIQUEMENT LES INFORMATIONS NÉCESSAIRES ?

Le SIPRP exige que les OAD ne traitent que les renseignements personnels nécessaires à leurs activités antidopage. Cette exigence applique le principe de la minimisation des données aux activités antidopage. Elle est également exprimée dans le SIPRP comme l'obligation de ne traiter que les renseignements personnels pertinent et proportionné à des fins de lutte contre le dopage.

Pour les OAD, la première étape pour évaluer si vous ne traitez que ce dont vous avez besoin consiste à comparer votre traitement des renseignements personnels aux exigences du Code et des Standard internationaux. Dans de nombreux cas, vous serez tenu, en vertu de ces documents, de recueillir des renseignements personnels spécifiques (par exemple, les exigences en matière de transmission d'informations sur la localisation pour les sportifs faisant partie d'un groupe cible soumis aux contrôles en vertu du Standard international pour les contrôles et les enquêtes (SICE)).

Si vous constatez que vous recueillez plus de renseignements personnels que ce qui est expressément requis par le Code, demandez-vous si vous respectez le principe de minimisation des données en ne recueillant que les renseignements personnels pertinents et proportionnés à vos activités. Par exemple, pour votre groupe de sportifs soumis à des exigences en matière de localisation de deuxième niveau, avez-vous veillé à ne recueillir que les informations nécessaires pour effectuer les contrôles sans préavis prévus dans votre plan de contrôle pour ce groupe de sportifs ?

LES RENSEIGNEMENTS PERSONNELS SONT-ILS EXACTS ?

Le SIPRP exige également que les renseignements personnels traités par les OAD soient exacts, complets et mis à jour.

Dans la pratique, les OAD recueillent généralement des informations directement auprès des sportifs et devraient informer les sportifs de leur obligation de veiller à ce que ces informations soient exactes, complètes et à jour. Dans la mesure du possible, les OAD devraient fournir aux sportifs des moyens facilement accessibles pour accéder à leurs propres renseignements personnels et effectuer les mises à jour requises. Par exemple, certaines informations contenues dans ADAMS peuvent être mises à jour directement par les sportifs à tout moment si leur OAD leur fournit un compte. Les OAD devraient également examiner s'il existe des mesures qu'elles peuvent prendre pour vérifier et améliorer l'exactitude des renseignements personnels détenus dans divers systèmes. Par exemple, demandez-vous si vous êtes en mesure d'identifier les profils en double dans vos bases de données.

QUEL EST VOTRE FONDEMENT JURIDIQUE DE TRAITEMENT ?

Le fondement juridique du traitement de vos renseignements personnels sera dicté par les lois sur la protection des données et de la vie privée, ainsi que par les lois sur le sport et la lutte contre le dopage qui vous sont applicables (voir 3. Intégrer les lois sur la protection des données et de la vie privée dans Chapitre 2 : Les fondements de votre programme de protection des renseignements personnels). L'exigence d'un

fondement juridique pour le traitement de renseignements personnels est liée au principe du traitement licite et loyal. Le traitement de renseignements personnels sera licite s'il est effectué conformément aux exigences en vertu de la loi, et il sera loyal s'il respecte les attentes des personnes concernées.

Historiquement, les lois sur la protection des données et de la vie privée ont souvent exigé des organisations qu'elles obtiennent le consentement des individus pour traiter leurs renseignements personnels. Afin de fournir un consentement valable, les personnes devaient avoir connaissance du traitement concerné, d'où la nécessité pour les organisations d'être transparentes quant à leur traitement avec ces personnes.

Aujourd'hui, les concepts de « connaissance et de consentement » ont été divisés dans de nombreux cadres juridiques. La transparence et la nécessité d'être informé du traitement des renseignements personnels par une organisation sont devenues une exigence distincte.

Le consentement, pour sa part, continue de figurer parmi les fondements juridiques possibles, mais de nombreuses lois modernes sur la protection des données et de la vie privée prévoient d'autres fondements juridiques, par exemple :

- Respect des obligations juridiques ;
- Exécution de tâches d'intérêt public ;
- Traitement nécessaire à des fins de santé publique ;
- Exécution d'un contrat ;
- Traitement nécessaire à la réalisation des intérêts légitimes d'une organisation ; ou
- Traitement lié à des demandes ou des procédures judiciaires.

Lorsque des fondements juridiques autres que le consentement existent dans un cadre juridique, ces alternatives peuvent être considérées plus appropriées dans le contexte de la lutte contre le dopage. En effet, les activités antidopage sont une caractéristique obligatoire du sport et ne peuvent être refusées ou rejetées par les sportifs qui souhaitent pratiquer un sport.

Même si votre juridiction considère généralement que le consentement est un fondement juridique valable pour le traitement antidopage des renseignements personnels, il existe souvent des exceptions au consentement qui peuvent s'appliquer à certaines activités. Par exemple, dans le cadre d'une enquête antidopage, vous pouvez être autorisé à divulguer des renseignements personnels aux autorités chargées de l'application de la loi, sans consentement, lorsqu'il y a une raison de croire qu'une violation de la loi a eu lieu, ou lorsqu'un ordre des forces de l'ordre vous y contraint.

En vertu de la Convention internationale de l'UNESCO contre le dopage dans le sport, les États partis se sont engagés à mettre en place des mesures appropriées pour atteindre les objectifs de la Convention, notamment des lois, des règlements, des politiques ou des pratiques administratives. De même, dans le cadre du Code, les OAD ont indiqué qu'elles attendaient des gouvernements qu'ils mettent en œuvre des mesures de coopération et de partage d'informations entre les OAD et l'AMA. En conséquence, plusieurs pays ont adapté leur droit du sport et antidopage afin de fournir les fondements juridiques nécessaires au traitement des renseignements personnels à de fins antidopage.

En fin de compte, il est possible que vous deviez consulter un conseiller juridique et vos autorités sportives et de protection des données pour déterminer les fondements juridiques les plus appropriés à vos activités antidopage.

LES PERSONNES CONCERNÉES COMPRENNENT-ELLES L'ACTIVITÉ DE TRAITEMENT ?

Comme mentionné dans la section précédente, quels que soient les fondements juridiques sur lesquels vous vous appuyez pour traiter des renseignements personnels, vous devez vous assurer que les personnes comprennent et connaissent le traitement que vous effectuez. Pour ce faire, vous devez fournir un avis de confidentialité aux personnes concernées (voir Chapitre 5 : Comment expliquer vos pratiques de traitement).

TRAITEZ-VOUS DES RENSEIGNEMENTS PERSONNELS À DES FINS QUI NE SONT PAS DES ACTIVITÉS ANTIDOPAGE ?

Les OAD ne devraient traiter des renseignements personnels à des fins de lutte contre le dopage que dans le cadre des « activités antidopage » prévues par le Code et les Standards internationaux, ou comme le prévoit ou l'exige la loi. Ces activités antidopage comprennent :

- L'éducation ;
- Les contrôles et analyses d'échantillons ;
- La gestion du passeport biologique de l'athlète (PBA) ;
- Le traitement des demandes d'AUT ;
- Recueillir des renseignements et mener des enquêtes ;
- La gestion des résultats ; et
- La supervision de la conformité et sa mise en application.

Dans les circonstances exceptionnelles où vous constatez que votre organisation traite des renseignements personnels à des fins non encore prévues par le Code ou les Standards internationaux, **le SIPRP exige que vous réalisiez et documentiez une évaluation pour vous assurer que ces objectifs sont pertinents pour la lutte pour un sport propre.** Cette disposition vise à prendre en compte les processus antidopage nouveaux ou innovants qui peuvent être mis au point entre les cycles de révision du Code. Elle ne sera pertinente que dans ces circonstances limitées.

Pour vous aider dans cette évaluation, réfléchissez aux questions suivantes :

- Comment cette nouvelle activité de traitement va-t-elle accroître l'efficacité de la lutte pour un sport propre ? Existe-t-il des preuves scientifiques ou autres qui démontrent que c'est le cas ?
- Les parties prenantes ont-elles été consultées ? L'AMA a-t-elle été consultée ?
- Quels sont les objectifs du Code que l'activité de traitement cherche à atteindre ?
- Même s'il s'agit d'une nouvelle activité, existe-t-il des dispositions du Code ou de Standard international qui s'appliquent à cette activité ?
- Cette activité comporte-t-elle des risques pour les individus ?

4. Évaluer et atténuer les risques

L'étape finale, après avoir documenté votre activité de traitement et avoir défini les exigences du SIPRP, consiste à évaluer et à atténuer les risques. Si vous avez identifié certaines lacunes par rapport aux exigences du SIPRP dans la section précédente, celles-ci doivent également être incluses dans votre évaluation et votre atténuation des risques.

Selon le SIPRP, une évaluation des risques n'est requise que pour les informations de localisation et les renseignements personnels sensibles. Cette évaluation doit être répétée régulièrement. Il est de bonne pratique d'aller au-delà de l'exigence du SIPRP et de procéder à cette évaluation pour toutes vos activités. Si vous évaluez de manière critique vos activités de traitement au fur et à mesure que vous les documentez, vous constaterez que vous pouvez facilement et efficacement identifier les domaines à améliorer.

Bien que le SIPRP ne définit pas la fréquence d'une évaluation régulière, il serait prudent de procéder à une évaluation au moins annuelle. Il serait également prudent de réévaluer une activité de traitement lorsque des modifications à cette activité ou aux systèmes techniques utilisés dans le cadre de cette activité sont envisagées.

Tout comme cela a été fait pour votre registre de traitement, commencez par créer un cadre pour enregistrer votre évaluation et les mesures que vous devez prendre pour atténuer les risques identifiés. Voir le modèle de matrice d'évaluation des risques de l'AMA pour un exemple de la manière d'identifier et d'évaluer les risques de la gestion des AUT.

Lorsque vous effectuez votre évaluation des risques, pensez à poser des questions comme :

- Les sportifs (ou d'autres personnes) reçoivent-ils **suffisamment d'informations** pour comprendre comment leurs renseignements personnels seront traités par les signataires, l'AMA, les tiers mandataires et d'autres tiers ?
  - Pour des conseils, voir Chapitre 5 : Comment expliquer vos pratiques de traitement.
- Quel personnel a accès aux renseignements personnels ? En ont-ils tous besoin pour remplir leurs fonctions ? Certains membres du personnel peuvent-ils remplir leurs fonctions en ne disposant que de renseignements personnels limités ?
- L'accès aux renseignements personnels **est-il limité et contrôlé** dans chaque système où ces informations sont stockées ou traitées (par exemple, documents internes, ADAMS, systèmes internes de gestion des documents, etc.)
- Considérez si des mesures de « **privacy-by-design** » (prise en compte du respect de la vie privée dès la conception) pourraient être appliquées à chaque système ou application concerné pour atténuer les risques de l'activité.
  - Les mesures de protection des renseignements personnels dès la conception incluraient un contrôle granulaire des privilèges d'accès pour garantir un accès selon le principe du besoin d'en connaître, des processus automatisés de suppression des données, s'assurer que tout système ou application de ce type n'exige des utilisateurs que la saisie d'informations pertinentes et proportionnées, etc.
- Est-ce que les renseignements personnels sont **supprimés** de chacun de ces systèmes conformément à l'Annexe A du SIPRP ?
- Quelles **exigences d'authentification** (par exemple, mots de passe, l'authentification à deux facteurs, etc.) existent pour chacun de ces systèmes ?
- Lorsque des renseignements personnels sont partagés, sont-ils protégées par **cryptage**, **contrôles d'accès** ou d'autres mesures ?
- Est-ce que tous les destinataires de renseignements personnels **ont signé un accord de confidentialité** ou sont-ils soumis à des obligations légales de confidentialité ?

Les OAD devraient examiner si des exigences spécifiques s'attachent à ces évaluations des risques, ou si des évaluations supplémentaires sont requises en vertu des lois applicables. Par exemple, une OAD peut être tenue de réaliser une évaluation de l'impact sur la protection des données pour ses activités antidopage, et les autorités règlementaires peuvent avoir publié des lignes directrices précisant les informations à inclure dans cette évaluation.

Si vous effectuez déjà des évaluations des risques plus générales dans le cadre d'une activité spécifique, envisagez d'intégrer des questions d'évaluation de la protection des renseignements personnels afin de rationaliser votre conformité aux exigences des différents Standards internationaux.

Par exemple, les OAD ont le pouvoir discrétionnaire, en vertu du SICE, de recueillir différents types et quantités d'informations sur la localisation auprès de différents niveaux de sportifs. Les OAD doivent procéder à une évaluation des risques en tenant compte d'un certain nombre de facteurs lors de l'établissement de ces niveaux de localisation. De même, les OAD ont le pouvoir discrétionnaire d'appliquer les règles antidopage à des sportifs autres que les sportifs de niveau international ou national, ce qui entraînera la collecte de renseignements personnels concernant ces sportifs. En intégrant le respect de la vie privée dans vos processus d'évaluation existants, vous disposerez d'une évaluation globale plus complète et vous atténuerez les risques de manière proactive.

CHAPITRE 5 :

Comment expliquer vos pratiques de traitement

1. Préparer un avis de confidentialité

Les OAD doivent faire preuve d'ouverture et de transparence dans le traitement des renseignements personnels. Pour ce faire, les personnes concernées doivent être informées des activités de traitement de données de l'OAD et de toute information connexe avant ou pendant la collecte de renseignements auprès de ces personnes.

QUE FAUT-IL INCLURE ?

Un avis doit fournir aux personnes concernées les réponses aux questions suivantes : Qui, quoi, pourquoi, comment et quels sont mes droits et mes choix en matière de vie privée ?

QUI ?

Les OAD doivent informer les participants de :

- L'identité de l'OAD qui collecte les renseignements personnels ;
- Les coordonnées de leur Responsable de la protection des renseignements personnels ; et
- Les catégories d'organisations qui recevront les renseignements personnels (par exemple, l'AMA, d'autres signataires ou de tiers délégués)

QUOI ?

Les OAD doivent décrire les types de renseignements personnels qui seront traités. Consultez votre registre de traitement pour vous assurer que votre avis décrit les types de renseignements personnels qui seront traités pour chaque activité concernée. Pour la plupart des activités antidopage, il s'agira généralement de coordonnées et de données démographiques de base, ainsi que d'informations issues de l'analyse des échantillons. Les informations de localisation, les informations médicales et les informations liées aux sanctions seront également traitées pour certaines activités antidopage.

POURQUOI ?

Les OAD doivent expliquer pourquoi elles traitent des renseignements personnels, ou en d'autres termes, quels sont les buts ou objectifs de leurs activités de traitement. Soyez aussi précis que possible, en tenant compte du contexte dans lequel les personnes verront un avis particulier. Par exemple, la mission des OAD est généralement de détecter, dissuader et prévenir le dopage dans le sport. Toutefois, les objectifs qui nécessitent le traitement de renseignements personnels liés à la gestion des AUT seront plus restreints, par exemple s'assurer que les critères pour l'octroi des AUT ont été remplis.

COMMENT ?

Les OAD doivent expliquer comment et dans quelles conditions les renseignements personnels seront traités. Au minimum, il s'agirait notamment d'informer les participants de:

- La durée de conservation des renseignements personnels ou les critères utilisés pour déterminer cette période ;
- Quand et quels renseignements personnels seront divulgués publiquement dans le cadre d'une VRAD; et
- Tout autre information nécessaire pour garantir que le traitement des renseignements personnels reste loyal (voir l'encadré ci-dessous pour plus d'informations).

QUELS SONT MES DROITS ET MES CHOIX EN MATIÈRE DE PROTECTION DES RENSEIGNEMENTS PERSONNELS ?

Les personnes doivent être informées de leurs droits et de leurs choix en matière de protection des renseignements personnels dans le cadre du SIPRP (et des lois applicables, le cas échéant) et de la manière d'exercer ces droits et ces choix, ainsi que des conséquences de l'exercice de ces droits et de ces choix. Il s'agirait notamment d'informer les participants de :

- Leur droit d'accès aux renseignements personnels et le droit de faire corriger, bloquer ou supprimer des informations si leur traitement est inexact, incomplet ou excessif ;
- Leur droit de déposer une plainte auprès de l'OAD, le droit d'informer l'AMA si la plainte n'est pas résolue et, lorsqu'il existe, le droit de déposer une plainte auprès d'une autorité compétente en matière de protection des données ;
- Les conséquences négatives qui pourraient découler d'un refus de participer à des contrôles antidopage (telles qu'une violation du Code, l'invalidation des résultats d'une compétition ou l'interdiction de participer à un sport organisé) ;
- Du fait que, malgré une demande de bloquer ou de supprimer des informations, ou malgré un retrait de consentement au traitement, les OAD peuvent avoir besoin de continuer à traiter ces renseignements personnels pour des enquêtes ou des procédures relatives à des violations des règles antidopage, ou pour établir, exercer ou se défendre contre des actions en justice relatives à l'OAD, à l'individu, ou aux deux.

