Politique de gouvernance sur la protection des renseignements personnels

TABLE DES MATIERES

PRÉAMBULE

La Politique de gouvernance sur la protection des renseignements personnels (ci-après « la Politique ») est adoptée en application de la *Loi sur la protection des renseignements personnels dans le secteur privé*, c. P-39.1 (ci-après « *Loi sur le privé* »).

L'Antre-Jeunes est une personne morale à but non lucratif qui traite des renseignements personnels dans le cadre de ses activités. Il est donc assujetti à la *Loi sur le privé*.

Dans le cadre de ses activités, l'Antre-Jeunes doit collecter, utiliser et conserver des renseignements personnels.

Cette Politique s'applique à l'Antre-Jeunes, ce qui inclut notamment les membres de son personnel, aux membres du conseil d'administration, aux stagiaires et bénévoles, le cas échéant, ainsi qu'à toute personne qui, autrement, fournit des services pour le compte de l'Antre-Jeunes.

Elle s'applique pour tous les renseignements personnels collectés, utilisés et conservés par l'Antre-Jeunes, et ce, peu importe leur forme. La Politique vise les renseignements personnels contenus dans tous les types de documents physiques ou numériques, au sens large, que leur forme soit écrite, graphique, sonore, visuelle, informatisée ou autre. Un renseignement personnel est défini comme étant tout renseignement qui concerne une personne physique et qui permet, directement ou indirectement, de l'identifier.

Elle s'applique également à l'égard du site internet de l'Antre-Jeunes, le cas échéant.

Les ANNEXES font partie intégrante de la Politique.

1. OBJECTIFS

La présente Politique décrit les normes de collecte, d'utilisation, de communication et de conservation des renseignements personnels afin d'assurer la protection de ces renseignements. Elle explique également les rôles et les responsabilités des membres du personnel de l'Antre-Jeunes tout au long du cycle de vie de ces renseignements et un processus de traitement des plaintes relatives à la protection de ceux-ci.

2. RENSEIGNEMENTS PERSONNELS

Dans le cadre de ses activités, l'Antre-Jeunes peut recueillir et traiter différents types de renseignements personnels, y compris :

- des renseignements d'identité, comme un nom ou un prénom, âge, date de naissance;
- des coordonnées de contact, une adresse, une adresse électronique et un numéro de téléphone;

- des renseignements nécessaires lors de l'inscription d'un jeune à l'Antre-Jeunes, notamment la fiche d'inscription ;
- des renseignements nécessaires durant la fréquentation d'un jeune, notamment les notes d'observation ;
- des renseignements relatifs aux membres du personnel, stagiaires ou bénévoles de l'Antre-Jeunes, notamment les dossiers du personnel, les documents relatifs à la vérification des empêchements, etc.;
- tout autre renseignement personnel nécessaire dans le cadre de ses activités.

3. COLLECTE

L'Antre-Jeunes collecte des renseignements personnels notamment auprès des jeunes et des parents qui fréquentent l'Antre-Jeunes, de ses membres, de son personnel, de ses administrateurs et de ses bénévoles.

De façon générale, l'Antre-Jeunes collecte les renseignements personnels directement auprès de la personne concernée et avec son consentement, sauf si une exception est prévue par la loi. Le consentement peut être obtenu de façon implicite dans certaines situations, par exemple, lorsque la personne décide de fournir volontairement ses renseignements personnels dans le cadre volontaire des activités de l'Antre-Jeunes, tels que lors de l'inscription d'un jeune ou lors d'une embauche.

Dans tous les cas, l'Antre-Jeunes ne collecte des renseignements personnels que s'il a une raison valable de le faire. De plus, la collecte ne sera limitée qu'aux renseignements nécessaires dont il a besoin pour remplir l'objectif visé.

À moins d'une exception prévue par la loi, l'Antre-Jeunes demandera le consentement de la personne concernée avant de collecter des renseignements personnels qui la concernent auprès d'un tiers.

Les renseignements personnels concernant une personne mineure de moins de 14 ans ne seront pas recueillis auprès de celle-ci sans le consentement de la personne titulaire de l'autorité parentale ou de la personne tutrice.

Considérant que l'Antre-Jeunes collecte des renseignements personnels par un moyen technologique, il s'est doté d'une Politique de confidentialité disponible à l'annexe 1 (Politique de cookies).

4. UTILISATION

L'Antre-Jeunes s'engage à utiliser les renseignements personnels en sa possession uniquement aux fins pour lesquelles ils ont été recueillis et pour lesquels la loi l'autorise à les utiliser. Il peut toutefois les recueillir, les utiliser ou les divulguer sans le consentement de la personne visée lorsque cela est permis ou exigé par la loi.

