



L'Association d'aide et de loisirs pour personnes à autonomie réduite

POLITIQUE DE CONFIDENTIALITÉ ET DE PROTECTION DES RENSEIGNEMENTS PERSONNELS DE L'ALPAR



**Adopté par le Conseil
d'Administration
le 30 octobre 2024**

TABLE DES MATIÈRES

1. Généralités	3
1.1. Avant-propos	3
1.2. Objectifs	3
1.3. Définitions	4
1.3.1. INDIVIDUS	4
1.3.2. RENSEIGNEMENT PERSONNEL	4
1.3.3. RENSEIGNEMENT SENSIBLE	4
1.3.4. CYCLE DE VIE D'UN RENSEIGNEMENT PERSONNEL	5
1.3.5. CONSENTEMENT TACITE OU EXPLICITE	5
1.3.6. INCIDENT DE CONFIDENTIALITÉ 6	6
1.3.7. CYBERSÉCURITÉ	6
2. Principes et pratiques	6
2.1. Notre engagement	6
2.2. Notre responsable de l'application des normes de protection des renseignements personnels	7
2.3. La collecte des renseignements personnels	7
2.4. Le consentement	8
2.5. L'utilisation et la communication des renseignements personnels	9
2.6. La conservation et la destruction des renseignements personnels	10
2.7. Les mesures de sécurité	10
2.8. La transparence et l'accès aux renseignements personnels	11
2.9. Comment porter plainte à l'égard du non-respect des principes	12
2.9.1. Réception de la plainte	12
2.9.2. Traitement d'une plainte	13
2.10. Les procédures en cas d'incidents de confidentialité	13
3. La gouvernance	14
3.1. Les responsabilités	14
3.1.1. Le conseil d'administration	14
3.1.2. La personne responsable de la PRP	14
3.2. La formation et la diffusion de cette politique	15
3.3. L'évaluation des facteurs relatifs à la vie privée (EFVP)	15
3.4. Les mesures supplémentaires à mettre en place à court et moyen termes	16
4. Tableau des modifications à cette politique	17
5. Références	17
6. Annexes	18
6.1. Annexe 1 : Tableau des renseignements colligés et de la durée de conservation des dossiers	18
6.2. Formulaire de consentement pour la collecte et l'utilisation de renseignements personnels	19
6.3. Accès aux renseignements personnels informatiques	20
6.4. Registre des incidents de confidentialités	20

1. Généralités

1.1. Avant-propos

La vie privée des particuliers doit être équilibrée avec le besoin légitime de l'Alpar de recueillir, d'utiliser et de divulguer des renseignements personnels à des fins raisonnables liées au filtrage et au suivi diligent de ses activités. La nature même des services offerts par l'Alpar, tel que l'accompagnement et le soutien des aînés ainsi que la participation sociale impliquent le recueil, l'utilisation, la divulgation et la conservation de plusieurs renseignements personnels sensibles.

La législation en matière d'accès à l'information et protection de la vie privée (loi 25) contient des dispositions voulant que les organismes doivent protéger les renseignements personnels en leur possession. Non seulement une telle protection est-elle importante pour les individus dont les renseignements personnels sont en jeu, elle l'est également pour les organismes qui pourraient être tenus responsables ou voir leur réputation ternie suivant l'accès, l'utilisation, la conservation ou la divulgation inadéquate de renseignements personnels. Une mauvaise utilisation de ces renseignements peut entraîner de graves conséquences, autant pour les individus que pour l'organisme impliqué.

Outre les exigences en matière de protection, la loi peut accorder aux individus le droit de consulter leurs propres renseignements, en tout ou en partie. Ils pourraient également avoir le droit d'exiger la correction ou la modification de tout renseignement personnel qu'ils jugent inexact. Enfin, les mesures législatives peuvent accorder aux individus le droit de déposer une plainte s'ils croient que l'organisme ne s'acquitte pas de ses obligations en vertu de la loi.

De bonnes pratiques en matière de protection de la vie privée sont essentielles à la bonne gouvernance, à la responsabilisation et à la gestion du risque.

