Guide de procédures de gestion des renseignements personnels

15 janvier 2025

Date d'entrée en vigueur

TABLE DES MATIÈRES

1. INTRODUCTION

Le présent guide de procédures découle de la « politique de protection des renseignements personnels » de l'ARLPH.

Le présent document se veut d'être un outil de gestion afin que l'ARLPH se conforme à sa politique précédemment mentionnée et, par conséquent, qu'elle se conforme aux lois visant la protection des renseignements personnels.

Les procédures suivantes sont contenues dans le présent guide de gestion :

- Procédure de conservation et de destruction des renseignements personnels,
- Procédure de demande d'accès aux renseignements personnels et de traitement des plaintes,
- Procédure de demande de désindexation et de suppression des renseignements personnels,
- Procédure de gestion des incidents de sécurité et violations des renseignements personnels,
- Procédure de gestion du roulement du personnel.

2. PROCÉDURE DE CONSERVATION ET DE DESTRUCTION DES RENSEIGNEMENTS PERSONNELS

2.1. APERÇU

La procédure de conservation et de destruction des renseignements personnels vise à garantir la protection de la vie privée des individus, se conformer aux lois sur la protection des renseignements personnels, prévenir les incidents de confidentialité impliquant des renseignements personnels et les atteintes à la sécurité, maintenir la confiance des membres et protéger la réputation de l'ARLPH.

2.2. OBJECTIF

Le but de cette procédure est de garantir la protection de la vie privée des individus et de se conformer aux obligations légales en matière de protection des renseignements personnels.

2.3. PORTÉE

La portée de cette procédure couvre 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 et la destruction des renseignements personnels conformément aux exigences légales et aux bonnes pratiques en matière de protection de la vie privée.

2.4. DÉFINITIONS

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 définitif des renseignements personnels.

2.5. PROCÉDURE

Préambule

L'ARLPH peut, au besoin, constituer un ou des dossiers contenant des renseignements confidentiels concernant des participants. La constitution de tels dossiers a pour objet de lui permettre de réaliser un évènement, une publication, de réaliser une activité ou de fournir un service.

L'ARLPH peut seulement recueillir les renseignements confidentiels qui sont nécessaires aux fins du dossier et peut utiliser les renseignements confidentiels seulement à ces fins. Au préalable, un tel consentement sera consigné à l'aide du « Formulaire de consentement pour la collecte et l'utilisation des renseignements personnels » joint au présent guide.

Les renseignements confidentiels peuvent seulement être recueillis auprès de la personne concernée, à moins que celle-ci consente à ce que la cueillette soit réalisée auprès d'autrui ou que la loi l'autorise.

L'ARLPH peut, au besoin, constituer un ou des dossiers contenant des renseignements personnels concernant ses employés et bénévoles. La constitution de tels dossiers a pour objet de :

- Maintenir les coordonnées à jour ;
- Documenter des situations de travail ou de bénévolat ;
- Permettre, dans le cas des employés rémunérés, la réalisation des tâches administratives requises ou permises par la loi (impôt sur le revenu, assurances collectives, etc.) ;

Les employées/employés ayant accès aux renseignements personnels doivent :

- s'assurer que les renseignements personnels sont gardés à l'abri de tout dommage physique ou accès non autorisé ;
- S'assurer que tous les documents électroniques comportant des renseignements personnels, incluant ceux copiés sur un appareil de stockage portatif, soient protégés par des mots de passe. Ces mots de passe sont modifiés à une fréquence régulière ainsi qu'à chaque fois que les personnes ayant accès aux dossiers concernés sont remplacées ;
- Garder les renseignements personnels en format papier dans des classeurs pouvant être verrouillés et s'assurer que les classeurs soient verrouillés à la fin de chaque journée de travail. Les clés des classeurs doivent être gardées dans des endroits sûrs.

Durée de conservation

Les renseignements personnels ont été catégorisés de la façon suivante :

- renseignements concernant les employés,
- renseignements concernant les membres du conseil d'administration,
- renseignements concernant les travailleurs autonomes collaborant avec l'organisation,
- renseignements concernant les membres de l'organisation,
- renseignements concernant les participants,
- renseignements concernant les bénévoles de l'organisation,
- renseignements concernant les donateurs de l'organisation.

Sous réserve du paragraphe suivant, les renseignements personnels sont conservés pendant la période nécessaire à la réalisation des activités pour lesquelles ils ont été collectés.

LA DURÉE DE CONSERVATION POUR CHACUNE DE CES CATÉGORIES A ÉTÉ ÉTABLIE DE LA FAÇON SUIVANTE :

Pour plus de détails sur la durée de conservation pour chacune de ces catégories, se référer à l'inventaire complet des renseignements personnels détenus par notre organisation dans le dossier électronique à cet effet.

