APHRSO

Partenaire du milieu depuis 1980

# Politique de gestion des renseignements personnels

*Adopté le 11 septembre 2023*

# Introduction

La présente politique constitue le fondement des règles de gouvernance et le cadre de référence en matière de gestion des renseignements personnels.

L'APHRSO accorde une grande importance à la confidentialité et à la protection des renseignements personnels qu'elle détient.

Pour protéger ces données contre tout accès, utilisation ou divulgation non autorisés, celles-ci sont conservées à des endroits à accès limité et sont protégées par divers mécanismes physiques ou informatiques (classement sous clé, utilisation de mot de passe, chiffrement des données informatiques, etc.).

# Contexte

L'APHRSO recueille et traite des renseignements personnels concernant diverses catégories de personnes (membres, répondants ou proches aidants, administrateurs, employés, etc.).

L'APHRSO recueille ces données dans le cadre de ses interactions et à travers ses activités et services. Celles-ci sont recueillies directement auprès des personnes avec lesquelles nous interagissons.

L'APHRSO a donc le devoir et la responsabilité d'assurer la protection des renseignements personnels qu'elle détient et de démontrer sa conformité aux obligations légales qui lui incombent.

Dans cette politique, le terme *renseignement personnel* désigne tout renseignement qui concerne une personne physique et permet, directement ou indirectement, de l'identifier (nom, prénom, adresse, courriel personnel, date de naissance, numéro de téléphone, pièce d'identité, etc.).

# Champ d'application

La présente politique s'applique à tout membre du personnel autorisé qui recueille, utilise, communique, conserve ou détruit des renseignements personnels dans le cadre de ses fonctions.

# Objectifs de la politique

La présente politique vise à :

- Respecter les obligations légales en matière de protection des renseignements personnels ;
- Établir les principes directeurs qui guident nos pratiques dans la gestion des renseignements personnels ;
- Préciser les rôles et les responsabilités des acteurs concernés par cette politique.

# Principes directeurs

Nos pratiques en matière de protection des renseignements personnels reposent sur les principes suivants.

**Responsabilité**
L'APHRSO est responsable des renseignements personnels qu'elle détient et met en place des mécanismes pour en assurer leur protection.

**Confidentialité des renseignements**
L'APHRSO s'assure de la confidentialité des renseignements qu'elle détient et met en place les mesures nécessaires afin de limiter l'utilisation et la communication de ceux-ci.

**Consentement**
L'APHRSO informe toute personne de la collecte de renseignements qui la concerne et obtient son consentement pour les utiliser, à moins que la loi l'autorise à faire autrement.

**Détermination des fins de la collecte de renseignements**
L'APHRSO détermine les fins pour lesquelles elle recueille des renseignements avant de les recueillir.

**Limitation de la collecte**
L'APHRSO ne recueille que les renseignements personnels nécessaires à la réalisation de sa mission et de ses activités.

**Limitation de l'utilisation, de la communication et de la conservation des renseignements**
L'APHRSO limite l'utilisation et la communication des renseignements personnels au personnel autorisé et aux fins auxquelles la personne concernée a consenti, à moins que la loi l'autorise à faire autrement. Les renseignements personnels sont conservés jusqu'à la finalité pour laquelle ils ont été collectés, sous réserve du délai prévu par la Loi pour des obligations fiscales. Ils sont ensuite détruits.

**Exactitude**
L'APHRSO s'assure que les renseignements personnels qu'elle détient sont à jour, exacts et complets tant qu'elle les utilise.

**Mesures de sécurité**
L'APHRSO prend les mesures de sécurité nécessaires pour assurer la protection des renseignements personnels qu'elle recueille, utilise, communique, conserve ou détruit. Les mesures prises doivent être raisonnable compte tenu, notamment, de leur sensibilité, de leur quantité, de la finalité, de leur utilisation et du support utilisé.

**Transparence**
L'APHRSO rend accessibles ses politiques et ses procédures concernant sa gestion des renseignements personnels.