1.2. Objectifs

La présente politique vise à définir le cadre et les responsabilités de chacun en lien avec ce qui suit :

- ⇒ Obtention du consentement des particuliers en ce qui a trait au recueil, à l'utilisation et à la divulgation de leurs renseignements personnels;

- ⇒ Importance de ne pas recueillir plus d'information que nécessaire pour ses activités;
- ⇒ Utilisation de l'information qu'aux fins prévues;
- ⇒ Vérification de l'exactitude de l'information et de sa conservation à des fins raisonnables;
- ⇒ Accès des particuliers à l'information à leur sujet;
- ⇒ Protection de l'information contre tout accès, utilisation ou divulgation inappropriée.

1.3. Définitions

1.3.1. INDIVIDUS

Les personnes à propos desquelles l'organisme collige, utilise et conserve des informations personnelles pour la bonne marche de ses activités. Les « individus » incluent dans ce contexte les membres, les bénévoles, les membres de soutien, les stagiaires, les donateurs, les employés, les collaborateurs et autres personnes ayant communiqué leurs données en vue de rester informés sur les programmes de l'organisme.

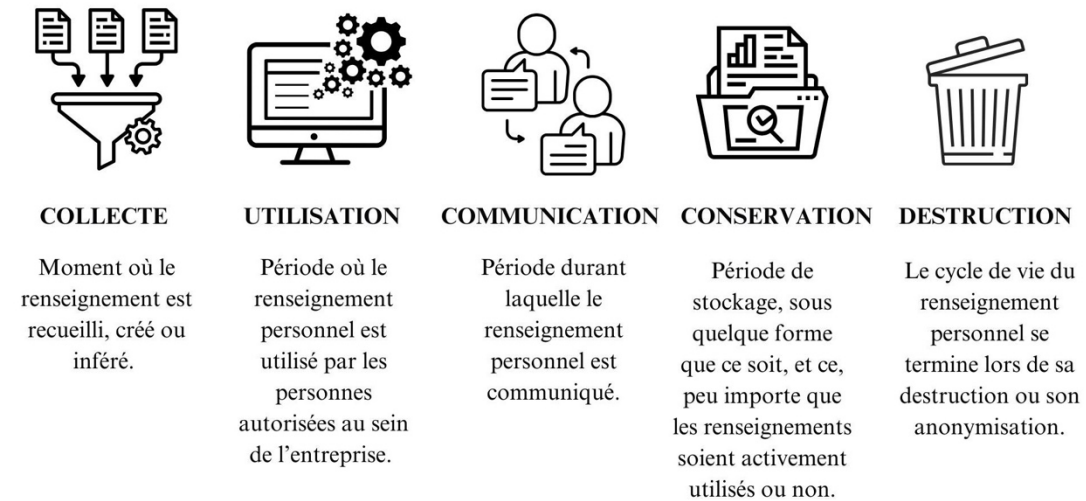
1.3.2. RENSEIGNEMENT PERSONNEL

Un renseignement personnel se définit par toute information permettant d'identifier une personne, telle qu'un nom, une adresse, le numéro de téléphone d'un individu, son dossier médical ou encore une photo ou une image.

1.3.3. RENSEIGNEMENT SENSIBLE

Un renseignement personnel est qualifié de sensible lorsqu'un haut degré d'atteinte raisonnable en matière de vie privée lui est lié, tels un numéro d'assurance social, la date de naissance complète ou des informations médicales.

1.3.4. CYCLE DE VIE D'UN RENSEIGNEMENT PERSONNEL



1.3.5. CONSENTEMENT TACITE OU EXPLICITE

Lorsque l'on recueille des renseignements personnels auprès d'individus, on doit expliquer le but de cette collecte d'information et obtenir leur consentement préalable.

Un consentement implicite (ou tacite) est un consentement qui va de soi, sans être formellement exprimé verbalement ou par écrit. Par exemple, si un bénévole potentiel remplit un formulaire d'inscription, il peut s'attendre raisonnablement à ce que ces informations soient colligées et utilisées dans le cadre de son implication dans l'organisme. Dans un tel cas, l'individu remet volontairement ses renseignements personnels. Habituellement, ce type de consentement ne concerne que les renseignements jugés non sensibles.

Un consentement explicite (ou exprès) est parfois exigé, ce qui signifie que l'organisme doit aviser clairement les individus (verbalement ou par écrit) qu'ils ont l'option d'y consentir ou non et obtenir un acquiescement formel de leur part. Par exemple, si la photo d'un individu est utilisée dans les publications de l'organisme. Des formulaires internes sont habituellement disponibles à ces effets. Ce type de consentement est obligatoire pour les renseignements sensibles.