Cependant, ils peuvent être conservés pour une durée différente lorsque des lois l'exigent. Ces renseignements personnels sont ensuite détruits de façon sécuritaire.

2.6. Méthode de stockage sécurisé

- Pour plus de détails sur les lieux de stockage des renseignements personnels, se référer à l'inventaire complet des renseignements personnels détenus par notre organisation dans le dossier électronique à cet effet.
- Le degré de sensibilité de chacun de ces lieux de stockage a été établi.
- Ces lieux de stockage, qu'ils soient papier ou numérique, sont adéquatement sécurisés.

2.7. Destruction des renseignements personnels

- Les renseignements personnels sur papier seront totalement déchiquetés.
- Les renseignements personnels numériques seront totalement supprimés des appareils (ordinateurs, téléphone, tablette, disque dur externe), des serveurs et des outils infonuagiques.
- Le processus de destruction des renseignements personnels sera mis en œuvre annuellement en fin d'exercice financier.
- La destruction sera réalisée de manière que les renseignements personnels ne puissent pas être récupérés ou reconstitués.

2.8. Divulgation des renseignements personnels

Tel que le stipule la politique de protection des renseignements personnels, sous réserve des situations pour lesquelles la loi le requiert, les renseignements personnels ne peuvent être divulgués à un tiers qu'après l'obtention du consentement manifeste, libre et éclairé de la personne concernée.

Un tel consentement ne peut être donné que pour une fin spécifique et pour la durée nécessaire à la réalisation de cette fin. Le consentement obtenu sera écrit si la situation le permet. Le « Formulaire d'autorisation de communiquer des renseignements » sera utilisé afin de consigner le consentement de la personne concernée. Ledit formulaire est annexé au présent guide.

Les renseignements personnels peuvent être divulgués sans le consentement de la personne concernée si la vie, la santé ou la sécurité de celle-ci est gravement menacée. La divulgation doit alors être effectuée de la façon la moins préjudiciable pour la personne concernée.

Tel que permis par la loi, l'ARLPH peut divulguer des renseignements confidentiels nécessaires à sa défense ou celle de ses employés contre toute réclamation ou poursuite intentée contre l'organisation ou ses employés, par ou de la part d'un participant, d'un employé, ou de l'une de ses personnes héritières, exécutrices testamentaires, ayants droit ou cessionnaires, y compris toute réclamation émanant de l'assureur d'un participant ou d'un employé.

2.9. Photographies et enregistrements

Tout individu a le choix d'être photographié ou non, ou d'être enregistré (audio/vidéo) ou non. Dans le respect de cet énoncé, l'ARLPH obtiendra l'autorisation de la personne concernée pour toute diffusion, publication, reproduction ou utilisation, et ce, à l'aide du « F*ormulaire de consentement pour la prise de photo ou vidéo* ». Voir ledit formulaire à la fin du présent guide.

Les photographies ou enregistrements qui permettent d'identifier un individu comme employé ou bénévole ne constituent pas un renseignement personnel relatif à cet individu.

3. PROCÉDURE DE DEMANDE D'ACCÈS AUX RENSEIGNEMENTS PERSONNELS ET TRAITEMENT DES PLAINTES

3.1. APERÇU

Puisqu'une personne peut demander à accéder aux renseignements personnels que l'ARLPH détient sur elle, ou pourrait également formuler des plaintes, la présente procédure en dresse les balises pour répondre à ce type de demande.

3.2. OBJECTIF

Le but de cette procédure est de garantir que toutes les demandes d'accès sont traitées de manière confidentielle, rapide et précise, tout en respectant les droits des individus concernés.

3.3. PORTÉE

La portée de cette procédure concerne la personne responsable du traitement des demandes d'accès et du traitement des plaintes, ainsi que les individus souhaitant accéder à leurs renseignements personnels.

3.4. PROCÉDURE DE DEMANDE D'ACCÈS

Soumission de la demande

- 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.
- La demande doit clairement indiquer qu'il s'agit d'une demande d'accès aux renseignements personnels, et fournir des informations suffisantes pour identifier l'individu et les renseignements recherchés.
- Ces informations peuvent inclure le nom, l'adresse ainsi que toute autre information pertinente pour identifier de manière fiable l'individu qui effectue la demande.

Réception de la demande

- Une fois la demande reçue, un accusé de réception est envoyé à l'individu pour confirmer que sa demande a été prise en compte.
- La demande devra être traitée dans les trente (30) jours suivant sa réception.
- Si ce délai ne peut pas être respecté, en informer l'individu et le tenir informé tout au long du processus.