Les OAD doivent également être conscientes de toute exigence particulière prévue par le droit applicable concernant leur avis de confidentialité. Par exemple, les OAD soumises au RGPD devraient examiner les Articles 13 et 14 du RGPD et déterminer si elles doivent fournir des informations supplémentaires, telles que : le fondement juridique ou le motif de leur traitement ; des détails sur tout traitement purement automatisé de renseignements personnels qui pourrait affecter de manière significative les individus ; des informations sur les transferts de renseignements personnels vers un autre pays (par exemple, que ces transferts comportent certains risques, quels mécanismes juridiques sont utilisés pour effectuer le transfert et, éventuellement, accorder l'accès aux mécanismes utilisés - voir Chapitre 8 : Comment partager les renseignements personnels de manière responsable); ou des informations sur tout droit supplémentaire en vertu des lois applicables (voir 1. Comprendre les droits individuels en matière de renseignements personnels dans Chapitre 10 : Comment répondre aux demandes et aux plaintes.

COMMENT LE RÉDIGER

Utilisez un langage clair et simple lors de la préparation de votre avis de confidentialité en gardant à l'esprit que des personnes d'âges et de niveaux de compréhension de la lecture différents le recevront. Pensez au type de langage utilisé dans vos programmes d'éducation - c'est un bon point de référence pour examiner vos avis de confidentialité. Vos avis de confidentialité sont destinés à informer les sportifs sur la manière dont vous traitez leurs renseignements personnels à des fins de lutte contre le dopage. Il peut également y avoir des outils intégrés à un logiciel de traitement de texte qui peuvent vous aider à identifier et à ajuster le niveau de lecture de votre document. Pour rendre vos avis de confidentialité encore plus compréhensibles, envisagez de mettre en œuvre d'autres bonnes pratiques telles que[7] :

- Permettre aux individus de contrôler la quantité de détails qu'ils souhaitent recevoir, et quand ;
- Tenir compte de la perspective, de l'âge et du niveau de compréhension de la lecture de l'individu lorsque vous concevez votre avis ;
- Adopter des méthodes de notification innovantes et créatives, qui sont juste à temps, spécifiques au contexte et adaptées au type d'interface (par exemple, en utilisant des vidéos, des infographiques, des icônes, etc.) ;
- Impliquer des concepteurs d'interaction/expérience utilisateur (UI/UX) ;
- Consulter des experts et/ou des autorités en matière de protection des renseignements personnels ; et/ou
- Porter à l'attention des personnes concernées les modifications importantes apportées à votre avis de confidentialité.

2. Communiquer votre avis de confidentialité aux bonnes personnes, au bon moment et de la bonne manière

QUAND ET COMMENT FOURNIR UN AVIS DE CONFIDENTIALITÉ

Votre avis de confidentialité doit être fourni aux personnes avant ou au moment de la collecte de renseignements personnels les concernant (voir Quand pouvez-vous retarder la fourniture de cet avis ? (voir ci-dessous pour les exceptions limitées).

[7] Adapté des Lignes directrices pour l'obtention d'un consentement valable du Commissariat à la protection de la vie privée du Canada (mai 2018), https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/collecte-de-renseignements-personnels/consentement/gl_omc_201805/ (dernier accès le 14 octobre 2020).

Par exemple, vous pouvez fournir un avis de confidentialité avant de recueillir des renseignements personnels en publiant un avis général de confidentialité sur votre site web à des fins d'information, ou en l'incluant dans vos règles antidopage. Des exemples d'avis de confidentialité fournis au moment de la collecte de renseignements personnels pourraient être un avis de confidentialité inclus dans votre formulaire de contrôle du dopage, dans votre formulaire de demande de licence, dans votre formulaire d'inscription à une manifestation sportive, ou dans le cadre de la connexion d'un sportif au système antidopage de votre organisation.

Nous recommandons que les OAD fournissent à la fois :

- des avis généraux sur la protection des renseignements personnels qui sont facilement accessibles ; et
- des avis spécifiques aux points d'interaction avec les sportifs qui impliquent la collecte de renseignements personnels.

Il peut vous être utile de tracer le parcours du sportif et d'identifier les contextes ou les évènements où vous aurez une interaction directe avec les sportifs, par exemple, une demande de licence ou d'accréditation/inscription, une séance de prélèvement d'échantillons, une demande d'AUT, l'inclusion dans un groupe de contrôle ou d'éducation, etc. Ce sont là de bonnes occasions pour vous d'inclure un avis de confidentialité dans les informations que vous fournissez aux sportifs. Si de tiers mandataires agissent en votre nom dans l'un de ces scénarios, assurez-vous qu'ils sont munis de votre avis de confidentialité approuvé, ou que vous avez examiné et approuvé l'avis de confidentialité qu'ils ont l'intention d'utiliser. N'oubliez pas que les OAD peuvent également être de tiers mandataires lorsqu'elles mènent une activité antidopage, comme une séance de prélèvement d'échantillons, sous l'autorité d'une autre OAD et en vertu d'une délégation de celle-ci.

Vous pouvez fournir un avis de confidentialité verbalement, par écrit ou par des moyens visuels comme des vidéos ou des icônes. Dans tous les cas, il est bon de conserver une copie de l'avis que vous donnez. Cela sera également important pour démontrer votre conformité dans le cadre d'un audit de conformité de l'AMA. Par exemple, si vous donnez un avis verbal lors d'une manifestation sportive expliquant que des contrôles antidopage pourraient être effectués et qu'ils impliqueront le traitement de renseignements personnels, vous pourriez conserver un document détaillant les informations que le personnel a été formé à fournir aux individus.

QUAND POUVEZ-VOUS RETARDER LA FOURNITURE DE CET AVIS ?

Les OAD peuvent retarder la communication d'un avis de confidentialité aux personnes lorsque cette communication pourrait raisonnablement compromettre une enquête antidopage en cours ou prévue ou porter atteinte à l'intégrité du processus antidopage.

Cela ne serait autorisé que dans des circonstances limitées et, dans de nombreux cas, les OAD devraient quand même être en mesure de fournir un préavis sur les types de traitement de renseignements personnels qu'elles effectuent et qui peuvent ne pas être immédiatement évidents pour un sportif ou une autre personne.

Dans tous les cas, un avis approprié devrait être fourni aux personnes concernées dès que cela est raisonnablement possible, et s'il était nécessaire de retarder la fourniture de cet avis, la justification du retard devrait être documentée.

Les deux exemples suivants illustrent la manière dont les OAD peuvent informer à l'avance de leurs activités de traitement.

EXEMPLE DE CONTRÔLE SANS PRÉAVIS

Une FI gardienne du passeport a un accord avec une ONAD partenaire, selon lequel l'ONAD partenaire effectue un certain nombre de contrôles PBA sur demande de la FI agissant sur la base de renseignements liés aux passeports biologiques des sportifs. L'ONAD inclura également ces contrôles dans son propre programme de contrôles.

La FI gardienne du passeport devra fournir à l'ONAD les informations nécessaires pour effectuer une mission de contrôle. Au moment du prélèvement de l'échantillon, l'ONAD devra fournir au sportif un avis de confidentialité expliquant comment elle traitera les renseignements personnels du sportif. L'ONAD n'aurait pas pu envoyer un avis de confidentialité au sportif au moment de la collecte des informations sur sa localisation sans porter atteinte à l'intégrité du contrôle sans préavis. Toutefois, le sportif devrait déjà avoir été informé - par le gardien du passeport et/ou de l'ONAD principale du sportif - de la réception possible de ses renseignements personnels par d'autres organisations antidopage ayant l'autorité de le contrôler, et des raisons pour lesquelles les informations sur la localisation et de passeport pourraient être utilisés.

EXEMPLE D'ENQUÊTES

Si une OAD enquête un individu qui n'est pas un sportif, et qui n'a donc peut-être pas reçu les avis de confidentialité de l'OAD dans le cadre d'un contrôle du dopage ou dans d'autres contextes antidopage, l'OAD peut ne pas être en mesure d'informer l'individu du traitement de ses renseignements personnels jusqu'à ce que l'enquête soit terminée. L'OAD doit cependant prendre des mesures pour s'assurer que toute personne soumise à ses règles reçoive (ou au moins ait accès) à des informations sur la manière dont elle traitera les renseignements personnels, y compris dans le cadre d'une enquête. Cet exemple montre pourquoi il peut être particulièrement utile pour les OAD de disposer d'un avis général de confidentialité qui soit facilement accessible.

OÙ TROUVER DE L'AIDE

Il existe de nombreux modèles de l'AMA que vous pouvez utiliser pour vous aider à fournir des avis de confidentialité appropriés à des moments pertinents du parcours du sportif :

- Le modèle de formulaire de contrôle du dopage de l'AMA contient un avis de confidentialité que vous pouvez utiliser pour donner un avis dans le cadre d'une séance de prélèvement d'échantillons ;
- Le modèle de formulaire de demande d'AUT de l'AMA contient un avis de confidentialité adapté au contexte de l'AUT ; et
- Le modèle d'avis de confidentialité antidopage (forme longue) peut être utilisé comme notice générale de confidentialité antidopage.
- Le modèle d'avis de confidentialité antidopage (forme abrégée) peut être utilisé dans d'autres formulaires que les sportifs doivent remplir ou recevoir, tel qu'une demande de licence ou un formulaire d'inscription à une manifestation.

3. Obtenir un consentement valable si vous en avez besoin

Comme nous l'avons vu plus haut (voir **Quel est votre fondement juridique de traitement ?** dans 3. Appliquer les exigences du SIPRP, Chapitre 4 : Comment identifier ce que vous détenez et pourquoi), un consentement valable est étroitement lié à la fourniture d'un avis approprié. Le principe de base est qu'un avis approprié est nécessaire pour que le consentement soit informé et, par conséquent, valable.

CONDITIONS DE VALIDITÉ DU CONSENTEMENT

Plus précisément, **selon le SIPRP, le consentement doit être éclairé, donné librement, spécifique et univoque.** En général, si vous avez suivi les exigences et les meilleures pratiques en matière d'avis de confidentialité que nous avons décrites dans les présentes Lignes directrices, vous serez bien placé pour démontrer que vous avez rempli les conditions d'un consentement valable. Dans la section suivante, nous nous concentrerons sur les mesures supplémentaires à prendre si le consentement est le fondement juridique du traitement des renseignements personnels.

Pour que le consentement soit **informé et libre,** les personnes concernées doivent avoir reçu toutes les informations décrites ci-dessus sur les questions « qui, quoi, pourquoi, comment et quels sont mes droits et mes choix en matière de vie privée » (voir Chapitre 5 : Comment expliquer vos pratiques de traitement). Il est particulièrement important de décrire les conséquences négatives qui pourraient résulter du refus de donner son consentement au traitement de renseignements personnels, et de décrire les circonstances dans lesquelles vous pourriez devoir continuer à traiter des renseignements personnels même après le retrait du consentement.

Adapter vos avis de confidentialité au contexte spécifique (par exemple, une session de prélèvement d'échantillons ou une demande d'AUT) vous aidera à répondre à l'exigence d'un consentement **spécifique et univoque**. Vous devez également prévoir un mécanisme permettant au sportif de confirmer qu'il comprend votre avis de confidentialité et qu'il accepte que vous traitiez ses renseignements personnels (par exemple, une signature, une case à cocher, un bouton « Accepter » ou « Refuser »). Cela devient une

exigence lors du traitement de renseignements personnels sensibles, pour lesquelles vous devez obtenir un consentement « explicite ».

Le consentement **explicite** est un critère légèrement plus élevé que le consentement « spécifique et univoque ». La différence entre les deux critères n'est cependant pas particulièrement grande. Tout consentement doit comporter une indication spécifique, éclairée et univoque des souhaits de la personne.

La différence essentielle est que le consentement « explicite » doit être affirmé dans une déclaration claire (qu'elle soit orale ou écrite), alors qu'un consentement univoque peut inclure un consentement déduit des actions d'une personne.

Un exemple de consentement univoque, mais non explicite, pourrait être lorsqu'un sportif est clairement informé des conséquences de la création d'un compte en ligne dans une base de données antidopage et qu'il procède à cette création. Un consentement explicite serait obtenu lorsqu'un sportif se voit présenter un formulaire antidopage et appose sa signature ou coche une case pour prouver son consentement à la collecte et au traitement de ses renseignements personnels.

QUELLES SONT LES ADAPTATIONS À ENVISAGER POUR LES MINEURS ET LES PERSONNES PROTÉGÉES

Lorsqu'une personne est incapable de donner un consentement valable en raison de son âge (mineurs), de sa capacité mentale ou d'autres raisons légitimes reconnues par la loi, un parent, un tuteur légal ou un autre représentant peut donner son consentement au nom de la personne. Pensez à inclure un espace dans votre avis de confidentialité ou votre formulaire de consentement pour documenter le consentement d'un parent ou d'un autre représentant au nom d'une personne, le cas échéant.

Dans la mesure du possible, les OAD doivent vérifier la relation entre la personne et le représentant. Cette vérification n'exige pas nécessairement des documents séparés. Par exemple, un parent pourrait accompagner un sportif mineur lors d'une séance de prélèvement d'échantillons lors d'une manifestation sportive, où le mineur confirme verbalement la relation. Lorsque le représentant a une relation plus éloignée avec l'individu, il peut être prudent d'exiger des documents. Par exemple, un entraîneur ou un formateur pourrait avoir reçu une lettre signée par un parent l'autorisant à signer un document pour un sportif mineur au nom du parent.

COMMENT TRAITER UN REFUS DE CONSENTEMENT OU UN RETRAIT DE CONSENTEMENT

Tout refus ou retrait de consentement nécessitera une évaluation des circonstances au cas par cas. À un haut niveau, le refus de consentir aux règles antidopage d'une OAD qui exigent le traitement de renseignements personnels peut rendre la personne inéligible à participer à d'autres manifestations sportives.

À un niveau plus granulaire, en fonction du moment du retrait ou du refus, une OAD peut avoir besoin de déterminer si ce dernier équivaut à une violation des règles antidopage (VRAD) en vertu du Code (par exemple, en vertu de l'Article 2.3 - Évasion, refus ou défaut de se soumettre à un prélèvement d'échantillon, 2.4 - Manquement à l'obligation de transmettre des informations sur la localisation, ou 2.5 - Falsification).

L'OAD devra également déterminer si elle doit continuer à traiter des renseignements personnels pour remplir ses obligations en vertu du Code (par exemple, pour mener des enquêtes ou des analyses d'échantillons ou pour mener à bien des procédures de gestion des résultats liées à d'éventuelles VRAD) ou pour établir, exercer ou se défendre ou défendre d'autres personnes contre des actions en justice.

Dans tous les cas, les OAD doivent tenir la personne informée, fournir les raisons de leurs actions et suivre les autres processus décrits dans Chapitre 10 : Comment répondre aux demandes et aux plaintes.

PARTIE B : PROTECTION DES RENSEIGNEMENTS PERSONNELS ET PRÉPARATION À UNE ATTEINTE ÉVENTUELLE

La Partie B comprend les Chapitres 6 et 7 et apportera un soutien à l'Article 9.0 du SIPRP - Préservation de la sécurité des renseignements personnels. Elle vous aidera à comprendre ce que vous devez faire pour protéger les renseignements personnels, comment vous préparer à une atteinte à la sécurité et ce qu'il faut faire en cas d'atteinte à la sécurité.

CHAPITRE 6 :

Comment protéger les renseignements personnels

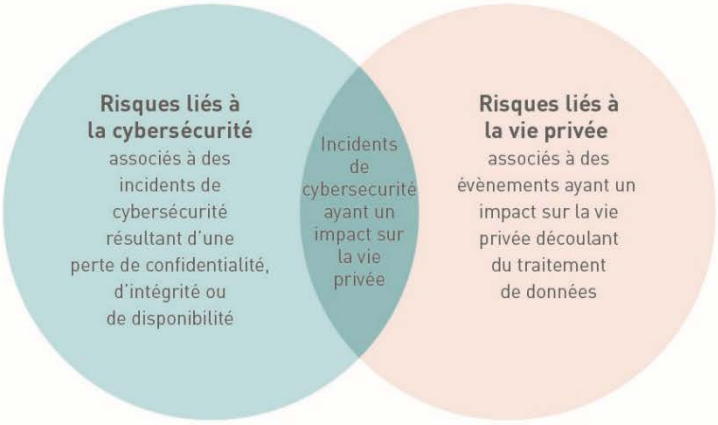
1. Élaborer et mettre en œuvre un programme de sécurité de l'information

Les OAD ont la responsabilité de protéger les renseignements personnels en leur possession en appliquant des mesures de sécurité adaptées à la sensibilité des renseignements personnels. Cela comprend des mesures physiques, organisationnelles, techniques, environnementales et autres. L'objectif de ces mesures est de protéger les renseignements personnels contre une atteinte à la sécurité.

La notion d'atteinte à la sécurité est large dans le cadre du SIPRP - il s'agit d'une « atteinte à la sécurité entraînant la perte, le vol, l'endommagement ou le traitement non autorisé et/ou illégal de renseignements personnels (...) ou toute manipulation d'un système d'information de nature à compromettre la protection, la sécurité, la confidentialité, la disponibilité ou l'intégrité de renseignements personnels. »

Pour protéger efficacement les renseignements personnels et se conformer à cette exigence du SIPRP, les OAD doivent élaborer et mettre en œuvre un programme de sécurité de l'information. Un programme de sécurité de l'information est un élément clé de votre programme de protection des renseignements personnels, mais c'est aussi son propre programme distinct qui nécessite des ressources humaines et financières dédiées.