1.3.6. INCIDENT DE CONFIDENTIALITÉ

Un incident de confidentialité correspond à tout accès, utilisation ou communication non autorisés par la loi d'un renseignement personnel, de même qu'à la perte d'un renseignement personnel ou à toute autre atteinte à sa protection.

Par exemple, un incident de confidentialité pourrait se produire lorsque :

- ⇒ Un membre de l'équipe consulte un renseignement personnel sans autorisation;
- ⇒ Un membre de l'équipe communique des renseignements personnels au mauvais destinataire;
- ⇒ Un membre de l'équipe perd une clé USB contenant des renseignements personnels.

1.3.7. CYBERSÉCURITÉ

La cybersécurité englobe l'ensemble des moyens qui permettent d'assurer la sécurité des réseaux et des systèmes informatiques. Il s'agit des manières d'assurer la confidentialité, l'intégrité et la disponibilité de ces systèmes et des données qu'ils hébergent. La cybersécurité est un complément à la sécurité de l'information qui, pour sa part, vise à assurer la confidentialité de toutes les informations, qu'elles soient sur un support numérique ou non.

2. Principes et pratiques

2.1. Notre engagement

- ⇒ Assurer la sécurité et la confidentialité des renseignements obtenus;
- ⇒ Mettre en place des mécanismes afin de protéger les informations confidentielles;
- ⇒ Assurer le traitement confidentiel des plaintes;
- ⇒ Recueillir seulement les données nécessaires ou utiles;
- ⇒ Appliquer la politique de confidentialité dans le respect des valeurs de l'Alpar;

⇒ Agir avec respect et transparence lors de l'application de cette politique et dans le respect des lois en vigueur.

2.2. Notre responsable de l'application des normes de protection des renseignements personnels

Selon l'article 3.1 de la Loi sur la protection des renseignements personnels dans le secteur privé, la personne ayant la plus haute autorité de l'organisation devra veiller à assurer le respect et la mise en œuvre de la Loi. Cette personne exercera la fonction de « responsable de la protection des renseignements personnels ». Cependant, cette fonction pourra être déléguée par écrit, en tout ou en partie, à toute personne.

Dès lors, la directrice générale, Josée Lambert, délègue en totalité sa fonction de « responsable de la protection des renseignements personnels » à la travailleuse sociale de l'organisme, Karine Imbeault.

2.3. La collecte des renseignements personnels

Les renseignements personnels sont recueillis auprès et au sujet des individus afin d'assurer l'efficacité des programmes ou des activités telles que la prestation de nos services, la collecte de fonds, le recrutement, la gestion et la terminaison des relations avec les bénévoles, les stagiaires, les collaborateurs et les employés. L'information peut également servir à tenir des statistiques.

L'annexe 1 du présent document présente les types d'informations colligées au sujet de chaque type d'individus et les fins espérées.

La gestion adéquate des informations permet d'assurer la disponibilité des renseignements personnels pour la prise de décisions et de protéger les droits de l'organisme et des individus. Elle constitue une preuve des progrès et de l'historique des individus, et peut servir de source documentée d'information exacte à leur sujet.

Les obligations suivantes doivent être respectées afin de protéger les renseignements personnels :

- ⇒ Déterminer les fins de la collecte : un intérêt sérieux et légitime doit motiver la constitution d'un dossier sur une personne;
- ⇒ Limiter la collecte de renseignements personnels : la collecte doit se limiter aux renseignements nécessaires aux fins déterminées. En cas de doute, un renseignement personnel est réputé non nécessaire;
- ⇒ Recueillir les renseignements personnels par des moyens légaux et légitimes : sauf exception, la collecte doit se faire auprès de la personne concernée ou son mandataire;
- ⇒ Informer la personne concernée, avant de constituer un dossier :
 - De l'objet du dossier;
 - De l'utilisation qui sera faite des renseignements personnels;
 - Des catégories de personnes qui y auront accès au sein de l'organisme;
 - De l'endroit où ils seront détenus;
 - De ses droits d'accès et de rectification.

2.4. Le consentement

Tout individu est informé de toute collecte, utilisation ou communication de renseignements personnels qui le concernent et y consent de manière tacite ou explicite, à moins qu'il ne soit pas approprié de le faire.