Vérification de l'identité

- Avant de traiter la demande, l'identité de l'individu doit être vérifiée de manière raisonnable. Cela peut être fait en demandant des informations supplémentaires ou en vérifiant l'identité de l'individu en personne.

- Si l'identité ne peut pas être vérifiée de manière satisfaisante, l'organisation se réserve le droit de refuser de divulguer les renseignements personnels demandés.

Réponse aux demandes incomplètes ou excessives

- Si une demande d'accès aux renseignements personnels est incomplète ou excessive, le responsable de la protection des renseignements personnels communique avec l'individu pour demander des informations supplémentaires ou des clarifications.
- Avant de communiquer tous les renseignements personnels en possession de l'organisation, il est possible de confirmer avec l'individu concerné s'il nécessite effectivement ces informations spécifiques ou si une énumération des catégories de renseignements personnels détenus serait adéquate.
- L'ARLPH se réserve le droit de refuser une demande si elle est manifestement abusive, excessive ou non justifiée.

Traitement de la demande

- Une fois l'identité vérifiée, le responsable consulte les dossiers pertinents pour recueillir les renseignements personnels demandés, en veillant à respecter les restrictions légales éventuelles.

Examen des renseignements

- Avant de communiquer les renseignements personnels à l'individu, le responsable examine attentivement les informations pour s'assurer qu'elles ne contiennent pas de renseignements tiers confidentiels ou susceptibles de porter atteinte à d'autres droits.
- Si des renseignements de tiers sont présents, le responsable évalue s'ils peuvent être dissociés ou s'ils doivent être exclus de la divulgation.

Communication des renseignements

- Une fois les vérifications terminées, les renseignements personnels sont communiqués à l'individu dans un délai raisonnable, conformément aux exigences légales en vigueur.
- Les renseignements personnels peuvent être communiqués à l'individu par voie électronique, par courrier postal sécurisé ou en personne, selon les préférences de l'individu et les mesures de sécurité appropriées.

Suivi et documentation

- Toutes les étapes du processus de traitement de la demande d'accès aux renseignements personnels doivent être consignées de manière précise et complète à l'aide du « *registre de suivi des demandes d'accès* » en annexe du présent guide de gestion.

Protection de la confidentialité

- Tout le personnel impliqué dans le traitement des demandes d'accès aux renseignements personnels doit respecter la confidentialité et la protection des données.

Gestion des plaintes et des recours

- Les plaintes doivent être traitées conformément à l'article intitulé « *mécanisme d'application* » du « *Code d'éthique et de déontologie* ».

- Si un individu est insatisfait de la réponse à sa demande d'accès aux renseignements personnels, il doit être informé des procédures de réclamation et des recours disponibles devant la Commission d’accès à l’information.

4. PROCÉDURE DE DEMANDE DE DÉSINDEXATION ET DE SUPPRESSION DES RENSEIGNEMENTS PERSONNELS

4.1. APERÇU

Cette procédure vise à répondre aux craintes et aux préoccupations de confidentialité et de protection des renseignements personnels de nos membres, employés, etc.

4.2. OBJECTIF

Le but de cette procédure est de fournir un mécanisme structuré pour gérer les demandes de désindexation et de suppression des renseignements personnels émanant des membres, employés, etc.

4.3. PORTÉE

Cette procédure s'applique aux employés chargés 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 utilisé par nos membres.

4.4. DÉFINITIONS

Suppression des renseignements personnels : action d'effacer complètement et définitivement 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.

4.5. PROCÉDURE

Réception des demandes

- Les demandes de désindexation et de suppression des renseignements personnels doivent être reçues par la personne responsable de la protection des renseignements personnels.
- Les individus peuvent soumettre leurs demandes par courriel ou par courrier postal.

Vérification de l'identité

- Avant de traiter la demande, l'identité de l'individu doit être vérifiée de manière raisonnable. Cela peut être fait en demandant des informations supplémentaires ou en vérifiant l'identité de l'individu en personne.
- Si l'identité ne peut pas être vérifiée de manière satisfaisante, l'ARLPH peut refuser de donner suite à la demande.

Évaluation des demandes

- Le responsable doit examiner attentivement les demandes et les renseignements personnels concernés pour déterminer leur admissibilité à la désindexation ou à la suppression.
- Les demandes doivent être traitées de manière confidentielle et dans le respect des délais prévus, soit dans les trente (30) jours suivant sa réception.

Raisons d'un refus

- Il existe aussi des raisons parfaitement valables pour lesquelles l'ARLPH pourrait refuser de supprimer ou de désindexer des renseignements personnels :
    - Pour continuer à fournir des biens et des services ;
    - Pour des raisons d'exigence du droit du travail ;
    - Pour des raisons juridiques en cas de litige.