Dans certaines circonstances particulières, l'Antre-Jeunes peut recueillir, utiliser ou divulguer des renseignements personnels sans que la personne concernée en soit informée ou qu'elle n'ait donné son consentement. De telles circonstances sont réunies notamment lorsque, pour des raisons juridiques, médicales ou de sécurité, il est impossible ou peu probable d'obtenir

son consentement, lorsque cette utilisation est manifestement au bénéfice de cette personne, lorsque cela est nécessaire pour prévenir ou détecter une fraude ou pour tous autres motifs sérieux.

L'Antre-Jeunes limite l'accès des membres du personnel et du conseil d'administration aux seuls renseignements personnels et connaissances de nature personnelle qui sont nécessaires à l'exercice de leur fonction.

5. COMMUNICATION

En principe, l'Antre-Jeunes ne peut communiquer les renseignements personnels qu'il détient sur une personne sans le consentement de celle-ci.

Toutefois, l'Antre-Jeunes peut communiquer à un tiers des renseignements personnels sans le consentement de la personne concernée lorsque la communication est due à une exigence réglementaire ou légale ou lorsque la *Loi sur le privé* ou toute autre loi le permet.

6. CONSERVATION

Conservation

Dans le cadre de ses activités, l'Antre-Jeunes doit conserver de nombreux documents comportant des renseignements personnels.

Certains documents doivent être conservés pendant une durée prescrite.

- Employés de l'entreprise : 7 ans après la fin d'emploi.
- Membres du C.A. : 7 ans après la fin du mandat.
- Membres : 2 ans après l'adhésion.
- Bénévoles et stagiaires : 2 ans après la fin de l'implication.
- Participants : 2 ans après la fermeture du dossier des jeunes.

Qualité des renseignements personnels

L'Antre-Jeunes s'assure de la qualité des renseignements personnels qu'il détient. En ce sens, les renseignements personnels conservés sont à jour, exacts et complets pour servir aux fins pour lesquelles ils ont été recueillis ou utilisés.

La mise à jour constante des renseignements personnels n'est pas nécessaire, sauf si cela est justifié par les fins pour lesquelles ce renseignement est recueilli. Cependant, si les renseignements doivent servir à une prise de décision, ils doivent être à jour au moment de celle-ci.

Documents physiques et numériques

Selon la nature des renseignements personnels, ceux-ci peuvent être conservés aux bureaux de l'Antre-Jeunes, dans divers systèmes informatiques de l'Antre-Jeunes ou de ses fournisseurs de services ou dans les installations d'entreposage de ses fournisseurs de services.

Mesures de sécurité

La sécurité et la protection des renseignements personnels sont importantes pour l'Antre-Jeunes. L'Antre-Jeunes met en place des mesures de sécurité afin que les renseignements personnels demeurent strictement confidentiels et soient protégés contre la perte ou le vol et contre tout accès, communication, copie, utilisation ou modification non autorisée.

Ces mesures de sécurité peuvent notamment comprendre des mesures organisationnelles telles que la restriction des accès à ce qui est nécessaire ; la sauvegarde et l'archivage des données au moyen d'un système externe, etc.); et mesures technologiques comme l'utilisation de mots de passe et de chiffrement (par exemple, le changement fréquent de mots de passe, activation d'authentification multifacteurs et l'utilisation de pare-feu).

Numérisation des documents

Dans l'éventualité où l'Antre-Jeunes désire détruire les documents originaux à la suite de leur numérisation, il respecte les conditions suivantes :

1. L'information contenue dans les documents numérisés n'a pas été altérée et elle a été maintenue dans son intégralité ;
2. La numérisation ainsi que le support pour conserver les documents numérisés doit assurer la stabilité et la pérennité des documents.

L'Antre-Jeunes choisit un support ou une technologie sur lequel il conserve ses documents qui lui permet de respecter ces conditions.
(voir annexe 2)

7. DESTRUCTION

La destruction des documents d'origine contenant des renseignements personnels ou confidentiels est faite de façon sécuritaire.

L'Antre-Jeunes utilise des techniques de destruction définitive de documents adaptées au niveau de confidentialité du document à détruire.

Il se réfère à l'annexe 3 pour les techniques de destruction définitive de documents.

8. ÉVALUATION DES FACTEURS RELATIFS À LA VIE PRIVÉE

L'Antre-Jeunes doit procéder à une évaluation des facteurs relatifs à la vie privée (ÉFVP) pour tout projet d'acquisition, de développement et de refonte de système d'information ou de prestation électronique de services impliquant des renseignements personnels.

L'évaluation des facteurs relatifs à la vie privée réalisée devra être proportionnée à la sensibilité des renseignements concernés, à la finalité de leur utilisation, à leur quantité, à leur répartition et à leur support.

L'Antre-Jeunes peut s'aider du guide développé par la Commission d'accès à l'information « Guided'accompagnement - Réaliser une évaluation des facteurs relatifs à la vie privée » pour

réaliser l'évaluation des facteurs relatifs à la vie privée, le cas échant.

Se référer à l'ANNEXE 8 pour les détails de la procédure.

9. DROITS INDIVIDUELS

9.1 Demande d'accès ou de rectification

Toute personne peut faire une demande d'accès ou de rectification concernant les renseignements personnels détenus par l'Antre-Jeunes.

