Scouts du Canada

Protection des renseignements personnels —

Guide pour les districts et les groupes

Table des matières

Contexte	3
Quels sont les avantages de cette mesure ?	3
Qu'est-ce qu'un renseignement personnel ?	3
Demande de consentement pour l'utilisation des renseignements des usagers	4
Incident de confidentialité	5
Quoi faire si une brèche de sécurité survient?	5
Quoi conserver?	5
Comment conserver les documents?	5
Destruction des données	6
Droit à l'effacement	6
Droit à la portabilité des renseignements personnels	7
Rappel sur les meilleures pratiques	7
Annexe A	8
Annexe B	10
Annexe C	10

Contexte

Depuis 2001, au niveau fédéral, la Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE) établit les règles de base sur la façon dont les organisations qui se livrent à des activités commerciales doivent traiter les renseignements personnels. Cette loi s'applique maintenant de façon générale à toutes les organisations du secteur **privé** qui recueillent, utilisent ou divulguent des renseignements personnels dans le cadre d'activités commerciales au Canada. De plus, les provinces peuvent adopter leurs propres lois essentiellement semblables sur la protection des renseignements personnels dans le secteur privé, et de nombreuses provinces l'ont fait.[1]

En outre, cette loi vient modifier et ajouter plusieurs droits et obligations au niveau de la protection des données personnelles des citoyennes et citoyens afin de mieux refléter la réalité d'aujourd'hui. Plus particulièrement, elle permet une meilleure protection des droits de la personne en lui donnant plus de pouvoir sur le traitement de ses données personnelles et en promouvant une meilleure compréhension quant aux conséquences de ses choix.

Ainsi, chaque personne naviguant sur le Web et donnant ses informations à un organisme possède un meilleur contrôle sur ses renseignements personnels.

Dans le cadre de cette nouvelle législation, nous tenons à vous informer que *L'Association des Scouts du Canada* est conforme et nous avons procédé à plusieurs mises à jour sur notre site Web. À cet effet, l'option de paramétrage des témoins sur notre site est maintenant active ainsi que la possibilité de prévaloir des droits d'effacement, d'indexation et de portabilité des renseignements de nos membres directement depuis la page de nos politiques de protection des données, que vous pouvez retrouver en pied de page de notre site Web. Nous vous invitons à en prendre connaissance en cliquant ici https://scoutsducanada.ca/politique-de-confidentialite/

Quels sont les avantages de cette mesure ?

Ces mesures assurent une meilleure protection de la vie privée, tout en tenant compte de la réalité technologique d'aujourd'hui. L'adoption de la loi permet aux citoyennes et aux citoyens de bénéficier particulièrement des consentements demandés en termes simples et clairs.

Qu'est-ce qu'un renseignement personnel ?

Un renseignement personnel est une information concernant une personne physique qui peut être identifiée, soit directement ou indirectement. Il s'agit d'informations qui, lorsque prises seules ou combinées avec d'autres données, peuvent permettre l'identification d'un individu. Il existe deux types d'identifiants pour les renseignements personnels : directs et indirects. Les identifiants directs se réfèrent aux informations qui peuvent identifier une personne sans avoir besoin d'autres données. Ces informations incluent mais ne sont pas limitées à ce qui suit:

- Nom complet
- Numéro de sécurité sociale

1 https://www.justice.gc.ca/fra/sjc-csj/lprp-pa/modern.html

- Numéro de permis de conduire
- Numéro de carte d'identité
- Adresse courriel personnelle
- Numéro de téléphone personnel
- Adresse physique personnelle
- Date de naissance
- Numéro de carte de crédit

Les identifiants indirects, en revanche, sont les informations qui, en elles-mêmes, ne permettent pas d'identifier une personne, mais qui, lorsqu'elles sont combinées avec d'autres données, peuvent mener à l'identification d'un individu. Ces informations peuvent inclure l'âge, le sexe, la profession, le niveau d'éducation, les données de localisation, les préférences de consommation, et d'autres informations démographiques ou comportementales.

- Sexe
- Âge
- Nationalité
- Profession
- Niveau d'éducation
- Code postal
- Religion
- État civil
- Préférences de consommation
- Données de localisation
- Autres informations démographiques ou comportementales

Il est important de noter que ce qui constitue un identifiant direct ou indirect peut varier en fonction du contexte et de la combinaison d'informations disponibles. Par exemple, un code postal peut être un identifiant direct dans une petite communauté rurale où il ne s'applique qu'à quelques maisons, alors qu'il est généralement considéré comme un identifiant indirect dans les zones urbaines denses. Par conséquent, lors de la manipulation de données personnelles, il est essentiel de considérer attentivement les implications potentielles en matière de confidentialité.