Pour ce faire, l'organisme :

- ⇒ Définit clairement quels renseignements sont obligatoires et essentiels à ses processus, et quels renseignements sont facultatifs;
- ⇒ Décrit comment l'information recueillie sera utilisée dans le cadre de ses activités;
- ⇒ Se montre transparent quant au moment où les renseignements personnels pourraient être divulgués et précise s'ils seront partagés avec d'autres programmes, des tiers externes ou selon les exigences de la loi;
- ⇒ Précise si l'organisme a l'intention de vérifier les renseignements personnels soumis;

- ⇒ S'assure, dans la mesure du possible, que l'information fournie par les individus est complète, exacte et vraie;
- ⇒ Indique des pénalités administratives ou autres qui peuvent s'appliquer si un individu fournit de faux renseignements;
- ⇒ Précise la période de conservation des renseignements personnels;

L'annexe 2 du présent document présente le formulaire remis aux individus pour recueillir leur consentement.

2.5. L'utilisation et la communication des renseignements personnels

Les renseignements personnels ne sont pas utilisés ou communiqués à des fins autres que celles auxquelles ils ont été recueillis, à moins que la personne concernée n'y consente ou que la loi ne l'exige. L'organisme ne conserve les renseignements personnels qu'aussi longtemps que nécessaire pour la réalisation des fins déterminées.

La divulgation de renseignements personnels est assujettie à la législation applicable à l'organisme. Ainsi les renseignements personnels peuvent être divulgués :

- ⇒ Aux fins pour lesquelles l'information a été recueillie ou pour une utilisation alignée avec un besoin particulier;
- ⇒ Si un individu a consenti par écrit à la divulgation de ses renseignements personnels (par exemple, afin de pouvoir communiquer avec le conjoint, un membre de la famille ou un ami d'un membre blessé ou malade);
- ⇒ Si une telle divulgation est nécessaire pour se conformer à une loi fédérale ou provinciale.

À l'Alpar, certains renseignements personnels sont transmis aux membres du personnel, aux stagiaires, aux membres du CA ou aux collaborateurs. Ils sont régis

par cette politique de confidentialité qui les oblige à respecter les normes de confidentialité édictées.

Quelles que soient les circonstances, l'organisme ne loue pas, ne vend pas, ni n'échange les renseignements personnels des individus.

2.6. La conservation et la destruction des renseignements personnels

L'Alpar s'engage :

- ⇒ À fermer à clé les classeurs contenant les dossiers des membres, des bénévoles, des employés, des stagiaires et des collaborateurs ainsi que ceux contenant des renseignements nominatifs, en dehors des heures de bureau ou en l'absence de leurs responsables;
- ⇒ À ne donner l'accès informatique qu'aux personnes responsables;
- ⇒ À assurer la destruction des informations sensibles lorsque celles-ci ne sont plus nécessaires ou à la fin de la période de conservation (voir annexe 1)

Les employées, stagiaires, collaborateurs et bénévoles de l'Alpar s'engagent :

- ⇒ À conserver ou transmettre de manière sécuritaire toutes informations confidentielles qu'ils détiennent dans le cadre de leur fonction;
- ⇒ À remettre à la fin de leur mandat toutes informations, documents reliés aux renseignements personnels auxquels ils ont eu accès durant leur mandat.

2.7. Les mesures de sécurité

Les renseignements personnels sont protégés au moyen de mesures de sécurité correspondant à leur degré de sensibilité.

L'organisme met en place et assure des mesures de protection adéquates afin que l'accès aux renseignements personnels des individus se limite aux personnes suivantes :

- ⇒ Personnes autorisées par l'organisme, qui en ont besoin dans le cadre de leurs fonctions;
- ⇒ Personnes à qui les individus ont donné leur consentement;
- ⇒ Personnes autorisées par la loi.

La préparation et la gestion de dossiers électroniques et papier assurent le maintien de leur intégrité et de leur authenticité par l'adoption des mécanismes de contrôle qui permettent le suivi de leurs mouvements et préviennent tout accès ou utilisation non autorisée, ou encore toute modification ou suppression inappropriée et malicieuse.

L'Alpar déploie tous les efforts raisonnables en lien avec la mise en place de mesures de protection nécessaires contre la perte, l'utilisation malveillante et l'altération des renseignements personnels qu'elle détient. Les politiques de sécurité sont révisées périodiquement et améliorées au besoin.