Désindexation ou suppression des renseignements personnels

- Le responsable doit prendre les mesures nécessaires pour désindexer ou supprimer les renseignements personnels conformément aux demandes admissibles.

Communication du suivi

- Le responsable est chargé de communiquer avec les demandeurs tout au long du processus, en fournissant des confirmations d'accusé de réception et des mises à jour régulières sur l'état d'avancement de leur demande.
- Tout retard ou problème rencontré lors du traitement des demandes doit être communiqué aux demandeurs avec des explications claires.

Suivi et documentation

- Toutes les étapes du processus de demande de désindexation et de suppression des renseignements personnels doivent être consignées de manière précise et complète dans le « *registre de suivi des demandes de désindexation ou de suppression des renseignements personnels* » en annexe du présent guide de gestion.

5. PROCÉDURE DE GESTION DES INCIDENTS DE SÉCURITÉ ET VIOLATIONS DES RENSEIGNEMENTS PERSONNELS

5.1. APERÇU

Un plan d'intervention est essentiel pour gérer des cyberincidents de manière efficace. Dans ces moments de crise, on ne sait pas toujours où mettre de la tête. Un plan d'intervention vient réduire le stress d'oublier des aspects importants.

5.2. OBJECTIF

Le but de cette procédure est de s'assurer que l'organisation est prête à intervenir en cas de cyberincident de manière à pouvoir reprendre rapidement ses activités.

5.3. PORTÉE

La portée de cette procédure inclut tous les réseaux, systèmes et données, ainsi que les parties prenantes (p. ex. : membres, partenaires, employés, sous-traitants, fournisseurs tiers) qui accèdent à ces réseaux, systèmes et données.

5.4. RECONNAÎTRE UN INCIDENT DE CONFIDENTIALITÉ

Lorsque toute personne ayant un lien avec l'organisation constate un incident de confidentialité, elle doit :

- Informer avec diligence la personne responsable de la protection des renseignements personnels afin que cette dernière documente l'incident de confidentialité dans le Registre,
- prendre les mesures raisonnables pour diminuer les risques qu'un préjudice soit causé,
- compléter le « Formulaire de signalement d'un incident de confidentialité » joint au présent guide et l'acheminer ensuite à la personne responsable.

5.5. ATTEINTE À LA PROTECTION DES DONNÉES – INTERVENTION SPÉCIFIQUE

La personne responsable juge si l'incident présente un « risque sérieux de préjudice » à l'aide de la « Grille d'analyse – Incidents de confidentialité » joint au présent guide de gestion.

S'il est 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 :

- Compléter le registre d'incidents de confidentialité pour documenter l'incident. Voir une représentation du registre joint au présent guide de gestion. Le document est en format Excel dans le dossier électronique à cet effet.
- Examiner l'atteinte à la protection des données pour déterminer si des **renseignements personnels** ont été perdus en raison d'un accès ou utilisation non autorisé, 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 à l'aide du formulaire « *Avis à la personne concernée par un incident de confidentialité causant un préjudice sérieux »* joint au présent guide de gestion.

- Les renseignements ainsi que les mesures à prendre afin de diminuer le risque qu'un préjudice sérieux soit causé aux personnes concernées sont versés au « Registre d'incident de confidentialité »
- Le registre conserve les informations sur un incident de confidentialité pour une période minimale de cinq ans à partir de la date ou de la période de prise de connaissance de l'incident par l'organisme.

5.6. RANÇONGICIEL – INTERVENTION SPÉCIFIQUE

S'il a été confirmé qu'un incident de sécurité de rançongiciel s'est produit, il faudra effectuer les étapes suivantes :

- Déconnecter immédiatement du réseau les appareils visés par un rançongiciel.
- Ne RIEN EFFACER sur de vos appareils (ordinateurs, serveurs, etc.).
- Examiner le rançongiciel et déterminer comment il a infecté l'appareil. Cela vous aidera à comprendre comment l'éliminer.
- Communiquer avec les autorités locales pour signaler l'incident et coopérer à l'enquête.
- Une fois le rançongiciel supprimé, une analyse complète du système doit être effectuée à l'aide d'un antivirus, d'un antimaliciel et de tout autre logiciel de sécurité le plus récent disponible afin de confirmer qu'il a été supprimé de l'appareil.
- Si le rançongiciel ne peut pas être supprimé de l'appareil (souvent le cas avec les programmes malveillants furtifs), l'appareil doit être réinitialisé au moyen des supports ou des images d'installation d'origine.
    - Avant de procéder à la réinitialisation à partir de supports/images de sauvegarde, vérifier qu'ils ne sont pas infectés par des maliciels.
- Si les données sont critiques et doivent être restaurées, mais ne peuvent être récupérées à partir de sauvegardes non affectées, rechercher les outils de déchiffrement disponibles sur **nomoreransom.org.**
- La politique est de ne pas payer la rançon, sous réserve des enjeux en cause. Il est également fortement recommandé de faire appel aux services d'un chef de projet expert en cyberattaques (breach coach).
- Protéger les systèmes pour éviter toute nouvelle infection en mettant en œuvre des correctifs ou des rustines pour empêcher toute nouvelle attaque.