Pour mieux comprendre où la vie privée et la sécurité de l'information se chevauchent, examinez le graphique suivant, qui illustre les différents risques que les programmes de protection des renseignements personnels et de sécurité de l'information cherchent à traiter :



Les risques de cybersécurité peuvent être conceptualisés comme des problèmes découlant d'une activité non autorisée entraînant une perte de confidentialité, d'intégrité et/ou de disponibilité des données.

Confidentialité : Les données sont conservées à l'abri de tout accès ou toute utilisation non autorisée. Les risques comprennent la perte d'informations confidentielles.

L'intégrité : Les données sont fiables et précises. Les risques comprennent les erreurs dues à une mauvaise configuration du système ou à une erreur humaine, ou les attaques malveillantes impliquant une manipulation des données.

Disponibilité : Les données sont disponibles pour être utilisées en cas de besoin. Les risques peuvent inclure des logiciels de rançon ou une attaque par déni de service distribué.

Figure 2 - Risques liés à la vie privée et à la cybersécurité[8]

Les risques liés à la cybersécurité se recoupent avec les risques liés à la vie privée lorsqu'ils ont un impact sur les renseignements personnels, par exemple, une perte de renseignements personnels ou une attaque de logiciel de rançon impliquant un système qui abrite des renseignements personnels. À l'inverse, si une attaque par déni de service distribué rend indisponible votre site web, il n'y a pas de chevauchement avec les risques liés à la vie privée.

Il est important de se rappeler que, si un programme de sécurité de l'information est essentiel pour protéger les renseignements personnels contre certains types de risques, il ne suffira pas à traiter tous les risques liés à la vie privée. Prenons par exemple un système qui a été programmé pour collecter certaines données. Le système fonctionne correctement et en toute sécurité, mais il collecte en fait trop de données, en violation du principe de minimisation des données. Ce risque pour la vie privée ne serait identifié qu'après évaluation de l'activité de traitement des données et des systèmes informatiques connexes, comme indiqué dans Chapitre 4 : Comment identifier ce que vous détenez et pourquoi.

QUELS SONT LES ACTIFS QUE VOUS DEVEZ PROTÉGER ?

Tout comme votre programme des renseignements personnels, un bon point de départ pour élaborer un programme de sécurité de l'information est de comprendre les informations que vous détenez, vos activités et les systèmes, applications et logiciels utilisés pour traiter ces informations.

QUELS SONT LES RISQUES ?

Ensuite, pour comprendre les cyberrisques auxquels vous êtes confronté, répertoriez les effets de toute perte de confidentialité, d'intégrité ou de disponibilité pour chacun de vos actifs informationnels. Vous devez considérer ces effets de la perspective à la fois de vos opérations et des personnes dont vous détenez les informations.

QUI EN EST RESPONSABLE ?

Enfin, vous devez attribuer la responsabilité pour la protection de vos actifs. Demandez-vous si vous disposez des compétences nécessaires en interne, si vous devez embaucher du personnel supplémentaire ou si vous pouvez confier la responsabilité de certaines parties de votre programme à des experts ou des prestataires de services externes.

[8] Adapté du cadre du NIST (National Institute of Standards and Technology (US Dept of Commerce) Privacy Framework : A Tool For Improving Privacy Through Enterprise Risk Management, version 1.0, 16 janvier 2020 (Figure 2 : Relation entre la cybersécurité et le risque de violation de la vie privée). https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01162020.pdf (dernier accès le 14 octobre 2020).

2. Mettre en œuvre des mesures de sécurité appropriées

Vous aurez besoin d'une combinaison de différentes mesures de sécurité pour protéger efficacement les renseignements personnels. Dans la prochaine section, nous passerons en revue des exemples pratiques de mesures que vous pouvez mettre en œuvre dans les quatre catégories mentionnées dans le SIPRP.

Nous vous encourageons également à écouter le webinaire SIPRP, *Cybersecurity Essentials for ADOs* (en anglais), pour plus de conseils sur la mise en œuvre des mesures de sécurité. De nombreux gouvernements ou autorités réglementaires ont également publié des conseils sur la sécurité des données et la cybersécurité[9].

QUE SONT LES MESURES PHYSIQUES ET ENVIRONNEMENTALES ?

Les mesures de sécurité physique comprennent :

- Les armoires à dossiers verrouillées ;
- Les systèmes d'accès par carte ;
- Les clés physiques ;
- Les registres des entrées pour l'accès des visiteurs aux bureaux physiques, aux postes de contrôle antidopage, aux centres de données ou à d'autres lieux où des renseignements personnels sont traités ou stockés ;
- La surveillance par caméra des points d'entrée/sortie ; et
- L'élimination sécurisée des fichiers physiques confidentiels (par exemple, déchiquetage).

Les mesures environnementales sont des mesures de protection contre la perte ou la destruction accidentelle des renseignements personnels à la suite de facteurs ou d'incidents environnementaux, telles qu'un incendie, une inondation ou une panne de courant. Les détecteurs de fumée et les systèmes d'extinction des incendies en sont des exemples.

Si vous êtes propriétaire ou locataire d'un espace de bureau dans un immeuble de bureaux, il est possible que le propriétaire ou le gestionnaire de l'immeuble soit responsable de la mise en œuvre d'un certain nombre de ces mesures. Faites l'inventaire de votre espace de bureau spécifique et documentez les mesures physiques et environnementales mises en place.

Si vous utilisez des services infonuagiques, votre fournisseur est généralement responsable de la mise en œuvre de mesures de protection physique et environnementale appropriées pour protéger ses centres de données. Vérifiez les accords que vous avez passés avec ces fournisseurs ou demandez à votre

[9] Voir par exemple : Contrôles de base de la cybersécurité pour les petites et moyennes organisations (gouvernement du Canada), https://cyber.gc.ca/fr/orientation/controles-de-cybersecurite-de-base-pour-les-petites-et-moyennes-organisations; Data Security Guidance (Commission irlandaise de protection des données), https://www.dataprotection.ie/en/organisations/know-your-obligations/data-security-guidance) ; Cyber Essentials (Centre de sécurité nationale, Royaume-Uni), https://www.ncsc.gov.uk/cyberessentials/advice; Guides de la CNIL, Sécurité des données personnelles, édition 2018, https://www.cnil.fr/sites/default/files/atoms/files/cnil_guide_securite_personnelle_gb_web.pdf; BSI IT-Basic Protection Compendium (Allemagne), https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2018.pdf?__blob=publicationFile&v=7; Code de la loi sur la cybersécurité (Espagne), https://www.boe.es/legislacion/codigos/codigo.php ?id=173_Codigo_de_Derecho_de_la_Ciberseguridad&modo=1 (pour tout ce qui précède, dernier accès le 14 octobre 2020).

représentant de compte des détails sur les mesures de protection qui ont été mises en œuvre pour les centres de données spécifiques où se trouvent vos données.

QUE SONT LES MESURES ORGANISATIONNELLES ?

Les mesures organisationnelles comprennent :

- Les politiques et procédures de sécurité de l'information ;
- La vérification des antécédents des nouveaux employés ;
- La formation et sensibilisation du personnel (voir le Chapitre 11 : Comment créer une culture de respect de la protection des renseignements personnels) ;
- Veiller à ce que votre personnel soit soumis à des obligations de confidentialité exécutoires ; et
- La mise en œuvre des processus d'approbation pour limiter l'accès aux renseignements personnels selon le principe du besoin de savoir.

Vous pouvez vous demander ce que le « **besoin de savoir ».** signifie en pratique. Ce terme est étroitement lié au principe de « minimisation des données » et il implique des contrôles tant organisationnels que techniques. Prenons l'exemple suivant :

EXEMPLE DE PROCESSUS DE CONTRÔLE D'ACCÈS

Jen est Responsable de l'éducation dans une OAD. Elle est responsable de la création et de la mise en œuvre d'un plan d'éducation, et du suivi de l'achèvement des cours de formation obligatoires pour les sportifs des groupes de contrôle de son OAD sur ADEL. Jen demande un compte ADAMS pour pouvoir télécharger la liste la plus récente des sportifs des groupes cibles de l'OAD et la comparer avec les sportifs ayant suivi des cours de formation sur ADEL.

Le Responsable d'ADAMS pose quelques questions à Jen pour clarifier sa demande :

***Q**: (Responsable d'ADAMS) À quelle fréquence devez-vous vérifier la dernière liste de sportifs ?*

***A**: (Jen) Pas très souvent. Je fais généralement un recoupement tous les quelques mois avec ma liste ADEL.*

***Q**: Avez-vous besoin d'accéder à ADAMS pour une autre raison ?*

***A**: Je ne pense pas.*

***Q**: La liste des sportifs est-elle disponible dans un fichier Excel ou dans un autre document en dehors d'ADAMS ?*

***A**: Je pense que oui, ou du moins, je pourrais probablement demander à quelqu'un qui a un compte de la télécharger pour moi.*

Sur la base des réponses de Jen, le Responsable d'ADAMS refuse la demande de Jen. Elle explique qu'il serait préférable pour Jen d'utiliser la version Excel de la liste des sportifs qu'un collègue peut télécharger pour elle. De cette façon, Jen n'aura accès qu'à la liste de sportifs concernée, plutôt qu'à des renseignements personnels supplémentaires qui auraient été disponibles pour elle avec un compte ADAMS. Elle explique que cette solution est également plus logique du point de vue de la sécurité, car il s'agit d'un compte de moins qui peut être compromis par un hameçonnage ou une autre cyberattaque.

Les procédures de contrôle d'accès d'une OAD doivent couvrir l'octroi des autorisations d'accès, le suivi et la mise à jour de ces autorisations, et la suppression des autorisations lorsque le rôle et les responsabilités d'une personne changent. Par exemple, si Jen passe à un nouveau rôle de Responsable des contrôles, elle aura alors probablement besoin d'un compte ADAMS pour planifier et suivre les contrôles. Cependant, elle n'aura peut-être plus besoin d'un compte ADEL.

QUE SONT LES MESURES TECHNIQUES ?

Les mesures de sécurité techniques contribuent à renforcer la sécurité de l'information d'une organisation en la protégeant contre les erreurs et les actions humaines.

Les mesures techniques de sécurité comprennent :

- Les exigences d'authentification (par exemple, connexion unique, mots de passe complexes, et étapes d'authentification secondaire ou à facteurs multiples, comme les codes TOTP ou SMS, l'authentification biométrique, etc.) ;
- Les restrictions techniques d'accès (par exemple, isolement ou segmentation des réseaux ou des bases de données) ;
- Le cryptage, y compris pour toute information transmise ;
- L'enregistrement et la surveillance de l'accès et des activités des utilisateurs pour garantir le respect des restrictions d'accès et aider à détecter tout accès non autorisé ou toute activité suspecte ;
- Les logiciels antivirus et pare-feux ;
- Appliquer les mises à jour et les correctifs de système ;
- Mettre en place un VPN pour l'accès à distance ;
- L'utilisation de logiciels de gestion des appareils mobiles ; et
- Appliquer des verrouillages et déconnexions automatiques des écrans sur tous les appareils.

CHAPITRE 7 :

Comment se préparer et réagir à une atteinte à la sécurité

1. Créer un plan d'intervention

Pour mieux se préparer à une atteinte à la sécurité, les OAD doivent mettre en œuvre un plan de préparation et de réaction aux atteintes à la sécurité et le tester pour s'assurer qu'il fonctionne.

QUI COMPOSE VOTRE ÉQUIPE DE RÉPONSE AUX INCIDENTS ?

Tout d'abord, identifiez votre équipe d'intervention. Vous aurez besoin d'un ensemble de compétences diverses pour répondre à une atteinte à la sécurité, notamment dans les domaines juridiques, de la protection des renseignements personnels, de l'informatique, des communications et de la haute direction. Assurez-vous que votre équipe comprend des responsables pour chacun de ces domaines d'intervention clés.

DE QUOI SERONT-ILS RESPONSABLES ?

Ensuite, documentez ce dont chaque membre de l'équipe est responsable. Envisagez de nommer un chef d'équipe ou un coordonnateur (par exemple, le Responsable de la protection des renseignements personnels) pour vous assurer que quelqu'un est responsable en dernier ressort de la gestion des différents aspects de votre réponse aux atteintes à la sécurité. N'oubliez pas d'attribuer la responsabilité de la mise en place d'activités connexes, comme la formation, la révision et la mise à jour régulière du plan, et la création d'un processus de maintien des dossiers pour consigner les informations relatives à chaque atteinte à la sécurité.

Vous devez également veiller à ce que votre personnel reçoive des instructions sur la manière de réagir rapidement en cas d'atteinte à la sécurité.

Par exemple, votre personnel doit être chargé de notifier tout incident suspect immédiatement à l'équipe d'intervention, de se conformer aux instructions de l'équipe d'intervention et de conserver tous les documents pertinents au cas où ceux-ci seraient utiles pour faire face à l'incident. Ils devraient également participer à toute formation sur la réponse aux atteintes qui leur est proposée.

AUREZ-VOUS BESOIN DE L'AIDE DE TIERS ?

Déterminez si vous aurez besoin de l'aide d'un tiers dans le cadre de votre réponse à une atteinte à la sécurité. Aurez-vous besoin d'un enquêteur judiciaire pour identifier la source et la cause d'une violation ? Aurez-vous besoin d'un soutien juridique externe ou de l'aide d'un cabinet de relations publiques ?

Certains fournisseurs de services de réponse aux incidents (tels que les enquêteurs judiciaires) offrent des solutions de mandat sans acompte pour l'organisation cliente. L'avantage de ce mandat est que l'organisation a alors accès immédiatement au fournisseur en cas d'atteinte, et n'a pas besoin de prendre le temps d'établir une relation avec ce dernier.

Vous pouvez également revoir vos polices d'assurance afin de déterminer si vous avez l'obligation d'impliquer votre assureur en cas d'atteinte.

Une fois que vous avez identifié les tiers externes avec lesquels vous serez en contact en cas d'atteinte, assurez-vous de documenter leurs fonctions ou leur rôle et leurs coordonnées dans votre plan.

COMMENT DÉFINIR LES ÉTAPES DE LA RÉPONSE

Votre plan d'intervention doit aborder et attribuer la responsabilité pour cinq étapes clés : la découverte, le confinement, l'évaluation, la notification et les mesures correctives. Ces étapes peuvent se dérouler simultanément selon le type d'atteinte et son évolution.

Les OAD devraient examiner les lois applicables et superposer ou adapter chacune de ces mesures d'intervention en fonction des exigences qui leur sont applicables.

Découverte

Documentez qui doit être notifié en cas d'atteinte à la sécurité. **Le Responsable de la protection des renseignements personnels de l'OAD doit figurer parmi les premiers à être avertis.** Identifier tout numéro ou ligne d'assistance spécifique à utiliser par le personnel pour cette notification.

Une fois qu'un incident a été signalé, le Responsable de la protection des renseignements personnels (ou un autre coordinateur d'intervention) doit documenter toutes les informations disponibles concernant l'atteinte. Considérez les questions suivantes :

- Quand l'atteinte a-t-elle été découverte ?
- Quelle est la date ou la période pendant laquelle l'incident s'est produit ?
- Quelle est la nature et la cause de l'incident ?
- Quels sont les types de personnes touchées et combien sont-elles ?
- Quels sont les systèmes concernés ou impliqués dans l'atteinte ?
- Quels types de renseignements personnels sont concernés ?
- Quels dommages éventuels pourraient résulter de la violation ?

Utilisez le modèle de compte rendu des atteintes à la sécurité, ou créez le vôtre, pour rassembler et enregistrer les détails pertinents.

Après une première évaluation de l'atteinte, le Responsable de la protection des renseignements personnels doit informer les autres membres concernés de l'équipe d'intervention afin qu'ils discutent et mettent en œuvre les mesures appropriées de confinement, de notification et de réhabilitation conformément au plan d'intervention en cas d'atteinte à la sécurité.

Confinement

Documentez qui est responsable de l'identification et de la prise de mesures de confinement appropriées. Cela pourrait impliquer :

- Des mesures de confinement techniques (telles que la mise hors ligne des systèmes, la réinitialisation forcée des mots de passe ou le lancement d'une enquête) ;
- Des actions en justice (telles que l'invocation de droits légaux en vertu de contrats lorsque l'atteinte a été causée par un tiers), ou
- D'autres mesures (telles que la communication interne et externe pour avertir les autres parties concernées de la violation et minimiser son impact).

Évaluation

Le Responsable de la protection des renseignements personnels et l'équipe d'intervention doivent enquêter et évaluer l'atteinte pour en comprendre la nature, la portée, l'impact et la gravité. Il s'agit d'une étape clé pour garantir le respect des exigences en matière de confinement et de notification.

Par exemple, la perte par un membre du personnel d'un ordinateur portable contenant des renseignements personnels limités, non sensibles, cryptés et pouvant être effacés à distance, donnera lieu à un ensemble de mesures de confinement, de notification et de réhabilitation différent de celui d'une attaque par logiciel de rançon par un attaquant malveillant et motivé affectant des fichiers contenant un volume élevé de renseignements personnels sensibles.

En particulier, les OAD devront évaluer l'atteinte à la sécurité afin de déterminer si elles sont tenues d'informer les personnes concernées. Ce sera le cas lorsque la violation est susceptible d'affecter les droits et les intérêts de l'individu de manière significative (voir 3. Répondre à une atteinte à la sécurité dans Chapitre 7 : Comment se préparer et réagir à une atteinte à la sécurité).