La personne concernée doit soumettre une demande écrite à cet effet au responsable de la protection des renseignements personnels de l'Antre-Jeunes (voir section 12 pour coordonnées). Avant de traiter la demande, l'identité de l'individu sera vérifiée de manière raisonnable.

Sous réserve de certaines restrictions légales, les personnes concernées peuvent demander l'accès à leurs renseignements personnels détenus par l'Antre-Jeunes et en demander leur correction dans le cas où ils sont inexacts, incomplets ou équivoques.

Le responsable de la protection des renseignements personnels de l'Antre-Jeunes doit répondre par écrit à ces demandes dans les 30 jours de la date de réception.

Pour la procédure de droit d'accès référer à l'annexe 5.

9.2 Droit à l'oubli ou droit à la désindexation

L'Antre-Jeunes s'engage à répondre à une demande à l'oubli dans les 30 jours suivant la date de réception. À ce moment, l'organisme applique les règles de conservation des documents (section 6) dont les principales règles sont les respects des exigences gouvernementales. Si toutes les exigences sont respectées, il y a alors destruction des données tel que mentionné à la section 7.

À l'Antre-Jeunes, il n'y a pas d'indexation publique ou de visibilité en ligne concernant des données. Une politique de désindexation sera mise en place advenant un changement à cet effet.

Pour la procédure de droit de l'oublie référer à l'annexe 6.

9.3 Droit à la portabilité des données

L'Antre-Jeunes s'engage à remettre les documents et les données aux personnes dans un format utilisé couramment, soit sous format PDF, Word ou Excel en fonction du logiciel où les données ont été fournies initialement. De façon générale, les documents générés par l'Antre-Jeunes sont sous format PDF. * moyen approuvé par la CAI en sept 2024.

Les données et les documents seront remis aux clients par l'entremise d'un portail sécurisé.

La présente obligation du droit à la portabilité des données s'applique aux données sensibles tel que défini dans la Loi sur la protection des renseignements personnels dans le secteur privé,

RLRQ c. P-39.1.

Pour la procédure de demande de portabilité, se référer à l'annexe 6 (procédure de demande d'accès).

10. INCIDENTS DE CONFIDENTIALITÉ

Les incidents de confidentialité

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

L'Antre-Jeunes, s'il a des motifs de croire que s'est produit un incident de confidentialité impliquant un renseignement personnel qu'il détient prend les mesures raisonnables pour diminuer les risques qu'un préjudice soit causé et éviter que de nouveaux incidents de même nature ne se produisent.

En cas d'incident de confidentialité, l'Antre-Jeunes procède à l'évaluation du préjudice. Cette évaluation tient compte notamment des éléments suivants : la sensibilité des renseignements personnels concernés ; les utilisations malveillantes possibles des renseignements et les conséquences appréhendées de l'utilisation des renseignements et la probabilité qu'ils soient utilisés à des fins préjudiciables.

Quand l'incident présente le risque qu'un préjudice sérieux soit causé aux personnes dont les renseignements sont concernés, l'Antre-Jeunes avise par écrit :

- La Commission d'accès à l'information via le formulaire d'avis ;
- La ou les personnes concernées. L'avis doit permettre de la renseigner adéquatement sur la portée et les conséquences de l'incident.
    - Cet avis doit contenir :
        - Une description des renseignements personnels visés par l'incident. Si cette information n'est pas connue, l'organisation doit communiquer la raison justifiant l'impossibilité de fournir cette description.
        - Une brève description des circonstances de l'incident ;
        - La date ou la période où l'incident a eu lieu, ou une approximation de cette période si elle n'est pas connue ;
        - Une brève description des mesures prises ou envisagées pour diminuer les risques qu'un préjudice soit causé à la suite de l'incident ;
        - Les mesures proposées à la personne concernée afin de diminuer le risque qu'un préjudice lui soit causé ou d'atténuer celui-ci;
        - Les coordonnées d'une personne ou d'un service avec qui la personne concernée peut communiquer pour obtenir davantage d'informations au sujet de l'incident.

Registre des incidents de confidentialité

L'Antre-Jeunes tient un registre des incidents de confidentialité.

Le registre collige l'ensemble des incidents de confidentialité impliquant un renseignement personnel :

- ceux ne présentant pas de risque de préjudice sérieux et;
- ceux présentant un risque de préjudice sérieux.

Les renseignements contenus au registre des incidents de confidentialité sont tenus à jour et conservés pendant une période minimale de cinq (5) ans après la date ou la période au cours de laquelle l'Antre-Jeunes a pris connaissance de l'incident.

** Voir « plan d'intervention en cas d'incident de confidentialité » pour les étapes de la procédure.

11. PROCESSUS DE TRAITEMENT DES PLAINTES EN LIEN AVEC LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

Toute personne concernée par l'application de la présente Politique peut porter plainte concernant l'application de la présente Politique ou, plus généralement, concernant la protection de ses renseignements personnels par l'Antre-Jeunes.

