

Politique relative à la protection des renseignements personnels

Ministère de l'Environnement,

de la Lutte contre les changements climatiques,

de la Faune et des Parcs

Coordination et rédaction

Cette publication a été réalisée par la Direction principale des renseignements, de l'accès à l'information, de l'éthique et des plaintes du ministère de l'Environnement, de la Lutte contre les changements climatiques, de la Faune et des Parcs (MELCCFP). Elle a été produite par la Direction des communications du MELCCFP.

Renseignements

Téléphone : 418 521-3830

1 800 561-1616 (sans frais)

Formulaire : www.environnement.gouv.qc.ca/formulaires/renseignements.asp

Internet : www.environnement.gouv.qc.ca

Dépôt légal – 2023

Bibliothèque et Archives nationales du Québec

ISBN : 978-2-555-00206-7 (PDF)

Tous droits réservés pour tous les pays.

© Gouvernement du Québec – 2

Table des matières

CHAMP D'APPLICATION	1
CADRE LÉGISLATIF	1
PRINCIPES DIRECTEURS	2
RÈGLES DE GOUVERNANCE	3
1. Collecte	3
2. Utilisation	6
3. Communication	7
4. Conservation	9
5. Demande d'accès ou de rectification	9
6. Destruction ou anonymisation	10
RÔLES ET RESPONSABILITÉS	10
SENSIBILISATION ET FORMATION DU PERSONNEL	16
PLAINTES EN MATIÈRE DE RENSEIGNEMENTS PERSONNELS	17
ENTRÉE EN VIGUEUR ET RÉVISION	17

CHAMP D'APPLICATION

La Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (chapitre A-2.1) (ci-après, la Loi) stipule à l'article 63.3 ce qui suit :

« Un organisme public doit publier sur son site Internet des règles encadrant sa gouvernance à l'égard des renseignements personnels. [...]

Elles peuvent prendre la forme d'une politique, d'une directive ou d'un guide et doivent notamment prévoir les rôles et les responsabilités des membres de son personnel tout au long du cycle de vie de ces renseignements ainsi qu'un processus de traitement des plaintes relatives à la protection de ceux-ci. Elles incluent une description des activités de formation et de sensibilisation que l'organisme offre à son personnel en matière de protection des renseignements personnels. »

La présente politique donne suite à cette obligation législative.

Un renseignement qui **concerne une personne physique et permet de l'identifier directement ou indirectement** constitue un renseignement personnel.

Cette politique s'applique à tout renseignement personnel détenu par le ministère de l'Environnement, de la Lutte contre les changements climatiques, de la Faune et des Parcs (ci-après le Ministère), y compris les renseignements dont la conservation est assurée par un tiers, quel que soit le support sur lequel il est conservé, et ce, de sa collecte à sa destruction.

Elle énonce les principes et les règles de gouvernance qui guident le fonctionnement du Ministère en matière de protection des renseignements personnels qu'il détient. Elle énonce aussi les rôles et les responsabilités des personnes à l'emploi du Ministère en cette matière, tout au long du cycle de vie des renseignements. Elle peut être complétée par des directives ou lignes directrices.

La Politique s'adresse à tout le personnel du Ministère, y compris les étudiants, les stagiaires et les contractuels. Elle s'applique également à toute personne à qui le Ministère confie des renseignements personnels dans le cadre de l'exécution d'un mandat, d'un contrat de service ou d'une entente avec un autre organisme public.

CADRE LÉGISLATIF

La Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (chapitre A-2.1) (ci-après, la Loi) contribue à protéger la vie privée des citoyens par un ensemble de dispositions et règles visant la protection des renseignements personnels au Québec.

D'autres lois contribuent au cadre législatif en matière de protection des renseignements personnels :

- La Charte des droits et libertés de la personne (chapitre C-12), qui stipule à son article 5 : « Toute personne a droit au respect de sa vie privée »;
- Le Code civil du Québec (CCQ-1991), par ses articles 35 à 41 concernant le respect de la réputation et de la vie privée;
- La Loi concernant le cadre juridique des technologies de l'information (C-1.1);

- La Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (G-1.03), par ses dispositions visant la sécurité de l'information et les renseignements personnels;
- La Loi sur les archives (A-21.1), notamment les dispositions relatives à la conservation des documents.

PRINCIPES DIRECTEURS

Responsabilité

Tout organisme public est responsable de la protection des renseignements personnels qu'il détient, que leur conservation soit assurée par ce dernier ou par un tiers.

Le Ministère prend les mesures nécessaires afin de protéger efficacement ces renseignements.