Notification

Documentez vos obligations de notification. Examinez notamment les circonstances dans lesquelles vous pourriez devoir notifier les groupes suivants :

- Personnes concernées ;
- Autorités règlementaires ;
- Autres entités gouvernementales ;
- OAD affectées ;
- Autres tiers concernés ; et
- Lorsqu'une atteinte implique ou peut impliquer une activité illégale, les forces de l'ordre ou autres autorités compétentes.

L'AMA encourage généralement les OAD à communiquer et à collaborer avec l'AMA et les autres OAD qui peuvent être concernées par l'atteinte ou qui ont une relation avec les personnes concernées. Lorsqu'une atteinte à la sécurité affecte le système ADAMS, les OAD sont tenues d'en informer rapidement l'AMA.

Au-delà de vos obligations de notification, il est bon de documenter et d'attribuer la responsabilité de la gestion des communications internes et externes. Le personnel peut avoir besoin d'être tenu informé des mesures à prendre pour remédier à une atteinte ou la contenir et, en cas d'incident majeur, vous pouvez avoir à répondre aux demandes des médias ou d'autres membres du public.

Les obligations de notification des atteintes à la sécurité sont de plus en plus courantes dans le monde entier, et les OAD pourraient bien être tenues de se conformer à des obligations qui vont au-delà du SIPRP en ce qui concerne les obligations de notification des atteintes à la sécurité. Les OAD peuvent également être soumises à des obligations contractuelles de notification à des tiers en cas d'atteinte.

Mesures correctives

Les mesures correctives à la suite d'une atteinte à la sécurité varient selon la cause, la nature et les circonstances de l'atteinte. Elles peuvent comprendre des garanties de sécurité renforcées, des sanctions disciplinaires pour les personnes jugées responsables de l'atteinte à la sécurité, ainsi qu'une formation et une sensibilisation accrues du personnel.

Veillez à ce que votre plan comprenne des exigences pour évaluer et mettre en œuvre des mesures correctives appropriées à la suite d'une infraction. Il peut être utile d'organiser un débreffage de l'équipe après l'incident afin d'identifier les leçons apprises et d'éviter que cela ne se reproduise. N'oubliez pas d'attribuer la responsabilité pour le suivi de la mise en œuvre des mesures correctives identifiées.

Notez que vous devez également tenir des registres appropriés concernant l'atteinte à la sécurité y compris les faits liés à l'atteinte, ses effets, l'évaluation de l'atteinte par l'OAD et les mesures correctives prises. Vous pouvez utiliser le modèle de journal des atteintes à la sécurité pour documenter ces détails, ou créer le vôtre.

2. Tester votre plan

Maintenant que vous avez créé votre plan, vous devriez le tester. Comment ? Le test de votre plan peut être aussi simple que d'utiliser un incident de violation réel rapporté dans les journaux, et d'imaginer qu'il s'est produit au sein de votre organisation. En général, la personne qui dirige votre séance de test commence par présenter les détails initiaux de la « découverte » d'une atteinte à l'équipe d'intervention. Au fur et à mesure que vous suivez les étapes de la réponse, la personne qui dirige la séance doit fournir à l'équipe d'intervention de nouvelles informations pour simuler la nature dynamique de la réponse à une atteinte.

Vous pouvez également demander l'aide d'un tiers pour vous aider à effectuer un test. De nombreux consultants ou cabinets de sécurité de l'information vous proposeront ce service.

La réalisation de ce type de test vous aidera à atteindre un certain nombre d'objectifs, notamment :

- Évaluer l'efficacité de vos processus d'intervention dans un espace sûr et sans risque ;
- Renforcer la compréhension du plan d'intervention et des responsabilités de chaque membre de l'équipe d'intervention ;
- Optimiser vos canaux de communication (par exemple, comment allez-vous maintenir l'équipe d'intervention à jour et alignée) ; et
- Obtenir des informations sur vos forces et faiblesses en matière de réponse aux atteintes.

Après le test, faites un débreffage avec votre équipe pour identifier les améliorations à apporter à votre plan.

3. Répondre à une atteinte à la sécurité

Dans le cas malheureux où vous seriez victime d'une atteinte à la sécurité, vous devrez activer votre plan et réagir. Une partie essentielle de cette réponse consiste à évaluer une atteinte à la sécurité afin de déterminer les notifications et autres mesures correctives à prendre.

COMMENT ÉVALUER UNE ATTEINTE À LA SÉCURITÉ

En vertu du SIPRP, vous devez informer les personnes concernées d'une atteinte lorsque celle-ci est susceptible d'affecter leurs droits et leurs intérêts de manière significative.

Pour déterminer si une atteinte rencontre ce standard, vous devrez procéder à une évaluation de la gravité et de l'impact d'une atteinte. Pour guider votre évaluation, posez-vous des questions telles que ;

- Quels types de renseignements personnels ont été atteints et dans quelles circonstances ? De multiples types des renseignements personnels ont-ils été atteints ?
- Quelle est la probabilité qu'une personne soit lésée par l'atteinte (par exemple, en subissant une détresse émotionnelle ou psychologique, une discrimination, un vol d'identité, une atteinte à la réputation, un préjudice économique) ?
- Depuis combien de temps les renseignements personnels ont-ils été exposés ?
- Existe-t-il des preuves d'une intention malveillante (par exemple, vol, piratage) ?
- Les informations ont-elles été exposées à des personnes/entités qui ont peu de chances de les partager d'une manière qui pourrait porter préjudice (par exemple, en cas de divulgation accidentelle à des destinataires non intentionnels qui s'engagent à détruire et à ne pas divulguer les données) ?
- Les informations ont-elles été exposées à des individus/entités inconnus ou à un grand nombre d'individus, de sorte que certaines personnes pourraient les utiliser ou les partager d'une manière qui pourrait porter préjudice ?
- Les informations sont-elles définitivement exposées à des entités/individus qui sont susceptibles d'en abuser (par exemple, des pirates informatiques), ou qui représentent un risque pour la réputation de l'individu ?
- Le préjudice s'est-il matérialisé (c'est-à-dire savez-vous que les données ont déjà été utilisées de manière abusive) ?
- Les informations ont-elles été perdues, consultées de manière inappropriée ou volées ?
- Les renseignements personnels ont-ils été récupérés ?
- Les renseignements personnels sont-ils adéquatement cryptés, anonymes ou difficilement accessibles ?

Des facteurs tels qu'un cryptage adéquat ou d'autres mesures de protection, ou la nature limitée de l'atteinte impliquant l'exposition à des entités connues qui ont supprimé les informations pertinentes tendront à atténuer la gravité et l'impact d'une atteinte. À l'inverse, un volume important ou une sensibilité élevée des renseignements personnels atteints, ou l'exposition de ces renseignements à des personnes ou des entités ayant des intentions malveillantes augmentera cette gravité et cet impact.

QUAND ET COMMENT NOTIFIER LES PERSONNES CONCERNÉES

Si vous avez déterminé que vous devez informer les personnes concernées d'une violation, **l'avis doit être envoyé dès que raisonnablement possible.** Cela signifie qu'après avoir découvert une violation, vous devez agir rapidement pour rassembler les détails pertinents, évaluer la violation, puis préparer votre notification aux personnes concernées.

La notification doit porter au minimum sur les éléments suivants:

- La nature de la violation ;
- Les conséquences négatives possibles pour les personnes concernées ; et
- Les mesures correctives prises ou à prendre par l'OAD.

Elle peut être fournie par tout moyen approprié, y compris verbalement ou par écrit, en tenant compte des circonstances particulières de l'atteinte ainsi que du préjudice que les personnes concernées peuvent subir du fait de la violation. Tout comme vous le feriez pour un avis de confidentialité, utilisez un langage clair et simple dans votre notification, et tenez compte du point de vue du destinataire de ces informations. Envisagez également de créer à l'avance un modèle de notification que vous pourrez ensuite compléter avec les détails pertinents en cas de violation.

Vous pouvez être soumis à des obligations de délai différentes pour les notifications à fournir aux personnes, aux autorités règlementaires ou à d'autres organisations en vertu des lois applicables. Par exemple, vous pouvez être tenu de fournir cette notification dans les 72 heures, lorsque cela est possible, ou sans retard injustifié. Consultez les lignes directrices des autorités règlementaires sur la manière d'interpréter et d'appliquer ces délais.

QUAND ET COMMENT INFORMER D'AUTRES ORGANISATIONS

Comme mentionné ci-dessus, l'AMA encourage les OAD à communiquer et à collaborer avec l'AMA et les autres OAD qui pourraient être affectées par l'atteinte ou qui ont une relation avec les personnes concernées. Lorsqu'une atteinte à la sécurité affecte les renseignements personnels traités via ADAMS, les OAD sont tenues d'en informer rapidement l'AMA.

Les OAD peuvent être tenues de notifier une autorité de protection des données. Les OAD peuvent également être fortement encouragées ou tenues de notifier les centres de cybersécurité ou les réseaux de renseignements sur les menaces en cas d'attaque malveillante, ou les forces de l'ordre en cas de soupçon d'activité illégale.

Dans le cadre du SIPRP, il n'y a pas d'exigences obligatoires en matière de délais ou de contenu pour la notification à d'autres organisations.

QUELLES SONT LES AUTRES MESURES CORRECTIVES QUE VOUS DEVEZ PRENDRE ?

Outre la notification des personnes et organisations concernées, vous pouvez prendre de nombreuses mesures pour remédier à une violation. Les mesures spécifiques dépendront de la nature de la violation que vous avez subie. Elles peuvent inclure :

- Reprendre une formation ou offrir une formation complémentaire à votre personnel ;
- Isoler ou désactiver les systèmes compromis ;
- Changer les mots de passe sur les systèmes compromis ;
- Essuyer à distance des appareils perdus ou volés ;
- Surveiller les journaux, les systèmes et les réseaux pour détecter des signes d'activité suspecte ; ou
- Restaurer des informations perdues à partir d'une sauvegarde.

COMMENT AMÉLIORER VOTRE RÉPONSE FUTURE

Comme toujours, pour améliorer votre gestion des atteintes futures, prenez le temps de réunir l'équipe d'intervention après avoir traité une atteinte pour faire le point sur les échecs ou les lacunes qui ont conduit à l'atteinte, les aspects positifs et négatifs de votre réponse et les leçons apprises au long du processus. Documentez ces leçons dans votre compte rendu de l'atteinte ou dans un autre document, et mettez à jour votre plan d'intervention si nécessaire.

PARTIE C : MISE EN ŒUVRE DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

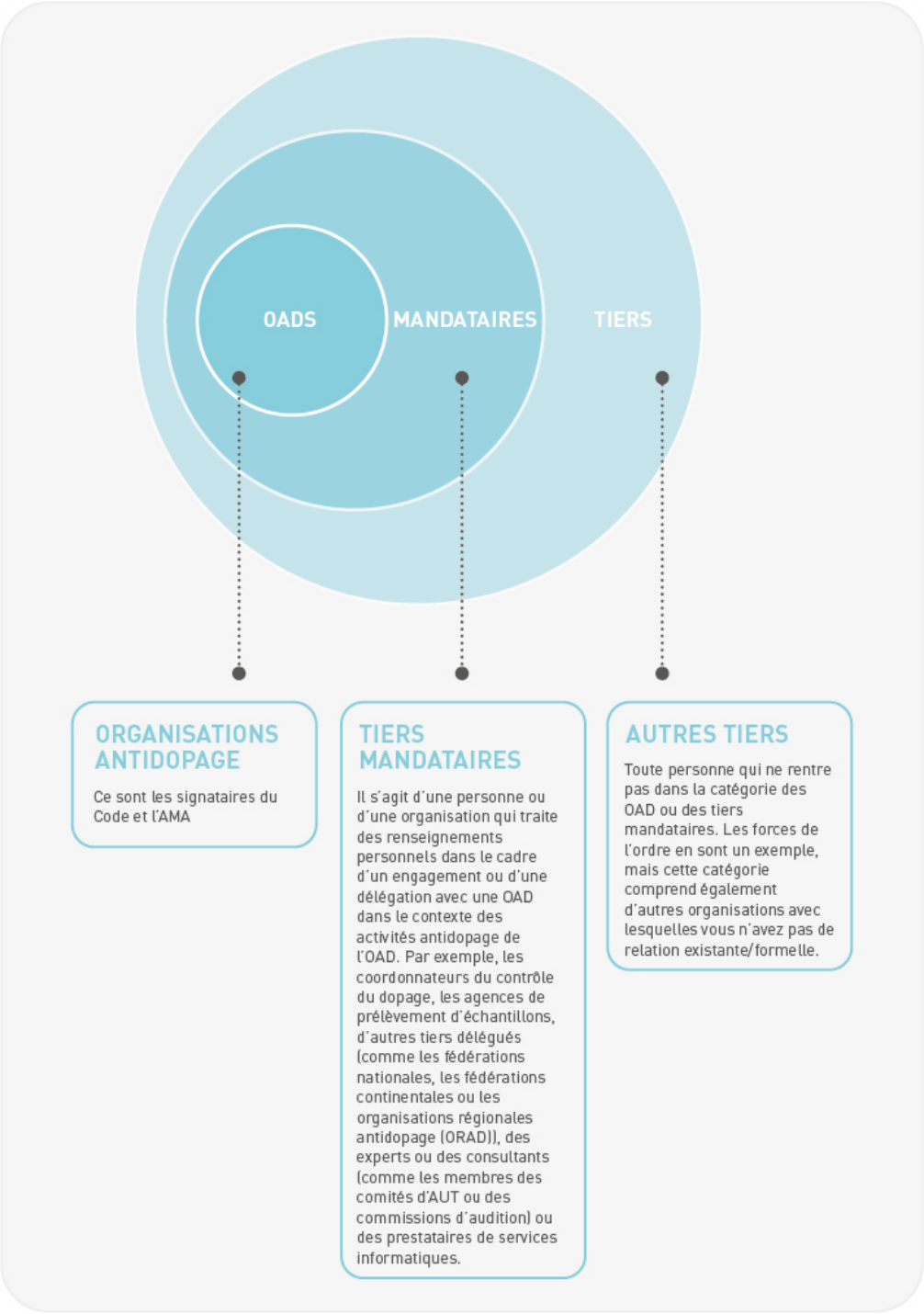
La Partie C comprend les Chapitres 8, 9 et 10 et apportera un soutien à l'Article 8.0 du SIPRP - Divulgation de renseignements personnels à d'autres organisations antidopage et à des tiers ; à l'Article 10.0 et à l'Annexe A - Conservation des renseignements personnels lorsque pertinent et destruction ; et à l'Article 11.0 - Droits des participants et des autres personnes relatifs aux renseignements personnels. Il vous aidera à gérer les risques associés au partage des renseignements personnels, à vous assurer que vous ne conservez pas les renseignements personnels plus longtemps que vous en avez besoin, et à répondre aux demandes et aux plaintes concernant vos pratiques en matière de protection des renseignements personnels.

CHAPITRE 8 :

Comment partager les renseignements personnels de manière responsable

1. Identifier et classifier les tiers

Avant de partager des renseignements personnels, vous devez comprendre avec qui vous allez les partager. Le SIPRP classe les destinataires possibles en trois catégories générales :



L'une des façons d'envisager ces trois catégories est de penser en termes de cercles de confiance. Au fur et à mesure que vous passez des OAD à des tiers, les conditions de partage des renseignements personnels dans le cadre du SIPRP deviennent plus strictes. En effet, vous avez moins de contrôle sur les destinataires lorsque vous vous rapprochez des cercles de confiance extérieurs.

En tant qu'OAD partageant des renseignements personnels avec une autre OAD, vous savez que vous êtes toutes deux soumises aux exigences du Code et des Standards internationaux (en particulier, le SIPRP). Lorsque vous passez à des tiers mandataires, vous pouvez - et êtes tenu - d'imposer certains contrôles contractuels et techniques pour continuer à protéger les renseignements personnels entre les mains du destinataire. En ce qui concerne les autres tiers, étant donné que vous n'avez pas de relation existante et que le destinataire utilisera les renseignements personnels à ses propres fins, votre contrôle effectif sur ces renseignements personnels une fois qu'elles sont entre les mains du destinataire peut être limité.

2. Appliquer les principes communs

Il existe des principes communs que vous devez appliquer lorsque vous partagez des renseignements personnels : veiller à ce qu'il y ait un besoin de partage, réduire au minimum ce qui est partagé et partager les informations en toute sécurité. En outre, vous devez garder à l'esprit votre obligation d'informer à l'avance les personnes du type de destinataires de leurs renseignements personnels (voir Chapitre 5 : Comment expliquer vos pratiques de traitement pour en savoir plus).

COMMENT IDENTIFIER UN BESOIN DE SAVOIR

Lorsque vous cherchez à déterminer si un destinataire potentiel a un besoin légitime de connaître les renseignements personnels demandés, commencez par identifier les objectifs déclarés du destinataire pour demander des renseignements personnels. Demandez-vous s'il s'agit d'une finalité légitime compte tenu des rôles et responsabilités du destinataire (que ce soit en tant que OAD, délégué d'une OAD ou autre tiers).

