Politique de confidentialité

Table des matières

Chapitre I – Objet et champ d'application

ARTICLE 01 – OBJECTIF

Les objectifs de cette procédure sont les suivants :

- Garantir la protection de la vie privée des individus et de se conformer aux obligations légales en matière de protection des renseignements personnels;
- Garantir que toutes les demandes d'accès sont traitées de manière confidentielle, rapide et précise, tout en respectant les droits des individus concernés;
- Fournir un mécanisme structuré pour gérer les demandes de désindexation et de suppression des renseignements personnels émanant de nos membres ou partenaires externes;
- S'assurer que l'organisation est prête à intervenir en cas de cyberincident de manière à pouvoir reprendre rapidement ses activités;
- Établir une liste de contrôle au sein de l'organisation pour encadrer le départ d'un membre de l'équipe.

ARTICLE 02 – PORTÉE

La portée de cette procédure et politique devrait couvrir l'ensemble du cycle de vie des renseignements personnels, depuis leur collecte jusqu'à leur destruction. Elle concerne tous les employés et parties prenantes impliquées dans la collecte, le traitement, la conservation, la destruction et l'anonymisation des renseignements personnels conformément aux exigences légales et aux bonnes pratiques en matière de protection de la vie privée.

ARTICLE 03 – DÉFINITIONS

Les définitions ci-bas s'appliquent à toute la politique de confidentialité :

- **Acteur·rice.s de l'organisme**: termes englobants toutes les personnes administratrices, dirigeantes, employées, bénévoles et participantes au programme PAAS action de l'organisme;
- **Renseignements personnels** : toute information permettant d'identifier, directement ou indirectement, une personne physique;
- **Conservation** : stockage sécurisé des renseignements personnels pendant la durée requise;
- **Destruction** : suppression, élimination ou effacement définitifs des renseignements personnels;
- **Anonymisation** : processus de modification des renseignements personnels de manière à ne plus permettre en tout temps et de façon irréversible l'identification, directe ou indirecte, des individus concernés;
- **Suppression des renseignements personnels** : action d'effacer complètement les données, les rendant indisponibles et irrécupérables;
- **Désindexation des renseignements personnels** : retrait des informations des moteurs de recherche, les rendant moins visibles, mais toujours accessibles directement;

Note : La suppression élimine définitivement les données, tandis que la désindexation limite leur visibilité en ligne.

Les renseignements personnels ont été catégorisés de la façon suivante :

- Renseignements concernant les acteur·rice·s de l'organisation (excluant les personnes du conseil d'administration);
- Renseignements concernant les membres du conseil d'administration (C.A.);
- Renseignements concernant les membres de l'organisation n'appartenant pas aux catégories précédentes;

ARTICLE 04 – RESPONSABILITÉS

Les responsabilités relatives à l'application de la présente politique sont segmentées en deux (2) rôles distincts, mais peuvent être assumées et redivisées au besoin par le conseil d'administration. La responsabilité est attribuée par le C.A., et peut être modifiée par celui-ci à tout moment par une résolution adoptée selon les procédures en vigueur.

- Responsable de la protection des renseignements personnels : assignée de facto à la direction générale, mais peut être redistribuée;
- Diffusion de et éducation sur la politique et ses annexes: doit être assigné par le CA, mais peut être temporairement assignée à une personne responsable par la direction générale.

Chapitre II – Procédure de conservation, de destruction, et d'anonymisation des renseignements personnels

ARTICLE 05 – DURÉE DE CONSERVATION

La durée de conservation pour chacune de ces catégories a été établie selon une grille jointe à la présente politique en Annexe A – Normes sur la protection des renseignements personnels – Cadre d'application.

Attention des délais de conservation spécifiques peuvent s'appliquer.

ARTICLE 06 – MÉTHODES DE STOCKAGE SÉCURISÉ

6.1 Les modalités précises de stockage de données sécurisées sont établies selon une grille jointe à la présente politique en Annexe A – Normes sur la protection des renseignements personnels – Cadre d'application.

6.2 Le degré de sensibilité de chacun de ces lieux de stockage a été établi.

6.3 Ces lieux de stockage, qu'ils soient papier ou numérique, sont adéquatement sécurisés.

6.4 L'accès à ces lieux de stockage a été restreint aux seules personnes autorisées.

6.5 Il est absolument interdit de transférer des données confidentielles très sensibles (NAS) par courriel. Ces informations, si elles existent de façon écrite, doivent être conservées sous clefs avec accès limités aux personnes en ayant absolument besoin, ou derrière un logiciel sécurisé.

ARTICLE 07 - DESTRUCTION DES RENSEIGNEMENTS PERSONNELS

7.1 Pour les renseignements personnels sur papier, ils devront être totalement déchiquetés.

7.2 Pour les renseignements personnels numériques, ils devront être totalement supprimés des appareils (ordinateurs, téléphone, tablette, disque dur externe), des serveurs et des outils infonuagiques.

7.3 Le calendrier de destruction en fonction de la durée de conservation devra être établi pour chaque catégorie de renseignements personnels selon la grille jointe à la présente politique en Annexe A – Normes sur la protection des renseignements personnels – Cadre d'application.