5.7. PIRATAGE DE COMPTE – INTERVENTION SPÉCIFIQUE

S'il a été confirmé qu'un piratage de compte s'est produit, il faudra effectuer les étapes suivantes :

- Aviser nos clients et fournisseurs qu'ils pourraient recevoir des courriels frauduleux de notre part, et spécifier de ne pas répondre ou cliquer sur les liens de ces courriels.

- Vérifier si on a encore accès au compte en ligne.
    - Sinon, communiquer avec le support de la plateforme pour tenter de récupérer l'accès.
- Changer le mot de passe utilisé pour se connecter à la plateforme.
- Si le mot de passe est réutilisé ailleurs, changer également tous ces mots de passe.
- Activer le double facteur d'authentification pour la plateforme.
- Supprimer les connexions et les appareils non légitimes de l'historique de connexion.

5.8. Perte ou vol d'un appareil – Intervention spécifique

S'il a été confirmé qu'une perte d'équipement s'est produite, il faudra effectuer les étapes suivantes :

- Le vol ou la perte d'un bien, tel qu'un ordinateur, un ordinateur portatif ou un appareil mobile, doit être signalé immédiatement aux autorités policières locales. Cela inclut les pertes/vols en dehors des heures d'ouverture normale et pendant les week-ends.
- Si l'appareil perdu ou volé contenait des données sensibles et qu'il n'est pas crypté, effectuer une analyse de sensibilité, du type et du volume des données volées, y compris les numéros de cartes de paiement potentiellement concernés.
- Dans la mesure du possible, verrouiller/désactiver les appareils mobiles perdus ou volés (p. ex. : téléphones intelligents, tablettes, ordinateurs portatifs, etc.) et procéder à un effacement des données à distance.

6. PROCÉDURE DE GESTION DU ROULEMENT DU PERSONNEL

6.1. APERÇU

Le départ d'un membre du personnel peut entraîner des dommages intentionnels, accidentels ou une perte de données. Avec une liste de rôles et de leurs accès ainsi que d'une politique à appliquer avant un départ, vous pourrez éviter la plupart de ces pertes.

6.2. OBJECTIF

Le but de cette politique est d'établir une liste de contrôle au sein de l'organisation pour encadrer le départ d'un membre de l'équipe.

6.3. PORTÉE

La portée de cette procédure inclut tous les individus qui quittent l'organisation et qui possédaient des accès physiques aux appareils et systèmes de l'organisation ou aux comptes et différentes plateformes de l'organisation.

6.4. PROCÉDURE

Entrevue de départ ou mise à pied

- Éteindre les ordinateurs et appareils professionnels de l'employé.
- Désactiver l'accès de l'employé à tous les systèmes.
- Supprimer les données professionnelles des appareils appartenant aux employés :
- S'assurer que l'employé retourne tout équipement appartenant à l'organisation : ordinateurs portables, tablettes, clés USB, etc.
- Compiler une liste de tous les emplacements où l'employé a stocké des données professionnelles, y compris les plateformes de stockage infonuagiques.

Téléphone

- Changer le mot de passe de la messagerie vocale.

Accès aux courriels

- Idéalement, ne jamais supprimer le compte courriel d'un employé. La bonne pratique serait de créer une boîte courriel partagée et de bloquer les accès comme mentionné plus bas.
- Modifier le mot de passe du compte dans le système de courriels de l'organisation. Passer en revue la section ci-dessous « Accès au réseau et au Cloud » avant de réactiver le compte.
- Si l'employé a utilisé un téléphone mobile personnel ou une tablette pour accéder à sa messagerie professionnelle, effacer ou supprimer le compte de messagerie si ce n'est déjà fait.
- Créer un message d'absence pour le compte de messagerie conformément aux directives de communication de votre organisation.
- Supprimer l'employé des listes de diffusion de courriels internes.

- Contacter les fournisseurs avec lesquels l'employé a travaillé pour les informer du départ et leur fournir un nouveau contact.
- Donner les accès à quelqu'un pour surveiller le courriel de l'employé. Déterminer combien de temps la boîte de courriels restera disponible — 30 jours — après quoi le compte sera supprimé. S'assurer de faire un suivi après la période établie.