Demande de consentement pour l'utilisation des renseignements des usagers

Avant toute utilisation des renseignements personnels de vos utilisateurs, vous devez demander leur consentement. Par exemple : lors de l'inscription d'un membre via le formulaire, une note doit être présente sur le formulaire qui stipule le consentement pour l'utilisation de ces renseignements. La forme du consentement peut varier selon les circonstances et le type de renseignements recherchés. Le consentement peut être explicite ou implicite et peut être fourni directement par la personne ou par son représentant autorisé.

De préférence, il faut obtenir un consentement explicite, que ce soit verbalement, par voie électronique ou par écrit. Le consentement implicite peut être raisonnablement déduit de l'action ou l'inaction d'une personne, par exemple, le fait de fournir un nom et une adresse pour recevoir une publication ou un nom et un numéro de téléphone pour obtenir une ré-

ponse à une question. Pour déterminer le type de consentement approprié, vous devez tenir compte de la sensibilité des renseignements personnels en cause, des fins auxquelles ils sont recueillis et des attentes raisonnables de la personne. Si vous voulez utiliser les renseignements personnels à une nouvelle fin, vous devez décrire l'utilisation prévue et devez demander à nouveau le consentement.

Incident de confidentialité

On entend par « incident de confidentialité » :

- L'accès non autorisé par la Loi à un renseignement personnel;
- L'utilisation non autorisée par la Loi d'un renseignement personnel;
- La communication non autorisée par la Loi d'un renseignement personnel;
- La perte d'un renseignement personnel ou toute autre atteinte à la protection d'un tel renseignement.

Quoi faire si une brèche de sécurité survient?

Advenant un incident qui met en jeu les données personnelles de nos membres, un *registre des incidents de confidentialité* doit être tenu et cela, peu importe leur ampleur ou leur risque de préjudice. Si un incident présente un risque qu'un préjudice sérieux soit causé, l'organisme public doit aviser la Commission d'accès à l'information. Les usagers concernés par un incident doivent être mis au courant; un avis de signalement d'incident est disponible et personnalisable pour que vous puissiez rapidement informer les gens touchés par une brèche de sécurité.

Pour la province de Québec, remplir l'avis suivant: *Formulaire d'avis de la Commission

Pour les autres provinces: *Signaler une atteinte à la vie privée

*Liens en annexe C

Quoi conserver?

Toutes données qui informent qu'une personne a été membre ou bénévole chez les scouts doivent être conservées et protégées. Les renseignements personnels comme les coordonnées d'un membre, renseignement sur l'identité (date de naissance, genre, photo) doivent être conservées jusqu'à l'arrête d'activité avec le membre. Après l'arrête d'activité, vous devez les archiver indéfiniment. Dans une situation qui impliquerait que l'on fasse appel aux assurances, il est primordial d'avoir accès aux données confidentielles et ce même des années, voir décennies plus tard.

Voir l'annexe A pour le tableau *Durée de conservation des documents*

Comment conserver les documents?

La conservation des renseignements personnels doit respecter certaines pratiques afin de prévenir tout incident de confidentialité, qui peut survenir à toutes les étapes du cycle de vie du renseignement personnel.

Afin d'assurer la protection des renseignements personnels sur support physique, il est recommandé de conserver sous clé tout document papier qui contient des renseignements personnels et d'adopter de bonnes pratiques de manipulation des support physiques contenant des renseignements personnels afin d'éviter qu'un document contenant une information confidentielle ne se trouve à la vue. À titre d'exemple, un cartable regroupant les fiches santé des jeunes ne doit pas être laissé sur une table sans surveillance. Ce type de document doit être gardé dans un endroit sûr et doit être consulté uniquement par les responsables.

*Si un groupe venait à fermer, tous les documents doivent être rapatriés au bureau de l'Association nationale pour être archivée. Si un groupe n'a pas de local permanent, il est préférable de transmettre les documents au district pour qu'il en assure la conservation. De la même façon, si un district n'a pas l'espace nécessaire pour archiver de la documentation, merci de contacter le centre national, nous vous proposerons des alternatives.

Destruction des données

Dans des cas rarissimes, des documents peuvent être détruit; une procédure rigoureuse doit être suivie. La destruction sécurisée des données est une étape essentielle pour garantir la confidentialité et la sécurité des informations.