La procédure de traitement de plainte relative à la protection des renseignements personnels est prévue à **l'annexe 7.**

12. COORDONNÉES DE LA RESPONSABLE DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

La Responsable de la protection des renseignements personnels de l'Antre-Jeunes peut être contactée par téléphone au 450-436-1547 poste 101 ou par courriel au renseignementspersonnels@antre-jeunes.org

Il est possible de communiquer avec la Responsable de la protection des renseignements personnels de l'Antre-Jeunes pour toute question en lien avec l'application de la présente Politique en matière de protection des renseignements personnels.

13. ENTRÉE EN VIGUEUR DE LA POLITIQUE

La Politique entre en vigueur le 18 juillet 2023.

La Politique a été approuvée par la Responsable de la protection des renseignements personnels.

LES ANNEXES

ANNEXE 1 - POLITIQUE DE CONFIDENTIALITÉ LORS D'UNE COLLECTE DE RENSEIGNEMENTS PERSONNELS PAR UN MOYEN TECHNOLOGIQUE

Le site web de l'Antre-Jeunes utilise des fichiers témoins (*cookies*). Les témoins sont de petits fichiers de données inscrits sur la mémoire de votre ordinateur ou appareil mobile lorsque vous visitez un site Web ou une application. Ils sont utilisés dans le but d'accroître votre expérience d'utilisation grâce à l'enregistrement de certaines données. Il vous est possible d'accepter ou non l'utilisation de ces cookies : dans ce dernier cas, votre expérience utilisateur sur nos site Web pourrait être réduite.

Nous pourrions utiliser les cookies aux fins suivantes :

- Cookies techniques ou fonctionnels : Certains cookies assurent le fonctionnement correct de certaines parties d'un site Web et la prise en compte de vos préférences en tant qu'utilisateur ou utilisatrice. En plaçant des cookies fonctionnels, cela facilite la visite de nos sites Web. Par exemple, vous pourriez ne pas avoir besoin de saisir à plusieurs reprises les mêmes informations lors de la visite de nos sites Web puisque ces informations sont sauvegardées dans un cookie.
- Cookies statistiques : Les cookies statistiques sont parfois utilisés afin d'optimiser l'expérience des internautes sur nos sites Web. Avec ces cookies statistiques, nous pouvons obtenir des informations sur l'utilisation de nos sites Web.
- Cookies de marketing/suivi : Les cookies de marketing/suivi sont des cookies ou toute autre forme de stockage local utilisés pour créer des profils d'utilisateurs et d'utilisatrices afin d'afficher de la publicité ou de suivre la personne sur un de nos sites Web ou sur plusieurs sites Web dans des finalités marketing similaires.

N/A

ANNEXE 2 – PROCÉDURE DE NUMÉRISATION

La personne responsable de la numérisation :

1. Numérise les documents et demeure présente tout au long du processus afin de protéger l'intégrité des données numérisées;

2. Effectue une vérification exhaustive des documents numérisés afin de s'assurer de la quantité, de la qualité et de l'intégrité des documents reproduits. Elle vérifie que :
   - les documents numérisés sont conformes aux documents sources;
   - les données sont lisibles et de bonne qualité (sans perte de détail ou d'information).

3. Vérifie que le nombre de documents ou de pages est exact (si des pages manquent, elle reprend la numérisation au complet);

4. Organise les documents numérisés à partir la structure de sauvegarde ou de stockage de l'organisme ;

5. Détruit le document papier suite à la numérisation.

ANNEXE 3 - TECHNIQUES DE DESTRUCTION DÉFINITIVE DE DOCUMENTS

Techniques de destruction définitive de documents[1]

Support utilisé	Exemples de méthodes de destruction
Papier (original et toutes les copies)	• Déchiqueteuse, de préférence à découpe microparticules.
Médias numériques que l'on souhaite réutiliser ou recycler Ex. disque dur d'ordinateur	• Formatage, réécriture, déchiquetage numérique (logiciel effectuant une suppression sécuritaire et qui écrira de l'information aléatoire à l'endroit où se trouvait le fichier supprimé).
Machines contenant des disques durs Ex. photocopieur, télécopieur, numériseur, imprimante, etc.	• Écrasement des informations sur le disque dur ou disque dur enlevé et détruit lorsque les machines sont remplacées.

[1] Commission d'accès à l'information, Procédure de destruction, en ligne : https://www.cai.gouv.qc.ca/entreprises/procedure-de-destruction/

ANNEXE 4 - REGISTRES DES INCIDENTS DE CONFIDENTIALITÉ

Registre des incidents de confidentialité								
Date ou période de l'incident	**Personnes concernées (informations compromises)**	**Description des circonstances de l'incident**	**Prise de connaissance de l'incident**	**Nombres de personnes concernées par l'incident**	**Description des éléments qui amènent à conclure qu'il existe ou non un risque qu'un préjudice sérieux[2] soit causé aux personnes concernées**	**Date de transmission de l'avis à la Commission d'accès à l'information**	**Date de transmission des avis aux personnes concernées**	**Description des mesures prises afin de diminuer les risques qu'un préjudice soit causé**

[2] L'évaluation du risque de préjudice sérieux tient compte notamment des éléments suivants : la sensibilité des renseignements personnels concernés; les utilisations malveillantes possibles des renseignements et les conséquences appréhendées de l'utilisation des renseignements et la probabilité qu'ils soient utilisés à des fins préjudiciables.