COMMENT MINIMISER CE QUI EST PARTAGÉ

Si le premier critère est rempli, vous devez alors essayer de réduire au minimum les renseignements personnels partagés. Réfléchissez au type et au volume de renseignements personnels strictement nécessaires pour atteindre les objectifs de la demande. Pour ce faire, n'hésitez pas à tester différents scénarios avec le destinataire :

- Pourrait-il d'abord utiliser un ensemble plus limité de renseignements personnels (par exemple, des noms) pour ensuite adapter la portée de sa demande pour d'autres types de renseignements personnels, idéalement relatifs à un groupe plus restreint de personnes ?
- Êtes-vous en mesure de confirmer simplement certains faits qui intéressent le destinataire, plutôt que de partager les renseignements personnels sous-jacents ?
- Des informations agrégées ou anonymisées/expurgées suffiraient-elles à la place ?

COMMENT PARTAGER DES INFORMATIONS EN TOUTE SÉCURITÉ

Le partage sécurisé des informations comporte deux aspects essentiels : les protections techniques et les engagements contractuels ou écrits.

En ce qui concerne les techniques de protection, les OAD devraient utiliser le cryptage ou un système de partage de fichiers sécurisé pour transmettre des renseignements personnels par voie électronique, plutôt que le courrier électronique ordinaire. Les systèmes de partage de fichiers sécurisés permettent à l'expéditeur de fixer des limites d'accès telles que des exigences d'authentification, des dates d'expiration pour l'accès ou des limites de téléchargement ou de visualisation. Le cryptage peut être quelque chose que votre système de courrier électronique vous permet d'activer pour des courriers électroniques spécifiques, mais comprend également le simple ajout d'une protection par mot de passe à un document partagé. En cas de doute, consultez vos experts informatiques internes ou externes pour déterminer quelles sont les techniques de protection dont vous disposez.

En ce qui concerne les engagements contractuels ou écrits des destinataires, ceux-ci peuvent varier considérablement selon le contexte de votre relation. Envisagez au minimum d'obtenir des garanties que les renseignements personnels seront :

- Protégés et conservés de manière confidentielle ;
- Accessibles et utilisés uniquement aux fins indiquées ; et
- Retournés ou détruits lorsque plus nécessaire.

Il arrive souvent que le transfert de renseignements personnels par-delà les frontières internationales soit régi par des lois sur la protection des données. Lorsque c'est le cas, vous devrez examiner les fondements sur lesquels vous vous basez pour effectuer ces transferts, qui pourraient impliquer le consentement d'une personne au transfert, des contrôles contractuels ou d'autres mesures. Dans certains cadres juridiques, tels que le RGPD de l'UE, les transferts qui servent des intérêts publics importants sont autorisés, et ces cadres peuvent même identifier explicitement la lutte contre le dopage comme un intérêt public important, comme celui de l'UE. De même, certaines lois sur le sport et la lutte contre le dopage autorisent expressément les transferts internationaux à de fins antidopage. Et, dans certains cas, certains pays dotés de régimes de protection des données particulièrement solides, comme ceux de l'UE, du Canada ou de la Suisse, sont réputés offrir des protections suffisamment élevées dans leur législation nationale pour qu'il soit souvent possible de transférer des données à des parties qui s'y trouvent sans autre formalités. Comme le stipule la Convention de l'UNESCO contre le dopage dans le sport, il est essentiel que les informations antidopage circulent par-delà les frontières étant donné la nature internationale du sport, et que les pays ayant ratifié la Convention mettent en œuvre des mesures appropriées pour y parvenir.

3. Partager avec d'autres OAD

QUEL PARTAGE SE FAIT-IL DANS ADAMS ?

Le système d'administration et de gestion antidopage de l'AMA (ADAMS) a été conçu pour faciliter la conduite des activités antidopage entre les organisations dont les responsabilités en matière de lutte contre le dopage se chevauchent à l'égard des sportifs et les organisations situées dans le monde entier.

À un haut niveau, les ONAD ont accès aux données relatives aux sportifs dont la nationalité sportive principale est celle de l'ONAD. Les FI ont accès aux données relatives aux sportifs associés au sport de la FI. Les organisations responsables de grandes manifestations ont accès aux données liées aux évènements qu'ils supervisent. Les OAD peuvent donner à de tiers mandataires l'accès aux données qu'ils saisissent dans ADAMS. L'AMA a accès aux données d'ADAMS pour contrôler la conformité et exploiter ADAMS. Les laboratoires ont la possibilité de communiquer les résultats tandis que les unités de gestion des passeports des athlètes gèrent les passeports.

Ces règles de partage sont basées sur la répartition des rôles et des responsabilités décrites dans le Code et les Standards internationaux. Dans ces Lignes directrices, nous nous concentrons sur des scénarios qui vont au-delà des règles de partage qui sont intégrées dans ADAMS. Pour plus de détails sur ces règles de partage, voir Quelles informations sont recueillies dans ADAMS et comment sont-elles utilisées et communiquées ? dans la FAQ sur la confidentialité et la sécurité d'ADAMS.

COMMENT ÉVALUER UNE DEMANDE AD HOC

Le SIPRP permet aux OAD de divulguer des renseignements personnels à d'autres OAD lorsque cela est nécessaire pour permettre aux OAD destinataires de remplir leurs obligations en vertu du Code.

Avant de partager des renseignements personnels avec une autre OAD, l'OAD qui les divulgue doit s'assurer que :

- La divulgation n'est pas interdite par les lois applicables de protection des données et de la vie privée ;
- L'OAD destinataire a le droit, l'autorité ou la nécessité d'obtenir les renseignements personnels demandés ;
- Les renseignements personnels demandés sont uniquement envoyés à la personne identifiée et pertinente de l'OAD destinataire ;
- Seuls les renseignements personnels qui sont nécessaires au droit, à l'autorité ou au besoin établi par l'OAD destinataire sont partagés ;
- Le mode de communication des renseignements personnels est sécurisé ; et
- Il n'y a aucune raison de croire que la divulgation compromettrait une enquête ou que l'OAD destinataire ne respecte pas le SIPRP.

En d'autres termes, vous devez vous conformer aux lois applicables, veiller à ce qu'il y ait un besoin de savoir, minimiser ce qui est partagé et protéger de manière appropriée les renseignements personnels en

transit. L'OAD requérante peut aider l'OAD divulgatrice dans son évaluation en remplissant le Modèle de formulaire de demande de divulgation. En remplissant ce formulaire, l'OAD divulgatrice pourra également documenter sa décision à des fins d'imputabilité.

EXEMPLE DE CONTRÔLE SANS PRÉAVIS

Notre exemple précédent de scénario sur les contrôles PBA est un bon exemple d'un besoin ponctuel de partager des renseignements personnels entre deux OAD. Pour résumer : L'ONAD a accepté d'effectuer un certain nombre de contrôles PBA lorsque le gardien du passeport identifie une opportunité de cibler un sportif pour un contrôle sur le territoire de l'ONAD. Pour les sportifs qui ne sont pas ressortissants de cette ONAD partenaire, mais qui s'entraînent ou participent à des compétitions sur son territoire, l'ONAD aurait l'autorité de contrôle, mais n'aurait pas accès aux informations de localisation nécessaires pour les localiser pour des contrôles sans préavis dans ADAMS, et pourrait ne jamais avoir eu d'interaction avec eux auparavant. L'ONAD demande à la FI gardienne du passeport de lui communiquer certaines informations de localisation afin qu'elle puisse localiser les sportifs à contrôler.

L'ONAD a le pouvoir de contrôler les sportifs se trouvant sur son territoire et utilisera les informations de localisation pour effectuer des contrôles sans préavis ; en d'autres termes, les objectifs de la divulgation sont compatibles avec les objectifs pour lesquels ces informations ont été recueillies. La FI gardienne du passeport doit s'assurer que les informations de localisation sont cryptées (par exemple en ajoutant un mot de passe au document ou en l'envoyant par un lien crypté plutôt que sous forme de pièce jointe à un courriel ordinaire) et que seules les informations de localisation liées à une période spécifique de l'ordre de mission, ou à une éventuelle fenêtre de contrôle, sont fournies. L'ONAD destinataire doit veiller à ce que le document contenant les informations de localisation soit supprimé lorsqu'il n'est plus nécessaire.

QUAND VOUS POUVEZ AVOIR BESOIN D'UN ACCORD DE PARTAGE DE DONNÉES

Dans les cas où les OAD ont des partenariats plus établis qui impliquent un échange régulier d'informations qui n'a pas lieu par le biais d'ADAMS (et qui n'est donc pas couvert par les accords régissant l'utilisation d'ADAMS), vous pouvez envisager d'établir un accord de partage de données à titre de bonne pratique. Il peut s'agir, par exemple, d'un accord de partage de renseignements ou d'informations concernant les passeports des sportifs ou d'autres types de renseignements. Il existe un modèle d'accord de collaboration aux fins du PBA. Ce type d'accord sert, entre autres, à documenter l'évaluation des facteurs décrits ci-dessus dans le cadre d'un accord de partage défini.

4. Partager avec les tiers mandataires

COMMENT ÉVALUER UN TIERS MANDATAIRE

Dans le deuxième cercle de confiance, on trouve les tiers mandataires. Même si vous concluez finalement un accord ou un engagement avec ce tiers mandataire, ces derniers ne sont pas directement soumis au Code et aux Standards internationaux, et vous avez donc moins de visibilité sur leurs politiques, processus et pratiques.

En conséquence, **avant que vous ne décidiez de travailler avec un tiers mandataire, le SIPRP vous demande de l'évaluer pour vous assurer qu'il peut fournir des garanties suffisantes quant aux mesures techniques et organisationnelles qui seront appliquées à son traitement des renseignements personnels**.

Pour évaluer la fiabilité de votre tiers mandataire à cet égard, assurez-vous d'abord de comprendre la nature des services qu'il fournira, s'il a besoin d'accéder à l'un de vos systèmes pour s'acquitter de ses fonctions et dans quelle mesure il doit avoir accès à des renseignements personnels pour s'acquitter de ses fonctions. Cela découle des principes communs évoqués ci-dessus.

Posez des questions à vos tiers mandataires et obtenez des pièces justificatives pour vérifier leurs pratiques. Voici quelques exemples :

- Quelles sont les fins auxquelles ils utiliseront les renseignements personnels ?
- Comment ces renseignements personnels seront-ils recueillis ou consultés, et où et comment seront-ils stockés ?
- Peuvent-ils décrire et fournir des preuves de leur programme de protection des renseignements personnels ?
- Peuvent-ils décrire et fournir des preuves de leur programme de sécurité de l'information ?
- Respectent-ils des standards ou des certifications en matière de sécurité ?
- Disposent-ils de processus pour identifier et évaluer les risques liés aux renseignements personnels dans le cadre de leurs activités ?
- Disposent-ils de rapports d'audit interne ou externe attestant de leurs pratiques ?
- Ont-ils un plan d'intervention en cas d'atteinte à la sécurité ? Ont-ils subi une atteinte à la sécurité au cours des dernières années ?
- Des personnes ou des équipes sont-elles affectées à la protection des renseignements personnels, à la sécurité des informations et/ou à la réponse aux atteintes à la sécurité ?
- Ont-ils une couverture d'assurance pour les atteintes à la sécurité ?

Si vous travaillez avec plusieurs tiers mandataires, une bonne pratique qui vous aidera également à démontrer la responsabilité et le respect de ces exigences SIPRP consiste à élaborer un questionnaire d'évaluation standard que vous demandez aux tiers mandataires de remplir.

Vous devrez peut-être adapter les questions à la nature et à la portée du mandat envisagé avec un tiers mandataire, et disposer d'un formulaire long et court, en fonction des risques associés au traitement des données. Par exemple, si vous travaillez avec des experts individuels, il est probable qu'ils ne disposent pas d'un programme de protection des renseignements personnels ou de sécurité des informations. Cela étant dit, vous devez tout de même discuter et convenir des mesures de protection pertinentes que les

experts doivent mettre en œuvre pour protéger les renseignements personnels en leur possession et veiller à ce qu'ils soient soumis à un devoir explicite de confidentialité. Par ailleurs, si vous travaillez avec des personnes comme des médecins ou des avocats, les obligations légales auxquelles ces personnes sont soumises seront pertinentes pour votre évaluation, car ces dernières sont souvent tenues de protéger les informations reçues et de les garder confidentielles en vertu des règles de déontologie applicables.

QUE FAUT-IL INCLURE DANS VOTRE CONTRAT ?

Une fois que vous avez une idée claire de la nature et de la portée des services du tiers mandataire et de ses besoins légitimes en matière de collecte, d'utilisation, de divulgation ou de tout autre traitement des renseignements personnels, vous devez consigner votre accord dans une convention.

Le SIPRP exige que les tiers mandataires soient soumis à des contrôles appropriés, y compris des contrôles contractuels et techniques, pour protéger les renseignements personnels qui seront sous leur garde dans le cadre de leur engagement avec une OAD.

Les contrôles contractuels appropriés comprennent des dispositions exigeant que :

- Les tiers mandataires se conforment au SIPRP et à toutes les lois applicables ;
- Les tiers mandataires ne traitent les renseignements personnels que conformément aux instructions documentées de l'OAD et à aucune autre fin ;
- Tout personnel traitant des renseignements personnels est soumis à un devoir de confidentialité ;
- Des mesures de sécurité techniques et organisationnelles appropriées sont appliquées aux renseignements personnels traités par le tiers ;
- Les tiers mandataires ne peuvent engager d'autres parties pour traiter des renseignements personnels sans l'autorisation préalable de l'OAD et sans que des contrôles contractuels appropriés avec ces autres parties soient en place ;
- Les tiers mandataires fournissent une notification et une assistance rapides à l'OAD lorsque des individus font valoir des droits en vertu du SIPRP ou des lois applicables, ou en cas d'atteinte à la sécurité ;
- Les renseignements personnels sont supprimés ou renvoyés à la fin de la prestation ou sur demande ; et
- Les tiers mandataires mettent à la disposition de l'OAD des informations permettant de démontrer le respect de ces contrôles, ou permettent à l'OAD de vérifier ce respect par des audits ou d'autres vérifications.

Les OAD devront adapter ces mesures au type de tiers mandataire et à la nature et à la portée de leur engagement. Par exemple, les OAD ont un devoir plus large de veiller à ce que les tiers mandataires qui sont également des tiers délégués en vertu du Code soient soumis à un devoir de coopération dans le cadre de toute activité de conformité de l'AMA. Pour ceux qui travaillent avec de nombreux tiers, il peut être utile d'élaborer un ensemble standard de contrôles à inclure dans les contrats impliquant des renseignements personnels, ou une liste des éléments qui doivent être inclus si vous êtes plus susceptible d'utiliser les modèles de contrat fournis par le tiers.

Les contrôles techniques appropriés peuvent inclure, selon la nature de l'accès du tiers mandataire aux systèmes ou aux informations de l'OAD :

Les OAD peuvent avoir besoin de soumettre les tiers mandataires à des contrôles contractuels spécifiques requis par le droit applicable. Ce sera le cas pour les OAD soumises au RGPD dans leurs accords avec un tiers mandataire agissant en tant que « sous-traitant » tel que défini par cette loi. Les OAD doivent garder à l'esprit que tous les tiers mandataires ne seront pas nécessairement qualifiés de « sous-traitants », ce qui nécessite une évaluation au cas par cas. De nombreuses autorités règlementaires et autres organes consultatifs ont publié des lignes directrices à cet égard. Quelle que soit la qualification du tiers mandataire, des contrôles contractuels appropriés doivent être inclus dans les accords avec ces derniers.

- Des restrictions d'accès
- Des exigences d'authentification (c'est-à-dire des identifiants d'utilisateurs, des mots de passe, des questions de vérification, etc.) ;
- Le cryptage, y compris en ce qui concerne toute information transmise ; et
- L'enregistrement et la supervision de l'accès et des activités des utilisateurs.

Si, dans le cadre d'un engagement avec une OAD, le tiers mandataire détient ou traite des renseignements personnels sur ses propres systèmes et dans ses propres bureaux, vous devez également tenir compte des mesures techniques, physiques et environnementales qui seront appliquées par le tiers mandataire à ces systèmes et bureaux. Voir Chapitre 6 : Comment protéger les renseignements personnels pour plus de détails sur les mesures de sécurité. Il est de bonne pratique de documenter dans votre contrat tous les contrôles techniques et autres pertinents ou nécessaires. Cela peut se faire de plusieurs façons, par exemple en incluant une annexe précisant les contrôles pertinents, ou en se référant à la documentation mise à disposition par le tiers mandataire concernant ses propres obligations de sécurité, ou aux standards/certifications de sécurité maintenus par les tiers mandataires.

L'importance des contrôles techniques ne doit pas être sous-estimée. Bien qu'ils ne soient pas totalement infaillibles, ils minimisent grandement les risques liés à l'erreur humaine et aux attaques malveillantes. L'impact d'une erreur humaine ou d'une attaque par un tiers sera minimisé si la personne/le tiers concerné-e avait lui/elle-même un accès limité aux renseignements personnels.

CONTRÔLES TECHNIQUES POUR LA COLLABORATION AVEC DE TIERS MANDATAIRES DANS ADAMS

Lorsque vous accordez des autorisations d'accès à un tiers mandataire dans ADAMS (nommés tiers délégués dans ADAMS), les OAD sont chargées de veiller à ce que ces autorisations respectent les principes communs de minimisation des données et du besoin de savoir.