Nécessité

La nécessité de recueillir des renseignements personnels découle directement des attributions du Ministère, c'est-à-dire des lois, règlements, programmes et fonds qu'il administre ou des services qu'il dispense, en vertu de l'application de lois du Québec.

En tout temps, le Ministère limite sa cueillette ou sa communication de renseignements personnels à ce qui est nécessaire aux fins pour lesquelles le renseignement est recueilli.

Information et consentement

Comme le stipule l'article 53.1 de la Loi, le consentement doit être **manifeste, libre, éclairé et donné à des fins spécifiques**. Il est **demandé à chacune des fins visées** par la collecte en termes simples et clairs et **ne vaut que pour la durée nécessaire** à leur réalisation.

Afin que les critères ci-dessus soient respectés, le Ministère informe la personne concernée, notamment, des fins spécifiques de toute collecte ou communication de renseignement, et de ses droits. Le Ministère a le devoir d'expliquer la portée de ce consentement.

Durée nécessaire

Un consentement ne vaut que pour la durée nécessaire à la réalisation des fins pour lesquelles il a été demandé, en tenant compte du calendrier de conservation des documents du Ministère.

Le Ministère s'assure de détruire de manière appropriée les renseignements personnels qu'il détient lorsque les finalités sont atteintes, sous réserve des délais prévus à son calendrier de conservation.

Confidentialité et sécurité

Le Ministère assure la confidentialité et la sécurité des renseignements personnels qu'il détient. Il s'est donné une politique de confidentialité et prend les mesures de sécurité nécessaires pour protéger les renseignements personnels, de leur collecte à leur destruction. Ces mesures tiennent compte de la sensibilité, de la finalité, de la quantité, de la répartition et du support des renseignements personnels.

Droits de la personne concernée par un renseignement

Le Ministère veille à ce que les renseignements personnels qu'il conserve soient à jour, exacts et complets pour servir aux fins pour lesquelles ils sont recueillis. Toute personne peut demander de consulter ou d'obtenir copie des renseignements personnels que le Ministère détient à son sujet. Elle peut aussi demander l'accès aux renseignements informatisés qu'elle a fournis au Ministère, dans un format technologique structuré et couramment utilisé.

Toute personne peut exiger que le fichier soit rectifié si elle constate qu'un renseignement est inexact, incomplet ou équivoque ou si sa collecte, sa communication ou sa conservation ne sont pas autorisées par la Loi.

RÈGLES DE GOUVERNANCE

La mise en œuvre de la Loi englobe tout le cycle de vie d'un renseignement personnel, lequel comprend cinq phases distinctes : la **collecte**, l'**utilisation**, la **communication**, la **conservation** et la **destruction** ou l'anonymisation.

1. Collecte

La collecte est le moment où le renseignement personnel est recueilli ou créé.

Exigences préalables à la collecte

Tout projet comportant une collecte de renseignements personnels doit faire l'objet d'une évaluation et d'une décision préalables à la collecte elle-même. Dans le cadre de ce processus, les éléments suivants doivent être fournis :

- Un avis en matière de protection des renseignements personnels (avis PRP);
- Une évaluation des facteurs relatifs à la vie privée (EFVP), requise par la Loi pour certains types de projets;
- Une entente, si un organisme public collabore avec le Ministère, ou un contrat, si un tiers est mandaté pour l'exécution d'une partie ou de la totalité d'un projet;
- Une décision du Comité sur l'accès à l'information et sur la protection des renseignements personnels (Comité AIPRP) lorsque le projet nécessite une EFVP;
- L'approbation du Comité sur l'accès à l'information et sur la protection des renseignements personnels (Comité AIPRP), si le projet implique l'acquisition, le développement ou la refonte d'un

système d'information ou d'une prestation électronique de services. Cela inclut, notamment, tout système informatique de traitement des dossiers, logiciel de vidéoconférence ou de collaboration, système biométrique, d'intelligence artificielle, de cartes à puce ou d'identification par radiofréquence (RFID), de vidéosurveillance, statistique ou de gestion de la paie.

La mise en œuvre de ces processus préalables sera détaillée dans des directives complémentaires à la présente politique.