ANNEXE 5 – 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.

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 peut 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 clarifications.
- L'organisation 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 de la protection des renseignements personnels pour traiter les demandes d'accès aux renseignements personnels procède à la collecte des renseignements demandés.
- 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.
- Les détails de la demande, les actions entreprises, les décisions prises et les dates correspondantes doivent être enregistrés dans un 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 ;
    - Méthode de vérification de l'identité ;
    - Décision – demande d'accès acceptée ou refusée ;
    - Date de la communication des renseignements (si applicable).

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

- 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.
- Les plaintes doivent être traitées conformément aux politiques et procédures internes en matière de gestion des plaintes (section suivante).

ANNEXE 6 - PROCÉDURE DU DROIT DE L'OUBLIE

Réception des demandes

- Les demandes de désindexation et de suppression des renseignements personnels doivent être reçues par l'équipe responsable désignée.
- Les clients peuvent soumettre leurs demandes par le biais de canaux spécifiques tels que le formulaire en ligne, l'adresse courriel dédiée ou le numéro de téléphone.

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 peut refuser de donner suite à la demande.

Évaluation des demandes

- L'équipe 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.

Raisons d'un refus

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

Désindexation ou suppression des renseignements personnels

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

Communication du suivi

- L'équipe responsable est chargée 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 demandes de désindexation et de suppression des renseignements personnels, ainsi que les actions entreprises pour y répondre, doivent être consignées dans un système de suivi dédié.
- Les enregistrements doivent inclure les détails des demandes, les mesures prises, les dates et les résultats des actions effectuées.

ANNEXE 7 - PROCÉDURE DE TRAITEMENT DES PLAINTES EN LIEN AVEC LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

Réception des plaintes

- Les plaintes peuvent être déposées par écrit, par téléphone, par courrier électronique ou via tout autre canal de communication officiel. Elles doivent être enregistrées dans un registre centralisé, accessible uniquement au personnel désigné.

- Les employés doivent informer immédiatement le service responsable de la réception des plaintes.

Évaluation préliminaire

- Le responsable désigné examine chaque plainte pour évaluer sa pertinence et sa gravité.

- Les plaintes frivoles, diffamatoires ou sans fondement évident peuvent être rejetées. Toutefois, une justification doit être fournie au plaignant.

Enquête et analyse

- Le responsable chargé de la plainte mène une enquête approfondie en collectant des preuves, en interrogeant les parties concernées et en recueillant tous les documents pertinents.

- Le responsable doit être impartial et avoir l'autorité nécessaire pour résoudre la plainte.

- Le responsable doit maintenir la confidentialité des informations liées à la plainte et veiller à ce que toutes les parties impliquées soient traitées équitablement.

Résolution de la plainte

- Le responsable de la plainte propose des solutions appropriées pour résoudre la plainte dans les meilleurs délais.

- Les solutions peuvent inclure des mesures correctives, des compensations financières ou toute autre action nécessaire pour résoudre la plainte de manière satisfaisante.

Communication avec le plaignant

- Le responsable de la plainte communique régulièrement avec le plaignant pour le tenir informé de l'avancement de l'enquête et de la résolution de la plainte.

- Toutes les communications doivent être professionnelles, empathiques et respectueuses.

Clôture de la plainte

- Une fois la plainte résolue, le responsable de la plainte doit fournir une réponse écrite au plaignant, résumant les mesures prises et les solutions proposées.

- Toutes les informations et documents relatifs à la plainte doivent être conservés dans un dossier confidentiel.

Annexe 8 : Procédure d'une évaluation des facteurs relatifs à la vie privée

Qu'est-Ce Qu'une Évaluation Des Facteurs De Relatifs À La Vie Privée (EFVP) ?
L'EFVP est une **démarche visant à protéger les renseignements personnels et à respecter la vie privée des personnes physiques**. Il s'agit d'une forme d'analyse d'impact5. Elle est évolutive et doit être revue tout au long du projet.
Elle consiste à considérer, avant de commencer un projet et tout au long de sa durée, **tous les facteurs ayant un effet positif ou négatif pour le respect de la vie privée** des personnes concernées.
Ces facteurs sont les suivants :

1. La **conformité** du projet à la **législation applicable** en matière de protection des renseignements personnels et le **respect des principes** l'appuyant;

2. L'identification des **risques** d'atteinte à la vie privée engendrés par le projet et l'évaluation de leurs conséquences;

3. La mise en place de **stratégies** pour éviter ces risques ou les réduire efficacement et leur maintien dans le temps.