Enfin, il est essentiel de documenter le processus de destruction des données. Cela peut inclure la date de la destruction, la méthode utilisée, et toute autre information pertinente. Cette documentation peut être importante pour prouver que vous avez respecté vos obligations de protection des données. Assurez-vous de toujours remplir un registre de destruction des données qui inclus les données suivantes;

1. Identification des données

Quelles données ont été détruites ? Cela peut inclure des informations telles que le type de données, l'emplacement de stockage, et toute autre information pertinente.

2. Méthode de destruction

Comment les données ont-elles été détruites ? Cela devrait inclure des détails sur la méthode de destruction utilisée, y compris le nom de tout logiciel ou équipement utilisé.

3. Date et heure

Quand les données ont-elles été détruites ? La date et l'heure précise de la destruction devraient être enregistrées.

4. Personnes impliquées

Qui a effectué la destruction des données ? Cela devrait inclure le nom de la personne ou de l'équipe qui a effectué la destruction, ainsi que le nom de toute personne qui a supervisé ou vérifié le processus.

5. Confirmation de la destruction

Comment pouvez-vous confirmer que les données ont été détruites de manière sécurisée? Cela peut inclure des détails sur les vérifications ou les audits effectués pour confirmer la destruction des données.

Droit à l'effacement

Les utilisateurs de vos services pourront demander que vous cessiez de diffuser leurs renseignements personnels que vous possédez à leur sujet. Vous devrez le faire dans un délai raisonnable. Dans le cas légitime où l'information vous serait cruciale et que vous ne pourriez

pas détruire les renseignements personnels, vous aurez le droit de les anonymiser, ce qui revient à les rendre complètement anonymes, de manière que personne ne pourra identifier cet utilisateur sur vos plateformes publiques.

Droit à la portabilité des renseignements personnels

Un usager sera en droit d'exiger une copie des renseignements personnels que vous détenez sur lui. Ainsi, dans un tel cas, vous devez lui transmettre le tout dans un délai raisonnable.

Rappel sur les meilleures pratiques

1. Lorsque vous transmettez de l'information par courriel à plusieurs personnes à la fois, cachez les destinataires. Inscrivez les adresses courriels en cci.
2. Minimisez les données collectées : Ne collectez que les données personnelles nécessaires à vos activités. Plus vous collectez de données, plus vous devez les protéger.
3. Consentement : Assurez-vous d'obtenir le consentement des individus avant de collecter, utiliser ou divulguer leurs informations personnelles. Le consentement doit être libre, éclairé et spécifique.
4. Accès et correction : Assurez-vous que les individus ont le droit d'accéder à leurs informations personnelles et de les corriger si elles sont inexactes.
5. Transparence : Soyez transparent sur votre façon de collecter, utiliser et divulguer les informations personnelles.
6. Partage de documents : Lorsque vous partagez un document qui contient des renseignements personnels (un programme de camp par exemple), assurez-vous d'en supprimer tous les renseignements personnels avant de le diffuser.

La loi mentionne que nous devrions détruire tous les renseignements lorsque nous n'en avons plus besoin. **Cependant, il est important de conserver toutes les informations qui se rattachent à des évènements scouts, camps, réunions et autres activités ainsi que les personnes qui y ont participé (jeunes et adultes).**

Il est préférable d'être conservateur et de garder davantage de renseignement que vous devrez sécuriser que de détruire des éléments qui pourraient être pertinents dans le futur.

Évitez le dilemme à savoir quoi conserver en recueillant l'information minimale à vos activités.

** Aux termes de la Loi, le consentement de tout mineur de moins de 14 ans doit être donné par le titulaire de l'autorité parentale ou un tuteur*.

*Tuteur : une personne peut être désignée à titre de tuteur à la suite du décès des parents d'un enfant mineur ou en raison de leur inaptitude à en prendre soin. Le tuteur doit veiller au bien-être de l'enfant ou gérer son patrimoine.