Des contrôles sont disponibles dans ADAMS pour aider les OAD à adapter les autorisations d'accès de leurs tiers délégués. Par exemple, les OAD peuvent :

- Limiter l'accès aux tiers délégués à des sportifs ou non-sportifs spécifiques, ou à des groupes de sportifs (par exemple un groupe cible de sportifs soumis aux contrôles) - cette limite s'appliquera à tous les modules auxquels le tiers délégué est autorisé à accéder ;
- Sélectionnez des modules spécifiques auxquels les tiers délégués auront accès (par exemple, les contrôles, les AUT, la gestion des résultats) ;
- Fixer une date d'expiration pour toutes les autorisations d'accès ; et
- Pour les tiers délégués qui sont des autorités de prélèvement des échantillons, limitez l'accès aux ordres de mission spécifiques.

Un type courant de tiers délégué dans ADAMS est une autorité de prélèvement des échantillons. Si vous travaillez avec une autorité de prélèvement des échantillons, vous pouvez limiter ses autorisations d'accès à des ordres de mission spécifiques uniquement. L'accès aux ordres de mission spécifiques permettra à l'autorité de prélèvement des échantillons d'accéder uniquement aux informations de localisation pertinentes à la durée de l'ordre, concernant uniquement les sportifs figurant sur l'ordre, pour effectuer les contrôles antidopage pertinents. Si vous donnez plutôt à une autorité de prélèvement des échantillons l'accès au module « Contrôles », celle-ci aura des autorisations d'accès plus larges, qui comprennent l'accès aux informations de localisation de tous les sportifs du groupe de sportifs auquel vous l'avez autorisé à accéder, et la possibilité de créer et de modifier des ordres de mission et des formulaires de contrôle du dopage.

Il est fortement recommandé de ne pas permettre aux tiers délégués d'accéder aux données relatives à « Tous les sportifs ». Vous devriez plutôt sélectionner un sous-ensemble approprié de sportifs (par exemple, les sportifs de votre groupe cible de sportifs soumis aux contrôles) ou créer vos propres groupes de sportifs, afin de garantir que les permissions d'accès du tiers délégué soient limitées à ce qui est nécessaire à ses fonctions.

Les OAD devraient examiner les orientations fournies dans le centre d'aide ADAMS concernant la Gestion des tiers délégués pour plus de détails.

PARTAGE AVEC D'AUTRES TIERS

Les tiers qui ne sont pas des tiers mandataires ou des OAD se retrouvent dans le cercle de confiance le plus éloigné. **La divulgation à ce type de destinataire est plus strictement règlementée dans le cadre du SIPRP.** Elle est uniquement autorisée :

- avec le consentement explicite et éclairé de la personne concernée ;
- si la loi, un règlement, ou une procédure judiciaire l'exige ; ou
- si nécessaire pour aider les autorités à détecter, enquêter ou poursuivre une infraction pénale, une infraction aux règles déontologiques ou une violation du Code.

Les principes communs consistant à garantir le besoin de savoir, à réduire au minimum ce qui est partagé et à transmettre les informations en toute sécurité continuent également de s'appliquer. Il est bon de documenter votre évaluation de ces facteurs avant de partager des renseignements personnels. Pour ce faire, vous pouvez adapter le modèle de formulaire de demande de divulgation et l'utiliser pour les demandes émanant d'autres tiers.

AVEZ-VOUS UN CONSENTEMENT ?

Pour déterminer si vous avez le consentement de la personne concernée pour la divulgation, examinez si vous avez rempli les conditions d'un consentement valable telles que décrites dans 3. Obtenir un consentement valable si vous en avez besoin dans Chapitre 5 : Comment expliquer vos pratiques de traitement. **Le norme ici est le consentement « exprès », c'est-à-dire le même standard que celui requis pour les renseignements personnels sensibles dans l'Article 6.3 du SIPRP.** Vous pouvez également obtenir un consentement spécifique pour la divulgation en confirmant avec la personne concernée qu'elle accepte la divulgation au moment où vous avez l'intention de la faire.

LE PARTAGE EST-IL REQUIS PAR LA LOI, UN RÈGLEMENT OU UNE PROCÉDURE JUDICIAIRE ?

Vous pouvez partager des renseignements personnels avec des tiers lorsque la loi, un règlement ou une procédure judiciaire obligatoire l'exigent. Par exemple, lorsque vous êtes obligé de fournir des informations en vertu d'une loi, d'un instrument statutaire, d'un règlement (y compris, dans des circonstances limitées, des règles antidopage) ou d'une décision judiciaire.

Pour vous prévaloir de cette disposition, vous devez être confronté à l'obligation de faire une divulgation. En d'autres termes, le simple fait d'être autorisé à faire une divulgation ou d'être invité à faire volontairement une divulgation n'entrerait pas dans le champ d'application de cette disposition.

EXEMPLE DE FÉDÉRATION NATIONALE

Les fédérations nationales ne sont pas des organisations antidopage. À moins qu'elles ne travaillent pour le compte d'une OAD en tant que tiers délégué, elles entrent dans la catégorie des « autres tiers » dans le SIPRP. Les fédérations nationales peuvent toutefois jouer un rôle de coordination entre les OAD et les sportifs.

Par exemple, le Code précise que les OAD peuvent avoir besoin d'informer les fédérations nationales d'une violation des règles antidopage avant la divulgation publique d'une sanction, sous réserve de procédures de confidentialité appropriées.

Pour partager des renseignements personnels avec une fédération nationale à des fins antidopage, les OAD doivent s'assurer que :

- la FN a besoin des informations en question pour remplir un rôle antidopage (par exemple, la signification de documents à un athlète) ;
- le rôle antidopage de la FN et le partage nécessaire sont spécifiés dans les règles antidopage de l'OAD qui sont contraignantes pour l'OAD et la FN ;
- -les règles antidopage de l'OAD sont conformes au Code et aux Standards internationaux (par exemple, elles doivent inclure des procédures appropriées pour la protection des informations confidentielles).

Prenons l'exemple des procédures de gestion des résultats :

- La FN ne peut recevoir des informations sur la gestion des résultats que dans les circonstances autorisées par l'article 14 du Code sur la confidentialité et le signalement des violations des règles antidopage.
- La FN ne devrait recevoir que les informations nécessaires, par exemple, un dossier intégral ne devrait être fourni à une FN que si cela est nécessaire pour exercer un droit d'appel de la FN, ou si l'athlète décide de partager ces informations avec la FN.
- Rappelant que les procédures de VRAD sont confidentielles et impliquent la discussion de renseignements personnels, les FN ne devraient être présentes à une audience que si elles comparaissent avec le consentement des sportifs ou si cette présence est nécessaire pour exercer un droit d'appel limité tel que prévu dans les règles antidopage d'une OAD.

VOUS PORTEZ ASSISTANCE À UNE AUTORITÉ SPÉCIFIQUE ?

La troisième possibilité de divulgation de renseignements personnels est la divulgation aux forces de l'ordre, autorités gouvernementales ou autres. **Avant de partager des renseignements personnels avec ce type d'entité, vous devez vous assurer que les conditions suivantes sont remplies**:

- La divulgation doit être nécessaire pour aider à la détection, à l'enquête ou à la poursuite d'une infraction pénale, d'une infraction aux règles déontologiques ou d'une violation du Code ;
- Les renseignements personnels doivent être raisonnablement pertinents à l'infraction ou à la violation en question ;
- Les renseignements personnels ne peuvent pas être raisonnablement obtenus par l'autorité compétente par d'autres moyens.

Comme mentionné dans le SIPRP, le partage de renseignements personnels avec ce type d'autorité peut également être règlementé par d'autres lois qui vous sont applicables. Il est possible que la législation antidopage ou sportive applicable encourage ou facilite ce type de partage. Il est également possible que ces mêmes lois ou les lois sur la protection des données contiennent des conditions supplémentaires à remplir avant que la divulgation puisse avoir lieu.

CHAPITRE 9 :

Quels renseignements personnels doivent être conservés

La conservation ou le stockage est un type de traitement des renseignements personnels. Par conséquent, le même principe de minimisation des données s'applique : **Les renseignements personnels ne doivent être conservés que dans la mesure où ils sont pertinents pour les activités antidopage ou que la loi exige leur conservation.**

1. Comprendre l'Annexe A du SIPRP

L'objectif de l'Annexe A du SIPRP est d'harmoniser les périodes de conservation des principales catégories de données antidopage, dans le cadre des principales activités antidopage.

Il y a maintenant sept modules dans l'Annexe A : profil du sportif, localisation, gestion des AUT, contrôles, résultats des contrôles, procédure VRAD (c'est-à-dire gestion des résultats) et PBA. La colonne « données » fournit plus de détails sur les types de données incluses dans chaque module. Ces types de

données correspondent aux données qui sont enregistrés dans ADAMS par toutes les OAD, pour chaque module. Ensuite, la colonne « délai de conservation » fournit un délai de conservation maximale ainsi que l'élément déclencheur de ce délai pour chaque type de données. L'élément déclencheur de conservation détermine le point de départ du calcul du délai de conservation. La colonne « remarques » explique pourquoi une période de conservation particulière a été fixée. La colonne « critères » précise les circonstances dans lesquelles une évaluation de la proportionnalité était nécessaire pour fixer une période de conservation appropriée, en plus de l'évaluation de la nécessité des données pour une activité antidopage.

La conservation des données dans ADAMS est alignée avec l'Annexe A du SIPRP, et la suppression des données se fait de manière automatisée une fois la période de conservation écoulée. Lorsque l'Annexe A fait référence à une possibilité discrétionnaire de prolonger une période de conservation, par exemple, dans le cas d'une VRAD, d'une enquête ou d'une autre procédure judiciaire en cours ou raisonnablement prévue, l'OAD doit s'assurer qu'elle conserve une copie des informations pertinentes et la conserve en dehors d'ADAMS, ou doit demander à l'AMA de conserver les informations associées au(x) profil(s) du sportif concerné(s) dans ADAMS.

Consultez la page Combien de temps les données sont-elles conservées dans ADAMS? dans le centre d'aide ADAMS pour une description détaillée de l'application de l'Annexe A dans ADAMS.

2. Mettre en œuvre l'Annexe A en dehors d'ADAMS

Les OAD doivent étendre l'application de l'Annexe A à leurs propres systèmes et dossiers. Consultez votre registre de traitement (voir Chapitre 4 : Comment identifier ce que vous détenez et pourquoi) afin de déterminer où vos documents et registres sont conservés et combien de temps ils sont entreposés. Évaluez vos réponses par rapport aux exigences de l'Annexe A du SIPRP 2021 afin de déterminer où vous devez effectuer des mises à jour.

Élaborez des plans ou des procédures spécifiques pour garantir que les renseignements personnels sont conservés en toute sécurité et éventuellement supprimés, détruits ou rendus anonymes. Pour la conservation, on utilise généralement un calendrier de conservation, semblable à celui de l'Annexe A, mais adapté à vos propres systèmes et pratiques de classement.

Au minimum, les calendriers de conservation documentent les types de documents, les délais de conservation et certaines informations justifiant le délai de conservation (par exemple, la valeur des documents d'un point de vue juridique, fiscal, administratif ou historique, ainsi que les exigences législatives, les délais de prescription et les exigences organisationnelles ou archivistiques).

Pour plus de contexte, et bien que cela ne relève pas du champ d'application du SIPRP, les calendriers de conservation couvrent généralement tous les types de dossiers d'une organisation (pas seulement les renseignements personnels).

Votre calendrier de conservation des dossiers devra être complété par des mesures de sécurité de l'information afin de garantir la protection des informations stockées et archivées. Si vous utilisez un logiciel pour automatiser l'application des délais de conservation dans vos systèmes, vous devrez probablement aussi mettre en place des processus pour vérifier le bon fonctionnement de ce logiciel. Si vous avez une petite organisation et que vous gérez la conservation manuellement, envisagez de mettre en place un processus par lequel le Responsable de la protection des renseignements personnels (ou un autre membre du personnel) confirme que les différents services de l'OAD ont respecté les dates de suppression prévues, en examinant régulièrement ces dates et en tenant un registre des suppressions.

Lors de la création de votre calendrier de conservation interne, vous devez examiner s'il est nécessaire d'adapter l'élément déclencheur de conservation prévu à l'Annexe A à un élément qui vous permettra de rendre opérationnelle le délai de conservation requise dans vos propres systèmes.

Exemple de VRAD (Module 6)

L'élément déclencheur de conservation figurant à l'Annexe A pour les procédures et les décisions relatives aux VRAD est la « date de la décision finale ». Dans ADAMS, la date pertinente sera généralement soit la date de la décision de première instance, soit, en cas d'appel, la date de la décision d'appel. Dans votre propre système de classement ou base de données, vous pouvez qualifier une affaire de finale en utilisant un autre terme, tel que « cas fermé ». Dans ce cas, vous devrez programmer votre système ou fournir des instructions si vous disposez d'une procédure de suppression manuelle indiquant que, pour vos besoins, la « date de la décision finale » signifie la date à laquelle un cas est classé comme « fermé ».

Exemple de profil d'un sportif (Module 1)

L'élément déclencheur de conservation des informations de l'Annexe A relatives au profil du sportif est soit l'exclusion du programme de contrôle d'une OAD, soit le moment où d'autres catégories de données ont été supprimées, selon la dernière éventualité. En se concentrant sur le premier cas, la date pertinente dans ADAMS est la date du dernier contrôle. Il s'agit d'un élément déclencheur continu, ce qui signifie qu'il sera constamment mis à jour - la suppression n'aura lieu que lorsque la dernière date de contrôle associée à un profil de sportif aura 10 ans. Cette date a été choisie parce qu'elle peut être appliquée de manière cohérente pour toutes les OAD qui utilisent ADAMS. Dans votre propre système de classement ou base de données, vous pourriez avoir des fichiers liés à la date d'inclusion ou d'exclusion d'un sportif dans un groupe de contrôle, ce qui s'aligne directement à l'élément déclencheur de conservation de l'Annexe A. Vous pourriez au contraire avoir besoin d'utiliser une autre date, comme la date de retraite du sportif ou la date du dernier contrôle comme dans ADAMS, comme date équivalente dans vos systèmes à la date d'exclusion d'un programme de contrôle. L'important est de choisir un élément déclencheur de conservation que vous pouvez appliquer de manière cohérente dans vos systèmes et bases de données, et qui est aligné à l'élément déclencheur de conservation de l'Annexe A.

Prenez note également que l'Annexe A prévoit un délai de grâce d'un trimestre civil pour la suppression des données une fois que la période de conservation a expiré. Ce délai de grâce est destiné à faciliter la mise en œuvre de l'Annexe A dans les systèmes de l'OAD ou dans le cadre d'un processus manuel de révision/suppression.

3. Définir des périodes de conservation pour d'autres données

Pour les renseignements personnels traités par les OAD, mais non couverts par l'Annexe A, les OAD doivent respecter les principes de conservation de l'Article 10 du SIPRP, c'est-à-dire ne conserver les renseignements personnels que lorsqu'ils sont pertinents pour une activité antidopage ou que la loi l'exige. Les OAD doivent tenir compte des finalités pour lesquelles les renseignements personnels sont traités afin d'évaluer la pertinence ou la nécessité de leur conservation (par exemple, la gestion des AUT, la localisation, les contrôles, etc.). En outre, lorsque des renseignements personnels sensibles sont concernés, les critères de « pertinence » doivent être interprétés de manière restrictive. En d'autres termes, des raisons plus convaincantes sont nécessaires pour conserver les renseignements personnels sensibles.

Les OAD sont encouragées à définir des délais de conservation spécifiques pour tout renseignement personnel non couvert par l'Annexe A, sur la base des critères de conservation susmentionnés, et à documenter ces périodes dans leur calendrier ou processus de conservation. Pour décider de la durée de conservation des informations, il convient de se poser les questions suivantes :

- Quel est le besoin organisationnel interne pour conserver les informations ?
- Existe-t-il des exigences règlementaires imposant la conservation des données et, si oui, que prévoient-elles ?
- Existe-t-il des délais de prescription légaux pertinents, ou ces informations seraient-elles nécessaires dans le cadre d'un litige en cours ou imminent ?
- Les informations sont-elles nécessaires pour répondre à une obligation juridique applicable de faire rapport ?

4. Supprimer, détruire ou anonymiser à l'expiration des délais de conservation

Une fois que les renseignements personnels ne sont plus nécessaires pour remplir les obligations du Code ou des Standards internationaux, ou qu'elles ne doivent plus être conservées en vertu de la loi, le SIPRP exige qu'elles soient supprimées, détruites ou rendues anonymes.

Le terme « destruction » désigne généralement les documents stockés sous une forme physique, comme les documents papier ou les données électroniques conservés sur des bandes d'archives physiques. Différentes techniques peuvent être utilisées pour détruire physiquement des documents.

Par exemple, vous pouvez détruire des documents papier en les déchiquetant et en vous assurant que les documents déchiquetés sont ensuite éliminés de manière sécurisée par un fournisseur de confiance. Les dossiers papier contenant des renseignements personnels ne doivent pas être mis au recyclage ou à la poubelle. Vous pouvez détruire les bandes physiques par incinération ou

démagnétisation (un processus qui brouille - c'est-à-dire détruit - les données sur une bande en l'exposant à un champ magnétique). Des fournisseurs spécialisés dans la gestion des documents peuvent vous aider à détruire les documents physiques en toute sécurité.