Pourquoi réaliser une EFVP ?
En dehors de son caractère obligatoire dans certaines situations prévues par la loi, l'EFVP a pour objectifs de :

- **Protéger les personnes** concernées par un projet, et ce, de la collecte de leurs renseignements personnels à leur destruction;

- **Mettre en place des mesures appropriées** pour respecter vos obligations en matière de protection des renseignements personnels;
- **Éviter les conséquences** que causerait une gestion inadéquate de ces renseignements (incidents de confidentialité, poursuites, atteintes à l'image, etc.).

Quand réaliser une EFVP ?
Vous devez commencer votre EFVP **dès le début de votre projet** :

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

En effet, attendre avant de commencer vous mettrait à risque de devoir apporter des modifications importantes tardivement, avec les coûts et les délais associés. Cependant, il n'est jamais trop tard pour amorcer votre EFVP si vous réalisez qu'elle s'impose.

L'EFVP doit évoluer tout au long du projet, selon les changements que vous y apportez. Si une EFVP a déjà été réalisée dans le passé pour le même projet, vous pouvez donc en faire la mise à jour.

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

I. Développer un nouveau système d'information ou une technique de personnalisation d'un produit ou d'un service ;
II. Chercher une nouvelle clientèle, explorer de nouveaux marchés ;
III. Faire appel à un système d'algorithme ou d'intelligence artificielle ;

IV. Installer un système de vidéosurveillance ;
V. Comparer différentes versions de bases de données ou de fichiers ;
VI. Acquérir ou fusionner des organisations ;
VII. Utiliser des empreintes digitales, la géolocalisation, un système de reconnaissance faciale, des objets connectés, des capteurs pour villes intelligentes, etc.

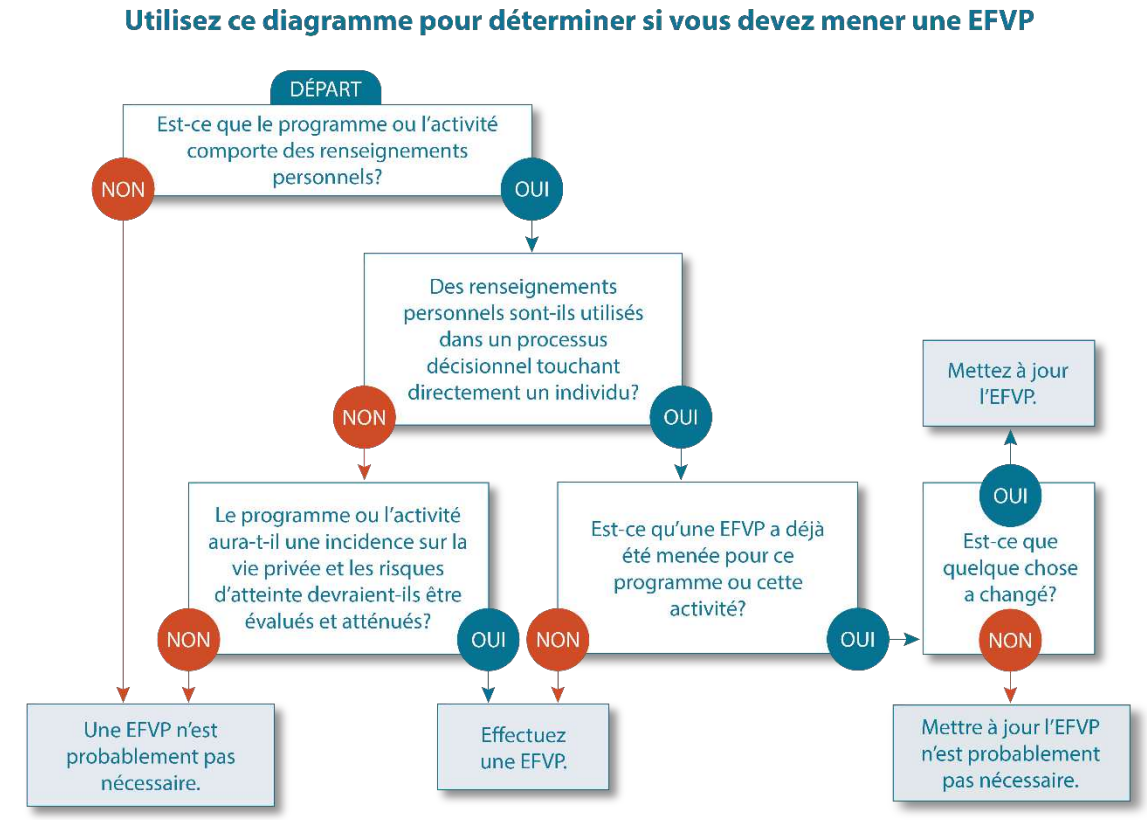
Cinq situations principales vous obligent à réaliser une EFVP :