7.4 Il faut s'assurer que la destruction est réalisée de manière à ce que les renseignements personnels ne puissent pas être récupérés ou reconstitués.

ARTICLE 08 - ANONYMISATION DES RENSEIGNEMENTS PERSONNELS

L'anonymisation des renseignements personnels ne devrait se faire que si l'organisation souhaite les conserver et les utiliser à des fins sérieuses et légitimes.

La méthode d'anonymisation des renseignements personnels choisie est la suivante : Utilisation du logiciel Acrobat de la firme Adobe, et de son utilitaire de caviardage. Suppression immédiate des fichiers originaux après la sauvegarde des fichiers caviardés.

Il faudra s'assurer que l'information restante ne permette plus de façon irréversible l'identification directe ou indirecte des individus concernés et s'assurer d'évaluer régulièrement le risque de réidentification des données anonymisées en effectuant des tests et des analyses pour garantir leur efficacité.

ARTICLE 09 - FORMATION ET SENSIBILISATION DU PERSONNEL

Il est essentiel de s'assurer de fournir une formation régulière aux employés sur la procédure de conservation, de destruction et d'anonymisation des renseignements personnels, ainsi que sur les risques liés à la violation de la vie privée.

Cela inclut également la sensibilisation du personnel aux bonnes pratiques de sécurité des données et à l'importance du respect des procédures établies.

Chapitre III – Protocoles de gestion des processus administratifs relatifs aux données confidentielles

ARTICLE 10 – PROTOCOLES DE GESTION ADMINISTRATIVE

Des protocoles précis de gestion administrative pour les différentes procédures à suivre sont instaurés par le conseil d'administration de l'organisation, et sous la responsabilité de la personne désignée par le C.A. comme responsable de la protection des renseignements personnels. Ces protocoles peuvent être modifiés par une résolution de C.A. afin de permettre à l'organisation de s'adapter aux divers changements de procédures et de technologies dans le futur.

ARTICLE 11 - PROCÉDURE DE DEMANDE D'ACCÈS

L'individu qui souhaite accéder à ses renseignements personnels doit soumettre une demande écrite au responsable de la protection des renseignements personnels de l'organisation. La demande peut être envoyée par courriel ou par courrier postal.

Le conseil d'administration doit maintenir un protocole à suivre pour cette procédure, et soutenir les personnes en ayant le besoin.

ARTICLE 12 - PROCÉDURE DE TRAITEMENT DES PLAINTES

L'individu qui souhaite porter plainte en matière de renseignements personnels doit pouvoir le faire. Cette personne doit soumettre une demande écrite au responsable de la protection des renseignements personnels de l'organisation. La demande peut être envoyée par courriel ou par courrier postal.

Le conseil d'administration doit maintenir un protocole à suivre pour cette procédure, et soutenir les personnes en ayant le besoin.

ARTICLE 13 – PORTÉE SPÉCIFIQUE DE LA PROCÉDURE DE DÉSINDEXATION ET DE SUPPRESSION DES RENSEIGNEMENTS PERSONNELS

Cette procédure s'applique à notre équipe interne chargée de la gestion des demandes de désindexation et de suppression des renseignements personnels. Elle couvre toutes les informations publiées sur nos plateformes en ligne, y compris notre site web, nos applications mobiles, nos bases de données ou tout autre support numérique.

ARTICLE 14 – PROCÉDURE DE DEMANDE DE DÉSINDEXATION ET DE SUPPRESSION DES RENSEIGNEMENTS PERSONNELS

Les membres, partenaires, ou acteur·rice·s de l'organisme peuvent soumettre leurs demandes de désindexation et de suppression des renseignements personnels par le biais de canaux spécifiques tels que l'adresse courriel dédiée ou le numéro de téléphone. Le conseil d'administration doit maintenir un protocole à suivre pour cette procédure, et soutenir les personnes en ayant le besoin.

ARTICLE 15 – RECONNAÎTRE UN CYBERINCIDENT

Tout·e acteur·rice de l'organisation doit être à l'affut de la possibilité d'un cyberincident. Des ressources appropriées, ainsi que des protocoles à suivre pour les différents cas de figure doivent être maintenus par le conseil d'administration, et mis à dispositions des personnes en ayant le besoin.

ARTICLE 16 – INCIDENTS

S'il a été confirmé qu'un incident de sécurité lié à une atteinte à la protection des renseignements personnels s'est produit, il faudra effectuer les étapes suivantes :

- Examiner l'atteinte à la protection des renseignements personnels pour déterminer si des renseignements personnels ont été perdus en raison d'un accès ou utilisation non autorisée, d'une divulgation non autorisée ou de toute atteinte à la protection de ces renseignements personnels et qu'il existe un risque de préjudice sérieux pour les personnes concernées.
    - Dans un tel cas, le signaler à la Commission de l'accès à l'information au Québec;
    - Et, le signaler également aux personnes dont les renseignements personnels sont visés par l'incident.

ARTICLE 17 - PROCÉDURES DE GESTION DU ROULEMENT DU PERSONNEL

Un protocole relatif à la gestion du roulement du personnel doit être maintenu par l'administration et validé par le conseil d'administration pour limiter la possibilité de tout incident relatif à la confidentialité des renseignements.