Les termes « suppression » et « anonymisation » font généralement référence aux documents stockés sous forme électronique. La suppression électronique est plus complexe que la destruction physique, car les données électroniques existeront probablement à plusieurs niveaux de système et d'application. L'assistance de professionnels de l'informatique est recommandée pour examiner et évaluer vos processus de suppression électronique.

Le standard d'anonymisation requise par le SIPRP pour le stockage continu des données une fois qu'elles ne sont plus nécessaires aux activités antidopage (en forme identifiable) et qu'elles ne doivent plus être conservées en vertu de la loi applicable est l'anonymisation « permanente ». Cela signifie que les individus ne peuvent plus être identifiés dans les données et que les moyens utilisés pour rendre les données anonymes ne peuvent pas être inversés pour identifier ces individus. Cela peut être un outil utile et plus approprié que la suppression des données lorsque les données anonymes ont toujours une valeur pour une organisation antidopage, mais ne sont plus nécessaires sous une forme identifiable. Par exemple, les statistiques sur les contrôles ou les VRAD sont créées à partir de fichiers identifiables, mais les renseignements personnels ont été supprimés. Elles continuent à avoir une valeur historique, scientifique et éducative sous une forme agrégée.

Pour que les systèmes contenant des renseignements personnels soient résistants et puissent être restaurés rapidement, il est important qu'ils soient sauvegardés ou archivés séparément du système principal et souvent dans un endroit éloigné. Cela peut entraîner la conservation des informations, même après leur suppression ou leur effacement du système principal, pendant des périodes plus longues. En fonction des lois applicables, il se peut que les informations placées dans des systèmes sécurisés d'archivage puissent être conservées plus longtemps. Les OAD doivent tenir compte de toute ligne directrice pertinente de leur autorité règlementaire nationale.

CHAPITRE 10 :

Comment répondre aux demandes et aux plaintes

1. Comprendre les droits individuels en matière de renseignements personnels

Les individus ont des droits concernant le traitement de leurs renseignements personnels en vertu du SIPRP. Cela est lié au principe de la participation individuelle. Dans ce chapitre, nous examinons tout d'abord les différents types de droits, puis les procédures à suivre pour répondre à une demande ou à une plainte.

DROIT D'ACCÈS À L'INFORMATION

Les personnes ont le droit de recevoir les éléments suivants de la part des OAD :

- Confirmation du fait que l'OAD traite ou non des renseignements personnels les concernant ;
- Les informations devant figurer dans l'avis de confidentialité d'une OAD conformément à l'Article 7.1 du SIPRP (voir Chapitre 5 : Comment expliquer vos pratiques de traitement) ; et
- Une copie des renseignements personnels demandés en possession de l'OAD.

Si les personnes ont des droits supplémentaires qui ne sont pas prévus par le SIPRP ou sont tenues de suivre des procédures spécifiques pour les exercer en vertu des lois applicables de protection des données et de la vie privée, il serait bon d'ajouter ces informations à votre avis de confidentialité. Ce serait un exemple d'informations supplémentaires fournies au titre de l'Article 7.1 pour garantir que le traitement des renseignements personnels reste loyal pour les personnes concernées. Par exemple, lorsque les personnes ont le droit de déposer des plaintes auprès d'une autorité de protection des données, les OAD devraient les en informer.

Bien que le SIPRP reflète la plupart des droits qui existent en vertu des lois sur la protection des données et de la vie privée, les OAD devraient examiner la législation pertinente (y compris la législation sur le sport et la lutte contre le dopage) et les lignes directrices d'autorité règlementaire afin de mieux comprendre comment ces droits sont appliqués dans leurs juridictions, et de déterminer s'il existe d'autres droits ou exceptions. Dans le cadre du RGPD de l'UE par exemple, les individus ont le droit de ne pas être soumis à une prise de décision purement automatisée ayant des effets juridiques ou équivalents, sauf si celle-ci est nécessaire à l'exécution d'un contrat, est autorisée par la loi ou a lieu avec le consentement de l'intéressé.

DROIT DE CORRIGER OU DE LIMITER LE TRAITEMENT

Une personne peut demander à une OAD de rectifier, modifier, bloquer ou supprimer des renseignements personnels si le traitement de ces informations par l'OAD s'avère inexact, incomplet ou excessif.

Un exemple de traitement excessif serait un traitement qui n'est pas nécessaire ou qui ne sert pas une activité antidopage légitime. L'inexactitude ou le caractère incomplet des informations se trouve généralement dans les renseignements personnels mêmes, plutôt que dans les opérations de traitement.

DROIT DE REFUSER OU DE RETIRER LE CONSENTEMENT

Lorsque les OAD se fondent sur le consentement pour traiter des renseignements personnels, une personne peut refuser d'accorder ou peut retirer son consentement au traitement de ses renseignements personnels à tout moment. Ce droit est traité à l'Article 6.2 du SIPRP, plutôt qu'à l'Article 11 du SIPRP. L'impact de l'exercice de ce type de droit est similaire dans la pratique à une demande de blocage ou de suppression de renseignements personnels.

Comme mentionné dans la section 3. Obtention d'un consentement valable si nécessaire du Chapitre 5 : Comment expliquer vos pratiques de traitement, les personnes devraient être informées à l'avance des circonstances dans lesquelles une OAD aurait encore besoin de traiter des renseignements personnels malgré une demande de blocage, de suppression ou de retrait du consentement. De même, les personnes devraient être informées des conséquences du refus de consentir ou du blocage ou de la suppression des renseignements personnels dans le contexte de la lutte contre le dopage (par exemple, une VRAD ou la disqualification/l'interdiction de participer à une manifestation sportive).

DROIT DE DÉPOSER UNE PLAINTE

Les personnes peuvent déposer une plainte auprès d'une OAD s'ils estiment que leurs renseignements personnels ne sont pas traités conformément au SIPRP ou aux lois applicables de protection des données et de la vie privée.

Les plaintes peuvent être liées aux types de demandes de droits décrits ci-dessus, ou peuvent être liées à des questions sur les autres pratiques, politiques ou procédures de traitement des renseignements personnels de l'OAD.

Si une personne estime que l'OAD n'a pas résolu le problème de manière satisfaisante, elle peut en informer l'AMA à l'adresse compliance@wada-ama.org ou privacy@wada-ama.org. L'AMA traitera la notification conformément au Standard international pour la conformité au Code des signataires (SICCS).

2. Répondre à une demande ou à une plainte

Maintenant que vous avez compris les types de droits dont disposent les personnes dans le cadre du SIPRP, passons en revue les principales étapes de la réponse. Il vous sera utile de documenter ces étapes dans une politique ou une procédure adaptée à votre organisation. Le SIPRP exige uniquement que vous disposiez d'une procédure documentée pour répondre aux plaintes, mais il serait plus efficace de créer une procédure pour répondre à tous les types de demandes ou de plaintes en matière de protection des renseignements personnels. Ce processus vous aidera à démontrer votre responsabilité et votre conformité avec le SIPRP.

COMMENT IDENTIFIER LE TYPE DE DEMANDE OU DE PLAINTE

Idéalement, les personnes qui ont des demandes ou des plaintes les adresseront à votre Responsable de la protection des renseignements personnels, en utilisant les coordonnées que vous avez fournies dans votre avis de confidentialité (voir Chapitre 5 : Comment expliquer vos pratiques de traitement).

Il est toutefois possible qu'une autre personne de votre organisation reçoive une demande ou une plainte dans le cadre du SIPRP. Il est également possible (et même probable) que le demandeur individuel n'invoque pas formellement ou expressément son « droit d'obtenir une copie » ou « d'accéder aux renseignements personnels » ou de « corriger ou limiter » le traitement de ses renseignements personnels.

Si une personne demande que des documents contenant des renseignements personnels lui soient fournis, ou conteste l'exactitude ou l'exhaustivité des renseignements personnels, cela doit être considéré comme une demande d'exercice des types de droits décrits ci-dessus. Vous pouvez également recevoir des demandes verbales, notamment si vous mettez à la disposition des personnes des lignes téléphoniques d'aide ou de soutien (notez que certaines juridictions exigent que les demandes d'exercice de droits soient faites par écrit).

Le Responsable de la protection des renseignements personnels doit s'assurer que le personnel, en particulier le personnel ayant des interactions fréquentes avec les sportifs et d'autres personnes, soit conscient qu'il puisse recevoir ce type de demande ou de plainte et qu'il soit formé pour les transmettre au Responsable de la protection des renseignements personnels. Si vous recevez des demandes verbales, il est conseillé de les consigner par écrit dans vos propres registres.

Si vous disposez des ressources nécessaires et que vous recevez un volume important de demandes, il existe des fournisseurs de services de protection des renseignements personnels qui proposent des solutions pour gérer le traitement de ces demandes. Ces solutions ont l'avantage de pouvoir être adaptées aux lois de protection des données et de la vie privée qui vous sont applicables. Elles impliquent généralement aussi la création d'un formulaire standard que les personnes peuvent remplir pour vous fournir les informations dont vous avez besoin pour classer correctement une demande et y répondre. Toutefois, n'oubliez pas que vous ne pouvez pas normalement exiger des personnes qu'elles utilisent un formulaire ou une procédure spécifique pour vous envoyer une demande d'exercice de leurs droits relatifs au traitement de renseignements personnels.

QUE DEVEZ-VOUS INCLURE DANS VOTRE ACCUSÉ DE RÉCEPTION ?

Après avoir identifié le type de demande ou de plainte, la première étape de la réponse consiste à en accuser réception. Il est bon de communiquer au demandeur que son message a bien été reçu et que vous le traiterez.

C'est également un bon moment pour poser toutes les questions de suivi dont vous avez besoin pour bien comprendre la nature et la portée de la demande et/ou vérifier l'identité du demandeur. Il est important d'évaluer si vous avez besoin de plus d'informations de la part du demandeur dans les quelques jours suivant la réception d'une demande, afin que vous puissiez recevoir ces détails en temps utile tout en respectant les délais de réponse.

Examinez les questions suivantes :

- Avez-vous besoin de confirmer l'identité du demandeur ?
- Une personne fait-elle une demande au nom d'une autre personne ? Dans l'affirmative, devez-vous confirmer son pouvoir d'agir au nom de cette autre personne ?
- La demande est-elle claire ? Comprenez-vous ce que la personne demande ?
- La demande est-elle très large ? Si oui, vous pouvez demander au demandeur de préciser la nature et la portée de sa demande.
- Les informations demandées par le demandeur sont-elles en votre possession, ou devriez-vous le rediriger vers une autre organisation ?
- La demande est-elle adressée à plusieurs destinataires ?
- La demande est-elle faite dans le cadre d'un processus de gestion des résultats ?
- La demande est-elle faite dans le cadre d'une enquête en cours ou est-elle liée à celle-ci ?

COMMENT VÉRIFIER L'IDENTITÉ DU DEMANDEUR

Vous avez la responsabilité de vous assurer que vous ne fournissez pas de renseignements personnels à la mauvaise personne ou que vous ne modifiez pas ou n'éditez pas des renseignements personnels sans le consentement de la bonne personne. Cela est important pour protéger les renseignements personnels contre tout accès non autorisé.

Vous pourrez donc avoir besoin de confirmer l'identité du demandeur avant de donner suite à sa demande. Cela dit, il y a des circonstances où cela peut ne pas être nécessaire. Par exemple, si une personne cherche simplement à obtenir des informations générales sur vos pratiques en matière de protection des renseignements personnels, il n'est pas nécessaire qu'elle s'identifie auprès de vous - vous pouvez simplement répondre en fournissant les informations générales demandées.

Si vous avez besoin de confirmer l'identité d'une personne, vous pouvez le faire de différentes manières. Comme toujours, vous ne devez demander que les renseignements personnels nécessaires à l'identification du demandeur. Par exemple, vous pouvez demander quelques renseignements personnels que vous pourrez ensuite confirmer dans votre système (par exemple, un numéro d'identification unique ADAMS ou autre, combiné au nom et à la date de naissance d'une personne). Si vous demandez une copie d'une pièce d'identité (comme un permis de conduire ou un passeport), ou si une personne vous la fournit de manière proactive avec sa demande, il est de bonne pratique de supprimer cette copie une fois que vous avez terminé votre vérification. Vous pouvez documenter, pour vos dossiers, que la personne s'est identifiée en fournissant une copie de sa pièce d'identité. Vous devez également prévoir un moyen sécurisé pour que la personne vous fournisse cette copie (par exemple, un lien de téléchargement ou un autre canal crypté).

Si vous recevez une demande d'un tiers agissant au nom d'un individu, le tiers devra prouver qu'il détient le pouvoir d'agir pour cet individu. Vous devrez également confirmer l'identité de la personne qui fait l'objet de la demande. Il s'agira souvent d'un avocat agissant au nom d'un client, mais il peut aussi s'agir d'un parent agissant au nom d'un enfant, ou d'un membre de la famille, d'un entraîneur ou d'une autre personne qu'un individu a mandaté pour agir en son nom. Là encore, vous devez toujours vous adapter aux circonstances pour effectuer cette vérification.

Voici des exemples de moyens pour prouver ce pouvoir d'agir:

- Demander une procuration générale ou spécifique ou une autre lettre d'autorisation ;
- Confirmer l'autorité déléguée directement auprès de la personne faisant l'objet de la demande ;
- Établir, au moyen de la documentation existante en possession de l'OAD, que la personne a l'autorisation appropriée pour présenter la demande ; ou
- Vérifier vos dossiers pour confirmer qu'une personne est bien le parent d'un sportif mineur et confirmer son identité.

COMMENT RECUEILLIR DES INFORMATIONS POUR VOTRE RÉPONSE

Le type de recherche que vous devez effectuer dépendra à nouveau du type de demande. S'il s'agit d'une demande d'accès ou de correction très spécifique, votre recherche sera limitée. Si vous recevez une demande portant sur un large éventail de données, vous devrez peut-être effectuer plusieurs recherches dans différents systèmes. Là encore, il peut être utile de clarifier l'étendue de la demande avec le demandeur.

Il vous sera également utile de comprendre, à l'avance, comment vos différents systèmes ou bases de données peuvent être interrogés. Par exemple, êtes-vous en mesure d'extraire toutes les entrées associées à un nom ou à un identifiant particulier ? Votre capacité de recherche est-elle plus limitée ? Quelle serait la charge de travail nécessaire si vous deviez répondre à une demande de copie d'un large éventail de renseignements personnels ?

N'oubliez pas que vous pouvez extraire les entrées associées à un identifiant ADAMS en utilisant les fonctions de rapport d'ADAMS.

En cas de doute, consultez les lignes directrices de votre autorité règlementaire pour mieux comprendre les attentes pour votre recherche d'informations en réponse à une demande. Dans la pratique, les autorités règlementaires s'attendent à ce que les organisations déploient des efforts raisonnables pour localiser toute information pertinente, mais ne s'attendent généralement pas à ce qu'elles remuent ciel et terre dans l'éventualité où cela pourrait mener à la localisation d'une information supplémentaire.

QUELLES EXCEPTIONS DOIVENT ÊTRE ENVISAGÉES ET APPLIQUÉES

Il y a des limites aux demandes et aux plaintes relatives aux renseignements personnels, tant en vertu du SIPRP que des lois applicables. Vous devez également tenir compte d'autres intérêts, notamment de la confidentialité des tiers et de l'intérêt public, lorsque vous répondez à ces demandes, en particulier des demandes d'accès ou de suppression.

Premièrement, si la demande porte sur ou vise des informations autres que des renseignements personnels (par exemple, des procès-verbaux d'organisation ou des statistiques générales), il ne s'agit pas d'une demande soumise au SIPRP (ou aux lois sur la protection des données et de la vie privée).

En supposant que les demandes concernent des renseignements personnels, examinez si l'une des exceptions suivantes s'applique:

- Si vous fournissez une copie des renseignements personnels, contient-elle des renseignements personnels sur une autre personne (notez que les opinions peuvent constituer un renseignement personnel à la fois de la personne qui émet l'opinion et de la personne qui en fait l'objet) ? Dans l'affirmative, pouvez-vous quand même répondre à la demande tout en supprimant les renseignements personnels du tiers ?
- Le fait de satisfaire à la demande entre-t-il en conflit avec votre capacité à effectuer des contrôles sans préavis, ou à enquêter ou à établir une VRAD ou une autre revendication juridique ?
- La demande est-elle par ailleurs en contradiction avec l'objectif de maintenir l'intégrité du système antidopage ?
- La demande impose-t-elle une charge disproportionnée à l'OAD en termes de coût ou d'effort, compte tenu de la nature des renseignements personnels demandés ?

Certaines de ces exceptions sont discrétionnaires et nécessitent une évaluation minutieuse au cas par cas qui doit être documenté. La documentation de votre évaluation vous aidera dans le cas où une autorité règlementaire, ou l'AMA, dans le cadre d'un processus de contrôle de conformité, vous demanderait de justifier tout refus de donner suite à une demande. Dans le contexte de la lutte contre le dopage, voici quelques exemples de cas où ces exceptions peuvent s'appliquer :

- Une demande de suppression de renseignements personnels pertinents pour une enquête ou un processus de VRAD en cours ou imminents ;
- Une demande de restriction du traitement des renseignements personnels lorsque ce traitement est nécessaire pour mener une activité antidopage (par exemple, un processus de contrôle antidopage obligatoire) ; ou
- Circonstances dans lesquelles les forces de l'ordre ou autres autorités ont indiqué que le fait de répondre à une demande de renseignements personnels entraverait leur enquête sur une violation d'une loi applicable.