Accès au réseau

- Changer le mot de passe des dossiers dont l'accès est partagé.

Matériel

- Récupérer tous les biens de l'organisation auprès de l'employé – ordinateur portable, téléphone mobile, clé de sécurité, imprimante domestique, logiciels, etc.
- Dans le cas où des appareils personnels sont utilisés dans le cadre du travail, s'assurer que le transfert des données soit effectué sur les outils internes avant le départ.
- Exiger que l'employé signe le formulaire « Attestation - Remise des biens et des données » confirmant que tous les biens ont été retournés à l'organisation. Ledit formulaire se retrouve en annexe du présent guide de gestion.

Formulaire de consentement pour la prise de photo et/ou vidéo

J'autorise l'Association régionale de loisirs pour personnes handicapées du Saguenay–Lac-Saint-Jean à diffuser, publier, reproduire, utiliser de façon illimitée ma voix et l'image prise de moi (photos et vidéos) dans le cadre des activités de l'ARLPH, et ce sans compensation aucune, sans restriction de durée, de format et de support pour des fins :

- de production
- de diffusion
- de publications
- d'impressions
- de promotion sur leur site web et leurs réseaux sociaux à des fins non commerciales.

Nous dégageons l'Association régionale de loisirs pour personnes handicapées du Saguenay–Lac-Saint-Jean de toute responsabilité, étant conscient(e)s qu'elle n'est pas responsable d'une utilisation non conforme de ma voix et de mon image (photos ou vidéos) par des tiers.

J'ai lu le présent formulaire de consentement, j'en ai compris les modalités et je signe de façon volontaire.

Signature du participant :

Nom : _____Date : _____

Signature : _____

Signature du parent ou du tuteur légal, s'il y a lieu :

Nom : _____ Date : _____

Signature : _____

ARLPH SAGUENAY LAC-SAINT-JEAN

Registre de suivi des demandes d'accès

Date de réception de la demande	*Date de l'accusé de réception*	*Date de la vérification de l'identité*	*Moyen de vérification de l'identité*	*Décision – demande acceptée ou refusée*	*Date de la communication des renseignements (si applicable*

ARLPH SAGUENAY LAC-SAINT-JEAN

Registre de suivi des demandes de désindexation ou de suppression des renseignements personnels

Date de réception de la demande	***Détail de la demande***	***Date de la vérification de l'identité***	***Moyen de vérification de l'identité***	***Mesures prises***	***Dates des mesures prises***	***Résultats des actions effectuées***

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

Je déclare par la présente que je consens à la collecte et à l'utilisation des renseignements personnels de _____ (prénom, nom) _____ (DDN) dans le cadre des services ou des activités de l'Association régionale de loisirs pour personnes handicapées du Saguenay–Lac-Saint-Jean (ARLPH 02).

Description des renseignements personnels qui seront collectés et conservés :

_____

_____

_____

J'autorise l'ARLPH02 à recueillir les renseignements mentionnés auprès de :

_____

_____

Signature du participant :

Nom : _____Date : _____

Signature : _____

Signature du parent ou du tuteur légal, s'il y a lieu :

Nom : _____ Date : _____

Signature : _____

ARLPH
SAGUENAY
LAC-SAINT-JEAN

Formulaire d'autorisation de communiquer des renseignements

Je soussigné(e), _____ (prénom, nom) en ma qualité de _____ (usager ou personne autorisée) autorise l'Association régionale de loisirs pour personnes handicapées du Saguenay–Lac-Saint-Jean à faire parvenir à _____ les renseignements suivants :

- _____
- _____
- _____
- _____

Cette autorisation est valable pour une période de _____jours à compter de la date de la signature de ce document.

Signature de l'usager ou de la personne autorisée :

Nom : _____Date : _____

Signature : _____

Témoin à la signature :

Nom : _____ Date : _____

Signature : _____

Registre d'incidents de confidentialité

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
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 activé

Renseignements personnels (RP) : Tout renseignement qui concerne une personne physique et qui permet, **directement ou indirectement,** de l'identifier.

Catégories de renseignements personnels

Renseignements d'identification : Adresse, numéro de téléphone, sexe, âge, numéro d'assurance sociale/maladie, identifiant numérique, permis de conduire, code d'utilisateur, mot de passe, etc.

Renseignements démographiques : Date de naissance, origines ethniques, orientation sexuelle, identité de genre, religion, etc.

Renseignements de santé : Dossier médical, diagnostic, consultation d'un professionnel de la santé, plan d'intervention, médicament, ordonnance, renseignements sur la cause du décès, etc.