Des réseaux de données sûrs, protégés par des pare-feux répondant aux normes de l'industrie, sont utilisés et s'appliquent aussi pour l'utilisation des ordinateurs, à Internet et du courrier électronique.

[L'annexe 3](#) vous renseigne sur les moyens de contrôle en place pour bien protéger les données informatiques.

2.8. La transparence et l'accès aux renseignements personnels

L'organisme fait en sorte que des renseignements précis sur ses politiques et ses pratiques concernant la gestion des renseignements personnels soient facilement accessibles à toute personne.

D'ailleurs, l'individu retrouve ces informations lors de son consentement à la collecte des renseignements personnels ([voir annexe 2](#)) ainsi que sur notre site web (Politique de protection des renseignements personnels).

En tout moment, tout individu peut s'enquérir, en formulant une demande écrite à la personne responsable de la protection des renseignements personnels, de l'existence de renseignements personnels le concernant, de l'usage qui en est fait et s'ils ont été

communiqués à des tiers. Il lui sera aussi possible de contester l'exactitude et l'intégralité des renseignements et d'y faire apporter les corrections appropriées.

Sous réserve des exigences juridiques et contractuelles, un individu peut, en tout temps, refuser ou retirer un consentement à certains buts mentionnés en communiquant avec l'organisme.

2.9. Comment porter plainte à l'égard du non-respect des principes

Tout individu peut se plaindre du non-respect de la présente politique ou des principes généralement reconnus en lien avec la protection de la vie privée en communiquant avec Karine Imbeault, la personne responsable de la protection des renseignements personnels (intervention1@alpar.ca ou 514-524-7328).

Toute plainte est traitée de façon confidentielle. Une plainte anonyme est considérée comme non reçue.

2.9.1. Réception de la plainte

Tout employé saisi d'une plainte doit la transmettre, dès sa réception, au responsable de l'application de la politique, soit Karine Imbeault.

Tout employé qui reçoit une plainte verbale doit informer le plaignant de la présente politique et l'inviter à faire parvenir à l'organisme sa plainte par écrit.

La responsable doit accuser réception de la plainte dans les 5 jours ouvrables suivant la réception.

L'accusé de réception doit contenir les renseignements suivants :

- ⇒ Une description de la plainte reçue, précisant le reproche fait à l'Alpar, le préjudice ou la mesure correctrice demandée;
- ⇒ Le nom et les coordonnées de la responsable du traitement de la plainte;

⇒ Dans le cas d'une plainte incomplète, un avis comportant une demande de complément d'information à laquelle le plaignant doit répondre dans un délai fixé, à défaut de quoi la plainte est réputée être abandonnée;

⇒ Les étapes du traitement de la plainte.

2.9.2. Traitement d'une plainte

Le processus de traitement d'une plainte est enclenché au maximum dans les 5 jours ouvrables de sa réception.

Le traitement de la plainte doit être effectué dans un délai raisonnable, soit dans les 30 jours suivant la réception de tous les renseignements nécessaires à son étude.

Dans l'éventualité exceptionnelle où une plainte ne peut être traitée dans le délai prévu, le plaignant doit être informé des motifs du retard et des démarches entreprises à ce jour dans le traitement de la plainte. Il doit également être avisé du délai dans lequel la décision lui sera transmise.

Une fois la plainte examinée et l'analyse complétée, le responsable doit transmettre au plaignant une réponse finale par écrit.

2.10. Les procédures en cas d'incidents de confidentialité

Un registre de tout incident doit être tenu. Voir [annexe 4](#) pour consulter le format de ce registre.

Pour des exemples d'incidents de confidentialité, se référer au point 1.3 des définitions.

Lors d'une détection d'un incident de confidentialité, la personne responsable de la confidentialité des renseignements personnels doit prendre rapidement des mesures afin de diminuer le risque qu'un préjudice soit causé aux personnes concernées. Elle doit enregistrer cet incident au registre et y indiquer les mesures prises pour corriger la situation et pour s'assurer que de nouveaux incidents de même nature n'arrivent plus.

Au surplus, l'Alpar devra aviser la Commission d'accès à l'information (CAI) et les personnes concernées de tout incident de confidentialité si celui-ci implique un renseignement personnel et présente un risque de préjudice sérieux. À titre d'exemples, un préjudice sérieux pourrait être une atteinte au dossier de crédit, un vol d'identité, etc.