Lorsque vous examinez si des exceptions s'appliquent et comment les appliquer, vous devriez vous référer aux lois applicables (y compris les lois sur le sport et la lutte contre le dopage) et aux lignes directrices de votre autorité règlementaire. Par exemple, les exceptions fréquentes au droit d'accès aux renseignements personnels en vertu des lois sur la protection des données incluent les circonstances dans lesquelles la fourniture de ces informations peut : porter atteinte aux droits et aux intérêts des organisations en divulguant des secrets commerciaux et d'autres informations commerciales sensibles ; ou entraîner la divulgation de matériel assujetti au secret professionnel.

COMBIEN DE TEMPS AVEZ-VOUS POUR RÉPONDRE ?

Vous devez normalement répondre à une demande ou à une plainte relative à la protection des renseignements personnels dans les trente (30) jours, ou quatre semaines, suivant la réception d'une demande dûment formulée.

« Dûment formulée » signifie que vous avez pu confirmer l'identité du demandeur (et le pouvoir d'agir de tout tiers, le cas échéant), et obtenir du demandeur toutes les clarifications raisonnablement nécessaires pour répondre à la demande.

Dans ce contexte, « répondre » signifie également fournir une réponse substantive, c'est-à-dire soit répondre à la demande, soit motiver le refus.

Si la quantité de renseignements personnels en cause est importante, et si leur collecte nécessite un effort disproportionné, votre réponse peut légitimement être retardée au-delà de 30 jours. Dans ce cas, vous devez informer la personne du retard, en expliquer les raisons et fournir une estimation révisée du délai de réponse avant l'expiration des 30 premiers jours.

Notez que la prolongation du délai au-delà de 30 jours nécessite une justification solide et ne devrait se produire que dans une minorité de cas avec des raisons documentées. Vous devez également noter que les lois applicables peuvent imposer un délai maximum pour ce type de retard (par exemple, 60 jours supplémentaires). Si vous le pouvez, vous pourriez également fournir des informations de manière progressive, ce qui signifie que certaines informations plus facilement accessibles pourraient être fournies plus tôt que d'autres.

QUE FAUT-IL INCLURE DANS VOTRE RÉPONSE ?

Votre réponse doit comprendre les informations minimales suivantes :

- Si vous répondez à la demande, en tout ou en partie, une confirmation que vous le faites ainsi que toute pièce justificative pertinente (par exemple, une copie des renseignements personnels demandés ou la preuve qu'une correction demandée a été effectuée) ; et
- Si vous refusez de donner suite à la demande, en tout ou en partie, les raisons de ce refus.

Si vous fournissez une copie des renseignements personnels, n'oubliez pas non plus :

- De le faire en utilisant des moyens sûrs, comme un document crypté ou un service de partage de fichiers ; et
- Que les informations doivent être présentées sous une forme intelligible pour l'individu. Si les données sont associées à de nombreux étiquettes ou codes (ce qui peut être le cas pour les données électroniques extraites d'une base de données), vous devrez peut-être expliquer ces étiquettes ou codes à la personne (par exemple, « 1 » signifie oui et « 0 » signifie non, ou sans objet).

POUVEZ-VOUS FACTURER DES FRAIS ?

Vous devez généralement répondre à ce type de demande sans frais pour la personne concernée. Les lois applicables peuvent autoriser les organisations à facturer des frais minimes pour des éléments tels que les frais d'impression, le cas échéant. En vertu du SIPRP, ces frais ne doivent pas être excessifs. Si vous exigez ce type de frais, vous devez en informer le demandeur à l'avance.

DEVRIEZ-VOUS EN INFORMER D'AUTRES ORGANISATIONS ?

Si vous apportez une correction, supprimez des informations ou acceptez de restreindre le traitement des renseignements personnels, vous devez en informer les autres OAD qui ont accès à ces informations ou les traitent, à moins que cela ne s'avère impossible ou n'implique un effort disproportionné.

Avant de prendre l'initiative de répondre à une demande, vous devriez également vous demander si une autre organisation serait mieux placée pour y répondre. À cet égard, le SIPRP prévoit que l'OAD qui a la relation principale avec le sportif (par exemple, l'ONAD dans le cas d'un sportif de niveau national, ou la FI dans le cas d'un sportif de niveau international) sera généralement chargée de répondre aux demandes ou aux plaintes relatives aux renseignements personnels de ce sportif. Pour donner un exemple simple, si un sportif a une question ou une demande concernant son passeport biologique, le gardien du passeport est probablement le mieux placé pour y répondre.

Cela dit, si une autre organisation détient des renseignements personnels sur ce même sportif et reçoit une demande, elle peut également y répondre. Dans le cas de l'AMA, nous communiquons ou nous collaborerons généralement avec l'OAD responsable d'un sportif particulier, à moins que cela ne soit inapproprié dans les circonstances (par exemple, si le sportif demande la confidentialité dans sa demande).

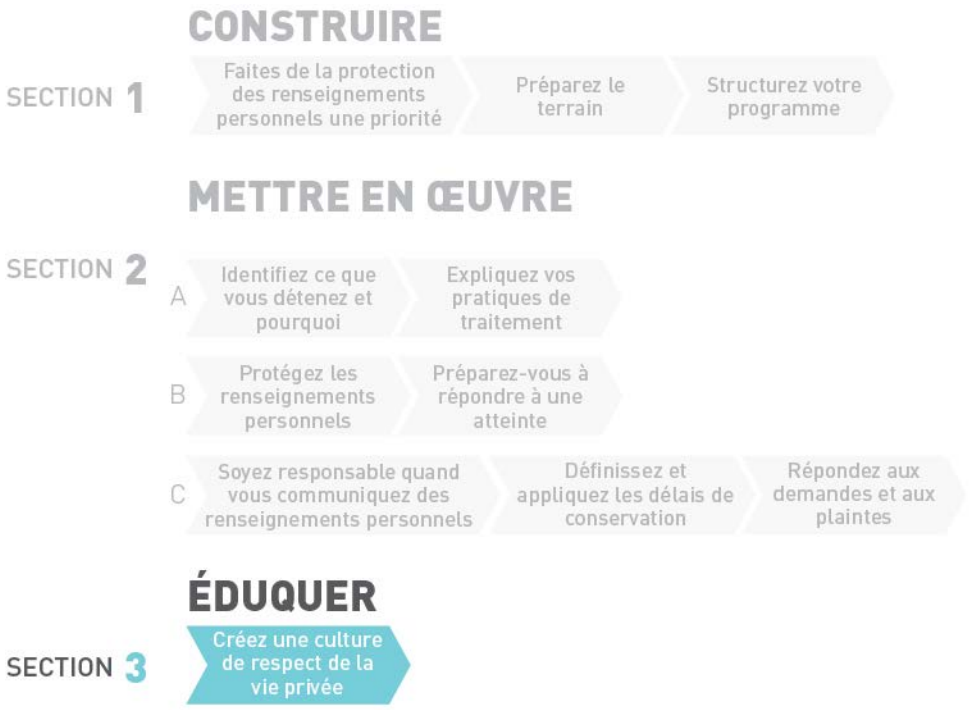
SECTION 3 :

Sensibiliser le personnel à votre programme de protection des renseignements personnels

La Section 3 comprend le Chapitre 11. Cette section apportera un soutien à tous les articles en vous aidant à valider que chaque personne de votre organisation comprend et applique les exigences de votre programme de protection des renseignements personnels. La création d'une culture de respect de la vie privée et la formation du personnel constituent en soi une mesure de sécurité essentielle pour les renseignements personnels.

CHAPITRE 11 :

Comment créer une culture de respect de la vie privée



Vous saurez que vous avez réussi à créer une culture du respect de la vie privée lorsque l'application des principes de protection des renseignements personnels aux activités antidopage quotidiennes deviendra naturelle pour chaque personne de votre organisation. Vous constaterez également que la conformité au SIPRP et aux lois sur la protection des données et de la vie privée ne sera plus que l'un des nombreux avantages de votre programme de protection des renseignements personnels, plutôt que son objectif principal.

Dans la Section 1, nous avons évoqué l'importance d'obtenir le soutien de la haute direction à votre programme et d'intégrer la protection des renseignements personnels dans les structures de gouvernance de votre organisation. C'est le premier élément de base de la création d'une culture de respect de la vie privée. Dans cette section, nous nous concentrerons sur deux autres éléments : la création de champions de la protection des renseignements personnels et l'engagement de tout le personnel dans la création de votre culture de respect de la vie privée.

1. Former vos champions de la protection des renseignements personnels

Le Responsable de la protection des renseignements personnels que vous devez nommer en vertu du SIPRP est votre principal champion de la protection des renseignements personnels. Si vous êtes une grande organisation, vous pouvez également envisager de créer des champions de la protection des renseignements personnels dans des domaines opérationnels clés de votre organisation, par exemple pour les contrôles ou la gestion des résultats.

Investir dans la formation de vos champions de la protection des renseignements personnels vous aidera à multiplier la force de votre programme de protection des renseignements personnels, car ces personnes utilisent et partagent leur expertise dans toute l'organisation.

Il existe de nombreuses ressources gratuites et peu couteuses pour aider à former les experts en matière de protection des renseignements personnels. Par exemple, l'International Association of Privacy Professionals (IAPP) rassemble des professionnels de la protection des renseignements personnels du monde entier. Ses membres peuvent accéder à des guides, des modèles, des webinaires et d'autres ressources. L'IAPP propose également divers programmes de certification pour les professionnels de la protection des renseignements personnels. Un certain nombre d'entreprises proposent également des plateformes de recherche et d'information sur la protection des renseignements personnels moyennant un abonnement. L'IAPP publie chaque année un rapport sur les fournisseurs de technologies de protection des renseignements personnels (*Privacy Tech Vendor Report*) dans lequel vous pouvez trouver un grand nombre de ces plateformes et déterminer si elles vous conviennent.

---

2. Former votre personnel et accroître la sensibilisation

Maintenant que vous avez votre (ou vos) champion(s) de la protection des renseignements personnels, la formation du reste de votre personnel est la prochaine étape. Il s'agit non seulement d'une étape clé dans la création d'une culture de respect de la vie privée, mais aussi d'une protection essentielle des renseignements personnels qui devrait figurer dans vos programmes de protection des renseignements personnels et de sécurité de l'information.

Le SIPRP exige que le personnel qui a accès aux renseignements personnels soit informé de la nécessité de préserver la confidentialité des renseignements personnels. De même, les OAD s'engagent à s'assurer que le personnel a reçu une formation appropriée en matière de protection des renseignements personnels et de sécurité dans l'accord régissant l'utilisation d'ADAMS.

Il existe de nombreuses façons d'atteindre cet objectif, et de nombreux outils existent pour vous aider, à commencer par des cours et des webinaires gratuits disponibles sur ADEL.

Utilisez le *Privacy Tech Vendor Report* susmentionné pour identifier les fournisseurs d'apprentissage en ligne. De nombreux fournisseurs d'apprentissage en ligne sont spécialisés dans la sécurité de l'information

et la protection des renseignements personnels et peuvent vous proposer une vaste bibliothèque de cours. Ils peuvent également vous donner accès à un système de gestion de l'apprentissage qui vous permettra d'évaluer facilement les connaissances, d'assigner des cours à votre personnel et de suivre les résultats obtenus. Certains outils offrent également des outils d'apprentissage de renforcement supplémentaires, comme la possibilité de créer et d'envoyer des simulations d'hameçonnage.

Vous pouvez combiner ces outils d'apprentissage en ligne avec une formation en direct ou en personne dispensée par votre Responsable de la protection des renseignements personnels. Si vous dispensez déjà une formation de sécurité de l'information, envisagez de combiner vos efforts pour offrir un programme de formation couvrant à la fois la vie privée et la sécurité. Les Responsables de la protection des renseignements personnels devraient également envisager de collaborer avec les responsables de l'éducation et à des membres du personnel des ressources humaines qui ont une expertise en matière d'éducation et qui disposent peut-être déjà d'outils de formation.

Quels que soient les outils et les formats que vous choisissez pour votre formation en matière de protection des renseignements personnels, nous vous recommandons d'intégrer des moyens d'évaluer les lacunes en matière de connaissances, de former le personnel régulièrement et de mesurer vos progrès.

COMMENT ÉVALUER LES CONNAISSANCES ET IDENTIFIER LES LACUNES

L'évaluation des connaissances existantes vous aidera à fournir un contenu de formation plus pertinent à votre personnel. Avant de commencer votre évaluation, réfléchissez aux questions suivantes:

- Combien de membres de personnel devez-vous former ?
- Comment reçoivent-ils généralement des informations sur les politiques et les codes de conduite de l'organisation ?
- Quels types de rôles existent au sein de votre organisation ?
- Combien de membres du personnel accèdent et utilisent régulièrement des renseignements personnels ?
- Quels sont les outils que le personnel utilise le plus souvent pour effectuer son travail (par exemple, word, excel, plateformes de tiers, etc.) ?
- Quels types de formation en matière de protection des renseignements personnels ou de sécurité de l'information votre personnel a-t-il reçu par le passé ?
- Quel est le niveau de compétence technique générale au sein de votre organisation ?

Utilisez les réponses à ces questions préliminaires pour élaborer vos questions d'évaluation et commencer à réfléchir au contenu de votre formation. Pour répondre à ces questions, vous pouvez utiliser des outils tels qu'un sondage ou un outil d'évaluation intégré à votre système de gestion de l'apprentissage. Vous pouvez également trouver des modèles de sondage en ligne.

Un outil de simulateur d'hameçonnage peut également être utile pour évaluer la connaissance et la compréhension des menaces d'hameçonnage. Ces outils peuvent être intégrés directement dans votre système de messagerie électronique et vous aideront à identifier les employés qui ont besoin d'une formation complémentaire.

QUE FAUT-IL INCLURE DANS VOTRE PROGRAMME DE FORMATION ?

Afin de garantir que la formation en matière de protection des renseignements personnels soit une priorité pour votre personnel, nous vous recommandons de rendre obligatoires au moins certains aspects de votre programme. Cela vous permettra de disposer des informations nécessaires pour mesurer l'impact de vos efforts.

Lorsque vous développez ou achetez un contenu de formation, demandez-vous si votre programme de formation couvre des sujets tels que :

- Les exigences légales pertinentes, les directives des autorités règlementaires et les normes applicables à votre industrie ;
- Les risques juridiques et de réputation liés aux fonctions de votre organisation ;
- Un aperçu des politiques et procédures pertinentes ;
- Les mesures de protection organisationnelles, techniques, physiques et environnementales mises en place pour protéger les renseignements personnels ;
- Les cybermenaces les plus courantes, la manière de les repérer et de s'en protéger ; et
- La manière de réagir à une atteinte à la sécurité.

Demandez-vous également si le contenu de la formation contribuera à combler les lacunes en matière de connaissances identifiées dans votre évaluation. Si votre évaluation a révélé des besoins éducatifs plus importants pour certains groupes, envisagez de fournir à ces groupes un contenu ou des activités de formation supplémentaires. Les grandes organisations devraient également envisager de fournir une formation basée sur les rôles pour les groupes ayant des besoins ou des fonctions spécialisés. Par exemple, un gestionnaire d'AUT doit être formé sur le traitement de données hautement sensibles. Un gestionnaire d'éducation traitant des données peu sensibles n'aura pas les mêmes besoins.

COMMENT MESURER LES PROGRÈS ET RENFORCER L'APPRENTISSAGE

Comme pour tout programme d'éducation, il est important de documenter les activités que vous entreprenez et de mesurer l'impact de vos efforts. Pour ce faire, assurez-vous qu'au moins une partie de votre contenu de formation comporte des questions d'évaluation. Si vous utilisez un système de gestion de l'apprentissage, vous avez probablement les outils nécessaires pour suivre les niveaux de participation et les résultats de la formation. Vous pouvez utiliser ces mesures pour identifier les apprenants qui ont besoin d'une formation supplémentaire pour renforcer leur apprentissage.

Ces outils peuvent également servir de passerelle pour intégrer des jeux ou des incitations à votre programme de formation (par exemple, vous pouvez décerner des prix au personnel ou aux services ayant obtenu les meilleurs résultats).

Si vous ne disposez pas d'outils d'évaluation intégrés dans le contenu de votre formation, vous pouvez facilement prévoir de procéder à vos propres évaluations sur une base régulière, en utilisant les stratégies d'évaluation décrites ci-dessus. Au fil du temps, cela vous aidera à identifier les tendances et les progrès.

Au-delà de la formation formelle, saisissez toutes les occasions de sensibiliser votre personnel aux questions de protection des renseignements personnels pour renforcer l'apprentissage. Cela peut se faire de différentes manières. Il peut être aussi simple que d'inclure la protection des renseignements personnels dans votre manuel de l'employé ou dans le processus d'accueil de nouveaux employés. Il peut également s'agir d'envoyer périodiquement des courriels de sensibilisation, ou de partager un article ou une ressource traitant des questions de protection des renseignements personnels avec un collègue.

L'outil d'hameçonnage mentionné plus haut est également un excellent outil pour renforcer l'apprentissage. Vous pouvez encourager les employés à signaler les éventuels courriels d'hameçonnage et profiter de l'occasion pour discuter avec votre personnel des raisons pour lesquelles ils ont signalé (ou non) le courriel en question.

❖ ❖ ❖