Pour toute question, n'hésitez pas à communiquer avec Valérie Masson, Responsable de la protection des renseignements personnels et Direction générale adjointe : valerie.masson@scoutsducanada.ca

Annexe A

Durée de conservation des documents

Administration du groupe – Général		
Document	Durée de conservation	Justification / Remarques
Lettres patentes	À vie	Classeur anti feu (À envoyer au district)
Liste des responsables et des administrateurs du Conseil de gestion	À vie	Conservation au SISC, donc aucune action à prendre pour le groupe
Assemblée générale annuelle : Avis de convocation, ODJ, procès-verbaux et documents afférents	À vie	À envoyer au district chaque année
Assemblée générale extraordinaire : Avis de convocation, ODJ, procès-verbaux et documents afférents	À vie	À envoyer au district (S'il y a lieu)
Rapports annuels	À vie	
Assurances (correspondance, polices, contrat, etc.)	5 ans + l'année en cours	*dépend de la durée de la police
Règlements généraux	À conserver jusqu'à leur remplacement	

Conseil d'administration		
Document	Durée de conservation	Justification / Remarques
Avis de convocation aux réunions	Deux ans	
Procès-Verbaux et documents afférents	À vie	
Résolutions (extraits)	2 ans + l'année en cours	
Avis de mise en candidature, d'élection, etc.	2 ans + l'année en cours	
Lettre de démission d'un administrateur	À vie	

Finances		
Document	Durée de conservation	Justification / Remarques
Budget (Documents relatifs aux budgets du groupe et de ses comités)	À vie	

Annexe A

Comptabilité		
Document	Durée de conservation	Justification / Remarques
Comptes à recevoir (factures / pièces justificatives, incluant les dons et souscriptions)	7 ans + l'année en cours	
Comptes à payer (factures / pièces justificatives)	7 ans + l'année en cours	Attention, conserver les factures et les pièces reliées aux investissements (ex. placement, immeuble, etc.)
Liste des comptes à recevoir	7 ans + l'année en cours	
Avis de paiement	7 ans + l'année en cours	
Frais de déplacement	7 ans + l'année en cours	
Reçus émis	7 ans + l'année en cours	
Chèques émis-retournés	7 ans + l'année en cours	
Talon de chèques	2 ans + l'année en cours	
Bordereaux de dépôts	7 ans + l'année en cours	
Comptes de banques (liste des comptes, correspondances, etc.)	7 ans + l'année en cours	
Relevés des compte et conciliations bancaires	7 ans + l'année en cours	
Grand livre général	À vie	
États financiers périodiques	2 ans + l'année en cours	
États financiers annuels	À vie	Mettre avec documentation de l'AGA
Rapport des dépenses de la petite caisse	7 ans + année en cours	
Relevé de carte de crédit	7 ans + année en cours	
Certificats de dépôt à terme et relevés	6 ans après la durée du certificat	
Rapport de vérification externe	À vie	Très rare !
Subventions (Correspondance, demandes, rapports de reddition de compte)	6 ans après la durée de la subvention	

Autres		
Document	Durée de conservation	Justification / Remarques
Plainte d'un membre	2 ans	Dépend de la nature de la plainte. En cas de doute, contacter le district.

Affaires juridiques		
Document	Durée de conservation	Justification / Remarques
Code d'éthique	À vie (jusqu'à son remplacement)	
Règlements du groupe, protocoles d'entente et conventions, contrats, poursuite judiciaire et avis juridiques	À vie	

Annexe A

Membres		
Document	Durée de conservation	Justification / Remarques
Liste des membres	À vie	Conservé via le SISC
Fiches d'inscription, formulaire d'acceptation des risques et fiche de santé	7 ans après que le membre a quitté le groupe	
Autorisation d'administration d'un médicament	7 ans après la tenue de l'activité	
Programme et permis de camp	À vie	Sera conservé par le District

Références

Association des archivistes du Québec, Calendrier de conservation pour associations et autres organismes de même nature, 1996.
Conseil québécois du loisir, Gestion documentaire, 2024.

Annexe B

Tableau comparatif des lois pour la protection des renseignements personnels

Rédigé par le cabinet d'avocats Fasken.

https://www.fasken.com/fr/knowledge/2022/07/26-comparative-table-of-personal-information-protection-laws

Annexe C

Formulaire pour déclarer une fraude/incident de confidentialité

Pour la **province de Québec**, remplir l'avis suivant: Formulaire d'avis de la Commission
https://cai.gouv.qc.ca/uploads/pdfs/CAI_FO_Incident_Conf.pdf

Pour les **autres provinces**: Signaler une atteinte à la vie privée
https://services.priv.gc.ca/atteinte-breach-lprpde-pipeda/fr/inscription

Association des Scouts du Canada

Centre national
7331 rue Saint-Denis,
Montréal, QC, H2R 2E5

514-252-3011 · 1 866 297-2688
infoscout@scoutsducanada.ca
scoutsducanada.ca