Le registre doit être communiqué à la Commission d'accès à l'information sur demande.

3. La gouvernance

3.1. Les responsabilités

3.1.1. Le conseil d'administration

Le conseil a pour responsabilité :

- ⇒ D'approuver la présente politique et ses modifications ultérieures;
- ⇒ D'assurer qu'un suivi adéquat est fait par la personne responsable de la protection des renseignements personnels;
- ⇒ De faire le suivi, sur une base annuelle, de l'application de la présente politique auprès de la personne responsable de la protection des renseignements personnels.

3.1.2. La personne responsable de la protection des renseignements personnels

La personne responsable de la protection des renseignements personnels s'assure :

- ⇒ Que tout le personnel, les collaborateurs, les stagiaires, les membres du CA et les bénévoles aient la formation et la connaissance requises à l'application adéquate de la présente politique et aux principes de la Loi et soulever, le cas échéant, les enjeux en lien avec la présente;

- ⇒ Que les mesures et contrôles soient en place pour assurer la collection adéquate et la bonne gestion des informations personnelles;
- ⇒ Que soit présenté annuellement au conseil d'administration, un bilan de l'application de la présente politique;
- ⇒ De recommander au conseil d'administration les éventuelles modifications à la présente politique.

3.2. La formation et la diffusion de cette politique

Dès l'adoption de cette politique :

- ⇒ Tous les employés, collaborateurs, stagiaires, membres du CA et bénévoles actuels seront formés et sensibilisés à cette politique. La personne responsable de la protection des renseignements personnels choisira et développera le moyen le plus approprié.
- ⇒ Les nouveaux employés, collaborateurs, stagiaires, membres du CA et bénévoles devront être sensibilisés et formés à cette politique dès leur embauche ou leur adhésion à l'organisme. La personne responsable de la protection des renseignements personnels devra leur remettre une copie de cette politique en même temps que les autres politiques et du code d'éthique de l'organisme inclut dans le guide des membres et bénévoles.
- ⇒ Une copie de cette politique sera disponible dans les bureaux de l'Alpar et sur le site Internet. Ainsi, nos membres, nos bénévoles, nos donateurs et nos partenaires pourront y avoir accès en tout temps.

3.3. L'évaluation des facteurs relatifs à la vie privée (EFVP)

L'EFVP est une démarche préventive visant à mieux protéger les renseignements personnels et à mieux respecter la vie privée des personnes physiques.

Elle consiste à considérer tous les facteurs qui auront un impact positif ou négatif pour le respect de la vie privée des personnes concernées.

Une évaluation des risques liés à la vie privée doit être réalisée si nous devons concevoir, développer ou exploiter :

- ⇒ Un projet ou une initiative impliquant des renseignements personnels;
- ⇒ Un projet ou une initiative risquant d'avoir une incidence sur le respect de la vie privée des personnes.

Exemples de projets concernés pouvant impliquer la collecte, l'utilisation ou la communication des renseignements personnels :

- ⇒ Développer un nouveau système d'information ou une technique de personnalisation d'un service
- ⇒ Chercher une nouvelle clientèle, explorer de nouveaux marchés;
- ⇒ Comparer différentes versions de bases de données ou de fichiers;

L'EFVP doit être réalisée au tout début du projet plutôt qu'en fin de parcours :

- ⇒ Pour pouvoir influencer son déroulement en cours de route;
- ⇒ Pour agir et choisir la solution qui protège et respecte le mieux la vie privée.

La personne responsable de la protection des renseignements personnels est également responsable d'effectuer cette démarche.

3.4. Les mesures supplémentaires à mettre en place à court et moyen termes

Même si nous jugeons nos mesures de cybersécurité actuelles suffisantes pour garantir la confidentialité des données, nous devons planifier des mesures supplémentaires afin de ne pas devenir vulnérables. Ce domaine est en constant changement et nous devons rester vigilants.