Renseignements financiers : Revenu d'une personne, renseignements relatifs à l'impôt, numéro de compte bancaire, biens possédés, numéros de carte de crédit, etc.

Renseignements relatifs au travail : Dossier disciplinaire, motifs d'absence, date de vacances, salaire, évaluation du rendement, heures d'entrée et de sortie liées au lieu de travail, etc.

Renseignements scolaires et relatifs à la formation : Inscription à des cours, choix de cours, résultats scolaires, curriculum vitae, etc.

Renseignements relatifs à la situation sociale ou familiale : Documents qui attestent l'état civil, le fait qu'une personne ait ou non des enfants ou qu'elle reçoive des prestations d'aide sociale ou de chômage, etc.

Autres : Antécédents judiciaires, dossier employé, etc.

Source : Gouvernement du Québec : https://www.quebec.ca/gouvernement/travailler-gouvernement/travailler-fonction-publique/services-employes-etat/conformite/protection-des-renseignements-personnels/definitions-concepts/concepts

Formulaire de signalement d'un incident de confidentialité

Je soussigné(e), _____ (prénom, nom) en ma qualité de _____ (poste occupé ou relation avec l'ARLPH) déclare avoir constaté un incident qui pourrait porter atteinte à des renseignements personnels détenus par l'Association régionale de loisirs pour personnes handicapées du Saguenay–Lac-Saint-Jean.

Renseignements en lien avec l'incident :

Date de l'évènement (si connu) : _____

Date du constat de l'incident : _____

Circonstance de l'incident : _____
_____

_____

Catégorie de renseignements personnels concernés : _____

_____

_____

_____

_____

Signatures :

_____ Date : _____
Signature de la personne qui déclare le risque d'un incident :

Réception du signalement

Nom : _____ Date : _____

Signature : _____

Avis à la personne concernée par un incident de confidentialité causant un préjudice sérieux

Dans le respect de ses obligations découlant de la *Loi sur la protection des renseignements personnels* (Loi 25), l'Association régionale de loisirs pour personnes handicapées du Saguenay–Lac-Saint-Jean souhaite vous informer de la survenance d'un incident de confidentialité qui concerne vos renseignements personnels. Les renseignements personnels visés dans cet incident sont _____

_____

_____

_____

En effet, voici les circonstances de l'incident : _____

_____

Cet incident est survenu le _____

Soyez assuré(e) que l'Association régionale de loisirs pour personnes handicapées du Saguenay–Lac-Saint-Jean met actuellement en œuvre des mesures afin de diminuer les risques qu'un préjudice vous soit causé. À cet égard, des mesures ont été mises en place à la suite de l'incident :

_____

_____

_____

Pour toute question ou précision complémentaire en lien avec cet incident en particulier, nous vous invitons à communiquer avec madame Manon Blackburn, directrice à l'Association régionale de loisirs pour personnes handicapées du Saguenay–Lac-Saint-Jean au 418 545-4132.

ARLPH SAGUENAY LAC-SAINT-JEAN

Grille d'analyse – Incidents de confidentialité

Notions importantes

Renseignement personnel (RP) : Tout renseignement qui concerne une personne physique et qui permet, directement ou indirectement, de l'identifier.

Incident de sécurité : Incident affectant la disponibilité, l'intégrité ou de la confidentialité d'un actif informationnel d'un organisme, incluant ou non des renseignements personnels.

Incident de confidentialité ; Incident touchant les renseignements personnels :

- Accès, utilisation ou communication non autorisés
- Perte d'un renseignement personnel
- Toute autre atteinte à la protection d'un renseignement personnel

Renseignements sensibles

Renseignement qui, de par leur nature notamment médicale, biométrique ou autrement intime, ou en raison du contexte de leur utilisation ou communication, suscite un haut degré d'atteinte raisonnable en matière de vie privée.

Ex : documents financiers, dossiers médicaux, biométrique, les renseignements personnels que l'on communique de manière courante ne sont généralement pas considérés comme sensibles (nom, adresse), sauf si le contexte en fait des renseignements sensibles : noms, adresses associées à des périodiques spécialisés ou à des activités qui les identifient.

1. Date de l'évènement : _____

2. Type d'incident/Cause de l'incident

☐ Accès non autorisé

☐ Utilisation non autorisée

☐ Communication non autorisée

☐ Perte ou autre atteinte à la protection des renseignements personnels

3. Des renseignements personnels sont-ils visés ?

☐ Oui. Il s'agit d'un incident de confidentialité. Compléter les questions subséquentes pour évaluer les risques de préjudice.

☐ Non. Il s'agit d'un incident de sécurité. Cependant, vous n'avez pas de déclaration à faire à la CAI. Inscrire l'incident au registre et continuer l'analyse pour évaluer les conséquences appréhendées et les mesures à prendre.