**Droit d'accès et de rectification**
Sous réserve de restrictions prévues par la Loi sur l'accès, l'APHRSO informe toute personne qui en fait la demande de l'existence de renseignements personnels qui la concerne, de l'utilisation qui en est faite et du fait qu'ils ont été communiqués à des tiers. Elle permet à toute personne de consulter ou d'obtenir copie de ses renseignements personnels et de les faire rectifier, le cas échéant.

**Droit de retrait**
Tout membre de l'APHRSO peut, s'il le souhaite, exercer son droit de retirer son consentement à la communication ou à l'utilisation de ses renseignements personnels. Il peut également demander en tout temps le retrait de son statut de membre et par conséquent, la destruction de ses informations personnelles. Il doit en formuler la demande, idéalement par écrit, auprès du personnel qui verra à répondre à cette requête dans les meilleurs délais.

**Traitement des plaintes**
L'APHRSO répond avec diligence à toute plainte concernant la gestion des renseignements personnels qu'elle détient.

## Responsable de la protection des renseignements personnels

Le conseil d'administration a désigné la direction générale pour agir de titre de responsable de la protection des renseignements personnels.

La direction générale vérifie la conformité des activités de l'organisme aux politiques, directives et lois applicables en matière de protection des renseignements personnels.

Elle voit à l'application des principes directeurs qui sous-tendent la présente politique.

Elle met en place des mécanismes pour assurer la protection des renseignements personnels détenus par l'organisme et en assure le suivi.

Elle veille à ce que le personnel développe de bons réflexes et utilise des moyens sécuritaires pour recueillir, utiliser, conserver, communiquer ou détruire des renseignements personnels et les sensibilise à leurs responsabilités à cet égard.

En matière de collecte et d'utilisation de renseignements, elle évalue la légitimité et la nécessité de recueillir de nouveaux renseignements personnels.

Elle procède à une évaluation des facteurs de risque pour tout projet, services ou mécanismes pouvant toucher la sécurité et la protection des renseignements personnels (collecte, utilisation, communication, conservation, destruction, etc.).

Elle donne suite aux demandes d'information et au traitement des plaintes relatifs à la protection des renseignements personnels.

En cas d'incident de confidentialité impliquant un renseignement personnel, elle prend des mesures raisonnables pour diminuer les risques qu'un préjudice soit causé et que de nouveaux incidents de même nature se reproduisent. Si l'incident présente un risque de préjudice sérieux, elle doit, avec diligence, en aviser les personnes concernées, le conseil d'administration et la Commission d'accès à l'information (CAI). Elle doit également tenir à jour un registre des incidents de confidentialité qui devra être transmis à la CAI à sa demande.

# Le personnel

Chaque membre du personnel a l'obligation de prendre les mesures nécessaires pour assurer la protection des renseignements personnels auxquels il a accès. Il doit notamment :

- Collecter uniquement les renseignements autorisés par la direction générale ;
- Utiliser les renseignements personnels uniquement s'il y est autorisé et pour les fins prévues ;
- S'assurer d'y être autorisé avant de communiquer des renseignements personnels ;
- Obtenir l'autorisation de la direction générale avant de détruire des renseignements personnels ;
- Utiliser en tout temps des moyens sécuritaires pour recueillir, utiliser, conserver, communiquer ou détruire des renseignements personnels ;
- Informer la direction générale de toute situation qui pourrait compromettre la protection des renseignements personnels détenus par l'organisme ;
- Informer la direction générale de tout incident de confidentialité ;
- S'assurer de toujours protéger l'information confidentielle pendant son utilisation (coordonnées écrites sur papier, utilisation d'une liste pouvant être vue par une personne non autorisée, etc.).

---

On entend par incident de confidentialité l'accès, le vol ou la perte de document papier contenant de l'information confidentielle; l'accès, la perte ou le vol d'ordinateur ou de support de stockage (disque externe, clé USB, etc.); la consultation ou l'utilisation d'information confidentielle non autorisée; la transmission d'un courriel contenant de l'information confidentielle à un mauvais destinataire; un incident de sécurité informatique, etc.

Pour évaluer le risque de préjudice sérieux, il y a des facteurs importants à considérer :

- La sensibilité des renseignements en cause ;
- Les conséquences appréhendées de leur utilisation (potentiel de fraude ou de vol d'identité) ;
- Utilisation de l'information à des fins malveillantes.