Voici une liste des activités à réaliser à court terme :

- ⇒ Réaliser une étude de vulnérabilité de nos postes actuels et identifier des solutions pour en améliorer la sécurité. Implanter par la suite les solutions choisies;
- ⇒ Démarrer un projet qui nous amènera à nous conformer à la dernière étape de la loi 25 : le droit à la portabilité des données (échéance septembre 2024)

Le droit à la portabilité des données permet à une personne d'obtenir une copie des renseignements personnels qu'une organisation détient à son sujet dans un format intelligible. Dans certains cas, ce droit permet également à la personne de demander le transfert de ses renseignements personnels d'une organisation à l'autre. L'un des objectifs principaux de ce droit est de permettre aux individus d'avoir plus de contrôle sur leurs renseignements personnels. La loi prévoit que l'entreprise qui détient un renseignement personnel sur une personne devra, à sa demande, lui en confirmer l'existence et lui communiquer ce renseignement personnel informatisé. Il devra lui être communiqué sur demande dans un format technologique structuré et couramment utilisé. Enfin, ce renseignement devra être communiqué, toujours à sa demande, à toute personne ou à tout organisme autorisé par la loi à recueillir un tel renseignement.

4. Tableau des modifications à cette politique

Date	Modification	Version du document
30 octobre 2024	Approbation par le conseil d'administration	24-01

5. Références

Voici la liste des documents consultés pour la rédaction de cette politique.

- ⇒ Application de la loi 25, COMACO
- ⇒ Guide pratique pour l'application de la loi 25 de Cybereco
- ⇒ Les obligations des organismes communautaires selon la loi 25 sur la protection des renseignements personnels (RP) de Dubé Latreille Avocats inc.
- ⇒ Loi 25 : Par où commencer? De CY-CLIC

- ⇒ Politique de protection des renseignements personnels des Accordailles
- ⇒ Politique de protection des renseignements personnels de la vie privée de l'Oasis des enfants
- ⇒ Vers la conformité à la loi sur le privé de la Commission d'accès à l'information du Québec

6. Annexes

6.1. Annexe 1 : Tableau des renseignements colligés et de la durée de conservation des dossiers

Quel type de RP collectons-nous ?	Pourquoi collecte-t-on ces RP ?	Quels sont les délais de conservation ?
-----------------------------------	---------------------------------	---

6.2. Annexe 2 : Formulaire de consentement pour la collecte et l'utilisation de renseignements personnels



Formulaire de consentement pour la collecte et l'utilisation de renseignements personnels

Je soussigné(e) donne par la présente mon consentement à la collecte, à l'utilisation et à la divulgation de mes renseignements personnels par ALPAR dans le but de me fournir des services d'aide et de loisirs.

Je reconnais avoir reçu des informations sur la manière dont mes renseignements personnels seront collectés, utilisés, partagés, stockés et protégés.

Je reconnais avoir reçu des informations sur mes droits relatifs à mes renseignements personnels et que ces dernières se retrouvent dans la politique de confidentialité de l'organisme.

Je comprends que le consentement est valide pour la durée de mon adhésion (1 an) et que je peux retirer mon consentement à la collecte et à l'utilisation de mes renseignements personnels à tout moment selon la procédure décrite dans la politique de confidentialité de l'organisme. Cependant, cela pourrait empêcher l'organisme de me fournir des services de qualité adaptés à mes besoins.

J'ai lu et compris les informations ci-dessus et je consens volontairement à la collecte et à l'utilisation de mes renseignements personnels telle que décrite.

Signature : _____

Nom (en lettre moulée): _____

Date : _____

☐ Je consens que mes photos et vidéos soient utilisées par l'Alpar à des fins de communication. Je comprends qu'à partir du moment où ma photo et/ou ma vidéo circule sur le web et les réseaux sociaux, elle appartient au domaine public.

5350 rue Lafond, Montréal (Québec) H1X 2X2 - Tél. : 514 524-7328 - info@alpar.ca-www.alpar.ca

6.3. Accès aux renseignements personnels informatiques

Source des données	Type des données	Qui a accès	Contrôle d'accès
--------------------	------------------	-------------	------------------

6.4. Annexe 4 : Registre des incidents de confidentialité - EXEMPLE

Date de l'incident	Date de détection	Circonstances de l'incident	Nbre de personnes	Noms et coordonnées	Catégorie de RP concernés	Préjudice sérieux	CAI informée	Date CAI avisée	Clients informés	Date clients avisés	Mesures prises
Exemple : 2023-01-19	2023-01-23	Compte MailChimp piraté	57	Prénom et nom - Adresse courriel - N° de téléphone	Nom, prénom, adresse courriel, date de naissance (avec année)	Oui	À faire	2023-02-27	Oui	2023-02-27	Sécurité renforcée : Mot de passe changé + 2FA activée