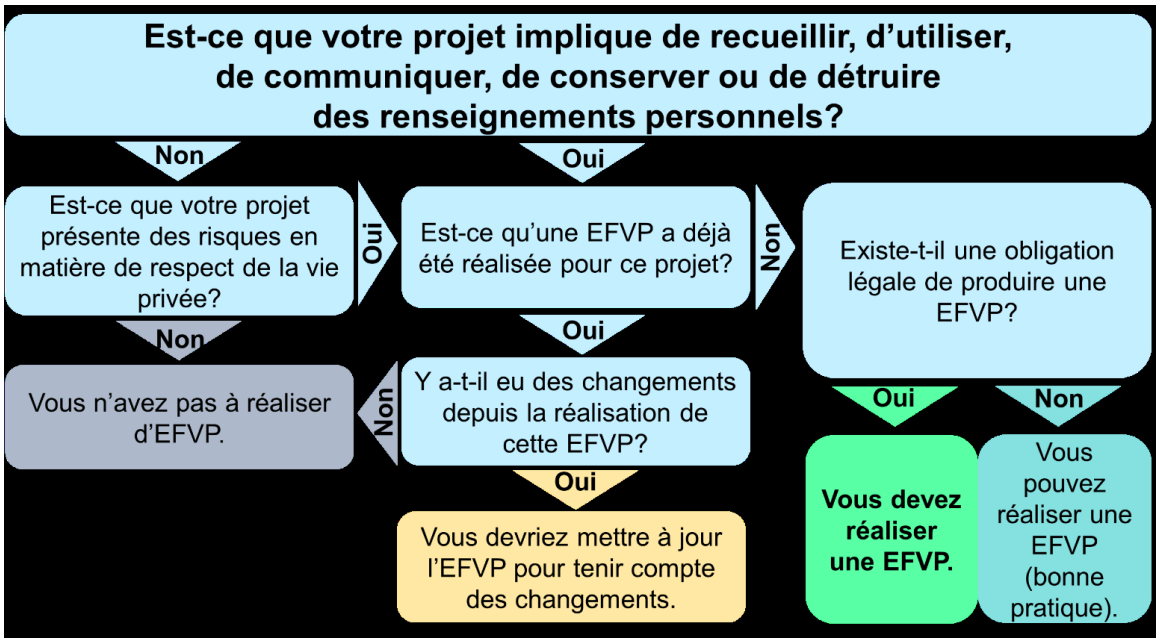
1. Pour un organisme ou une entreprise : Pour communiquer des renseignements personnels sans consentement à un tiers à des fins d'étude, de recherche ou de production de statistiques.
    a. La communication doit être faite dans le cadre d'une entente écrite, transmise à la Commission. Cette entente entre en vigueur dans les 30 jours suivant sa réception.
    b. Consultez la section sur la communication de renseignements personnels sans consentement à des fins de recherche.
2. Pour un organisme ou une entreprise : Dans le cadre d'un projet d'acquisition, de développement et de refonte de système d'information ou de prestation électronique de services impliquant la collecte, l'utilisation, la communication, la conservation ou la destruction de renseignements personnels.
    a. Dès le début du projet, aux fins d'évaluation :
        i. L'organisme public doit consulter son comité sur l'accès à l'information et la protection des renseignements personnels.
        ii. L'entreprise doit consulter son responsable de la protection des renseignements personnels.
3. Pour un organisme ou une entreprise : Avant la communication d'un renseignement personnel à l'extérieur du Québec.
    a. L'organisme public et l'entreprise privée doivent procéder à une EFVP :
        i. Avant de communiquer un renseignement personnel à une entité située à l'extérieur du Québec.
        ii. Avant de confier à une personne ou à un organisme à l'extérieur du Québec la tâche de recueillir, d'utiliser, de communiquer ou de conserver, pour votre compte, un tel renseignement.
        iii. Consultez la section sur la Communication de renseignements personnels à l'extérieur du Québec.
4. Pour un organisme public : Dans le cadre de la collecte d'un renseignement personnel nécessaire à l'exercice des attributions d'un autre organisme public.
    a. Il peut également s'agir de la mise en œuvre d'un programme de l'organisme public avec lequel il collabore pour la prestation de services ou pour la réalisation d'une mission commune.
    b. Par exemple, un organisme peut recueillir un renseignement personnel afin de vérifier l'admissibilité de personnes à un programme qu'il administre.
    c. Les organismes qui collaborent doivent conclure une entente et la transmettre à la Commission. Consultez la section sur les ententes de communication.
5. 5- Pour un organisme public : Pour certaines autres communications d'un renseignement personnel sans le consentement de la personne concernée.
    a. Plus précisément, une EFVP doit aussi être réalisée avant de communiquer un renseignement personnel sans consentement :

i. À un organisme public ou à un organisme d'un autre gouvernement lorsque la communication est manifestement au bénéfice de la personne concernée ;
ii. À un organisme public ou à un organisme d'un autre gouvernement pour l'exercice de ses attributions ou la mise en œuvre d'un programme dont il a la gestion ;
iii. À une personne ou à un organisme lorsque des circonstances exceptionnelles le justifient ;
iv. À une personne ou à un organisme si cette communication est nécessaire dans le cadre de la prestation d'un service à rendre à la personne concernée par un organisme public, notamment aux fins de l'identification de cette personne ;