4. Quels renseignements sont visés :

☐ Renseignements d'identification : Adresse, numéro de téléphone, sexe, âge, numéro d'assurance sociale/maladie, identifiant numérique, permis de conduire, code d'utilisateur, mot de passe, etc.

☐ Renseignements démographiques : Date de naissance, origines ethniques, orientation sexuelle, identité de genre, religion, niveau d'instruction, etc.

☐ Renseignements de santé : Dossier médical, diagnostic, consultation d'un professionnel de la santé, plan d'intervention, médicament, ordonnance, renseignements sur la cause du décès, etc.

☐ Renseignements financiers : Revenu d'une personne, renseignements relatifs à l'impôt, numéro de compte bancaire, biens possédés, numéros de carte de crédit, etc.

☐ Renseignements relatifs au travail : Dossier disciplinaire, motifs d'absence, date de vacances, salaire, évaluation du rendement, heures d'entrée et de sortie liées au lieu de travail, etc.

☐ Renseignements scolaires et relatifs à la formation : Inscription à des cours, choix de cours, résultats scolaires, diplômes, curriculum vitae, etc.

☐ Renseignements relatifs à la situation sociale ou familiale : Documents qui attestent l'état civil, le fait qu'une personne ait ou non des enfants ou qu'elle reçoive des prestations d'aide sociale ou de chômage, etc.

☐ Autres, précisez : _____
(Antécédents judiciaires, dossier employé, etc.)

5. Les renseignements visés étaient-ils chiffrés/protégés par un mot de passe ?
☐ Oui, passez à la question 8
☐ Non, continuez l'analyse

6. Ont-ils été récupérés ou détruits ?
☐ Oui, passez à la question 8
☐ Non, continuez l'analyse

7. Combien de personnes sont visées ? _____

8. Des conséquences peuvent-elles néanmoins être appréhendées ?
☐ Oui, continuez l'analyse
☐ Non, vous n'avez pas de déclaration à faire à la CAI, mais vous devez inscrire l'incident au registre.

9. Quelles sont les conséquences appréhendées de l'utilisation du renseignement personnel :
☐ Humiliation, atteinte à la réputation, à la vie privée
☐ Répercussion sur la santé physique ou psychologique
☐ Impact sur les relations professionnelles ou d'affaires
☐ Perte d'emploi ou d'occasion d'affaires
☐ Perte financière
☐ Fraude financière/Atteinte au dossier de crédit
☐ Dommage aux biens ou à leur perte
☐ Vol d'identité

10. Quelles sont les probabilités de l'utilisation du renseignement personnel à des fins préjudiciables :
☐ Faible
☐ Moyenne
☐ Élevée

Qu'est-il est arrivé et quels sont les risques qu'une personne subisse un préjudice en raison de l'atteinte ?

Qui a eu accès aux renseignements personnels ou aurait pu y avoir accès ?

Combien de temps les renseignements personnels ont-ils été exposés ?

A-t-on constaté un mauvais usage des renseignements ?

L'intention malveillante a-t-elle été démontrée (vol, piratage) ?

Les renseignements ont-ils été exposés à des entités ou à des personnes susceptibles de les utiliser pour causer un préjudice ou qui représentent un risque pour la réputation de la ou des personnes touchées ?

11. En fonction de cette évaluation (niveau de préjudice, du type de renseignements personnels visés, de la probabilité que les conséquences appréhendées se réalisent), l'incident de confidentialité doit (plus d'un choix peut s'appliquer) * :

☐ Être inscrit au registre des incidents de confidentialité
☐ Être déclaré avec diligence à la CAI (formulaire)
☐ Être déclaré aux personnes concernées

*Si l'analyse fait ressortir un risque de préjudice sérieux, l'organisation doit aviser la CAI. Dans le cas contraire, elle doit tout de même poursuivre ses travaux pour réduire les risques et éviter qu'un incident de même nature se produise à nouveau.

Signature de la personne ayant fait l'évaluation :

_____

Signature du responsable de la protection des RP :

_____ _____

Source : CDC Maria-Chapdelaine, CY-CLIC et Fédération des enseignements privés : chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.feep.qc.ca/wp-content/uploads/2022/09/Grille_evaluation_incident_confidentialite.pdf

Attestation – Remise des biens et des données

Je soussigné(e), _____ atteste avoir remis à l'Association régionale de loisirs pour personnes handicapées du Saguenay-Lac-Saint-Jean, l'ensemble des biens et des données lui appartenant.

Cela inclut les données pouvant se trouver sur mes appareils personnels.

J'atteste également n'avoir fait une copie de ces données.

_____ _____

Signature de l'employé(e) Date