Êtes-vous obligé de faire une EFVP ?
Faire une EFVP n'est pas obligatoire, sauf pour certains organismes publics. Mais si votre projet implique la collecte, l'utilisation ou la communication de renseignements personnels, une EFVP est fortement recommandée.
Si vous décidez de ne pas réaliser d'EFVP, soyez en mesure d'expliquer et de justifier pourquoi vous ne le faites pas.

Comment déterminer quand une ÉFVP doit être effectuée ?





Procédure pour réaliser une EFVP
La suite de ce guide est structurée selon les étapes de la démarche proposée par la Commission, présentées dans la synthèse suivante :

Rédiger un Rapport D'évaluation
Le rapport est la dernière étape de votre processus de réflexion. Il devrait être simple et accessible : tout lecteur qui n'aurait pas été directement impliqué dans votre projet devrait pouvoir comprendre quel est le projet, comment ce projet est susceptible d'affecter la vie privée et comment vous avez considéré et mesuré les risques identifiés.
Un rapport d'EFVP sert à consolider les résultats de votre évaluation. Il permet d'attester de vos démarches et de votre réflexion dans le cas d'une vérification, d'une inspection ou d'une enquête par une autorité réglementaire. Un résumé de votre rapport peut également être diffusé auprès de vos clients, de vos partenaires, de toute autre entité concernée, ou même au sein de votre organisation. Vous pouvez rendre ce résumé public en le publiant sur votre site Web. Le diffuser permet de :

- Faire preuve de transparence auprès des personnes qui font affaire avec votre organisation ;
- Démontrer que vous avez pris en considération le respect de la vie privée dans l'élaboration et la mise en œuvre de votre projet.

Rédiger un rapport est-il obligatoire ?
Le Rapport n'est pas obligatoire, sauf pour les organismes publics, dans certains cas précis prévus par la Loi sur l'accès. Faire une EFVP est alors obligatoire et requiert la rédaction et la diffusion d'un rapport.

Exemples de projets où une EFVP est exigée :

- Projets gouvernementaux visés par la Loi favorisant la transformation numérique de l'administration publique ;
- Projets d'acquisition, de développement et de refonte d'un système d'information ou de prestation électronique de services qui recueille, utilise, conserve, communique ou détruit des renseignements personnels en vertu du Règlement sur la diffusion de l'information et sur la protection des renseignements personnels **(R.L.R.Q chapitre A-2.1, r.2).**

Que devrait contenir le rapport ?
L'essentiel de votre projet et le cadre dans lequel il s'inscrit

- La description de votre projet;
- Ce qui l'a motivé (contexte) et les objectifs poursuivis;
- Toutes les parties prenantes au projet, en incluant la description de leur rôle et de leurs responsabilités : celles impliquées dans sa mise en oeuvre et celles impliquées par la suite, c'est-à-dire les ressources de votre organisation, vos différents partenaires et votre clientèle;
- Les personnes ou les secteurs de votre organisation qui seront responsables de gérer les risques résiduels;
- Un résumé des consultations, s'il y a lieu;
- Un aperçu de l'inventaire et de la cartographie des renseignements personnels impliqués (catégorie(s) de renseignements impliqués, source(s) des renseignements, support(s), destinataire(s), interactions avec d'autres systèmes, etc.);
- Une évaluation des critères de sensibilité, de finalité, de quantité, de répartition et de support des renseignements personnels et une justification de la profondeur d'analyse (ampleur de l'EFVP);
- Une description des moyens mis en place pour respecter les obligations et les principes de protection des renseignements personnels (y compris sectoriels ou situationnels, au besoin);
- Une liste et une catégorisation des risques identifiés pour les personnes concernées;
- Les stratégies, mécanismes et mesures déployés pour éliminer ou réduire ces risques;
- Les personnes responsables de mettre en oeuvre ces stratégies, mécanismes et mesures;
- Un plan d'action avec un échéancier comprenant une réévaluation périodique des mesures mises en place (**exemple** : un audit).

Le rapport devrait-il être diffusé ?
À titre de bonne pratique de transparence, votre organisation pourrait décider de diffuser une version abrégée du rapport d'EFVP sur son site Web ou par tout autre moyen. Cette démarche peut témoigner d'un souci du respect de la loi et de l'information des personnes concernées.

Les organismes publics, en particulier, peuvent envisager de divulguer proactivement des résumés des EFVP concernant les projets touchant directement les citoyens.

Exemple de Rapport d'évaluation de l'impact sur la vie privée :
La Commission propose également un modèle générique de rapport permettant de rendre compte des résultats d'une EFVP.