Renseignements personnels nécessaires

Le Ministère limite la collecte aux renseignements qui sont nécessaires à l'exercice de ses attributions, notamment les suivants :

- Identité et localisation : nom et prénom, adresse postale, adresse électronique ou numéro de téléphone;
- Renseignements techniques, par exemple pour un projet ou une demande nécessitant des informations de nature technique, des plans et devis, la localisation exacte du projet et des renseignements qui peuvent varier d'un projet à un autre ou d'un programme ou d'une mesure à l'autre;
- Facturation : renseignements financiers tels qu'une adresse de facturation, renseignements relatifs à un compte bancaire ou données de paiement, lorsque des frais sont facturés;
- Preuves du consentement qui a été accordé au Ministère, y compris la date et le moyen;
- Aux fins d'embauche de personnel, le Ministère recueille notamment les renseignements suivants : coordonnées personnelles, curriculum vitae, scolarité et antécédents professionnels tels qu'un titre de poste, noms de personnes-ressources, numéro de téléphone et adresse courriel au travail;

Renseignements que le Ministère recueille (numéro d'assurance sociale) ou crée (renseignements liés au classement, à la rémunération et à l'assiduité) au moment de l'embauche.

Collecte aux fins d'un sondage

Le Ministère peut procéder occasionnellement à des cueilletes de renseignements personnels dans le cadre de sondages visant notamment la satisfaction des clientèles ou visant à mieux connaître les préoccupations ou préférences des utilisateurs ou clients, en relation avec les attributions du Ministère.

Tout sondage fait l'objet d'une évaluation particulière qui abordera notamment les points suivants :

- La nécessité de recourir au sondage;
- L'aspect éthique du sondage, compte tenu, notamment, de la sensibilité des renseignements personnels recueillis et de la finalité de leur utilisation;
- Les mesures de protection additionnelles à prendre à l'égard des renseignements personnels recueillis ou utilisés dans le cadre d'un sondage.

Les règles de PRP applicables à la réalisation d'un sondage feront l'objet d'une directive complémentaire à la présente politique.

Collecte par des moyens technologiques

La collecte de renseignements personnels en ayant recours à des moyens technologiques, y compris toute collecte par vidéosurveillance ou biométrie, fait l'objet des mesures suivantes prises par le Ministère :

- Mise à jour de sa politique de confidentialité sur son site Internet et diffusion par tout moyen propre à atteindre les personnes concernées;
- Établissement des paramètres de confidentialité au plus haut niveau de protection possible lorsque le Ministère recueille des renseignements personnels en offrant un produit ou un service qui dispose de tels paramètres. Par défaut, ces paramètres assurent le plus haut niveau de protection, sans aucune intervention de la personne concernée;
- Désactivation par défaut des fonctions technologiques permettant d'identifier une personne, de la localiser ou d'effectuer un profilage, dans l'éventualité où de telles fonctions seraient en usage. La personne concernée doit pouvoir activer ces fonctions elle-même, volontairement et sans aucune pression.

La Loi définit le profilage comme la « collecte et l'utilisation de renseignements personnels afin d'évaluer certaines caractéristiques d'une personne physique, notamment à des fins d'analyse du rendement au travail, de la situation économique, de la santé, des préférences personnelles, des intérêts ou du comportement de la personne »;

- Information au public d'une collecte par vidéosurveillance, au moyen d'un avis bien en vue indiquant notamment les fins de la surveillance, les périodes d'activation et les coordonnées pour joindre l'unité administrative utilisatrice de l'équipement.

Information à la personne concernée par la collecte

Avant d'accorder son consentement, la personne doit d'abord pouvoir prendre connaissance de l'information. Celle-ci doit être rédigée en termes simples et clairs. Lorsque la demande de consentement est faite par écrit, elle doit être présentée distinctement de toute autre information communiquée à la personne concernée.

L'information à fournir avant la collecte inclut notamment :

- l'identification de l'organisme au nom de qui la collecte est faite, une description de chacune des fins visées par la collecte, les moyens de collecte, la nécessité de recourir à un sondage, le cas échéant, les mesures de protection propres au sondage et le droit de la personne de refuser d'y participer;
- les paramètres de confidentialité au plus haut niveau, le caractère obligatoire ou facultatif du consentement, la possibilité de refuser et de retirer le consentement, ainsi que les conséquences en cas de refus.

Les éléments d'information à fournir avant toute collecte sont présentés en détail dans la directive relative à la collecte.

Obtention du consentement

Le consentement est demandé :

- pour chacune des fins visées par la collecte, exposées en langage simple et clair;

- dès qu'il s'agit d'un renseignement personnel sensible, le consentement est demandé de façon manifeste et précise, en faisant ressortir le caractère sensible du renseignement visé.

Un renseignement personnel est sensible lorsque, du fait de sa nature notamment médicale, biométrique ou autrement intime, ou en raison du contexte de son utilisation ou de sa communication, il suscite un haut degré d'attente raisonnable en matière de vie privée.

Un renseignement personnel, dans les catégories suivantes, doit généralement être considéré comme sensible : renseignements financiers, génétiques ou biométriques, sur la santé, la vie et l'orientation sexuelle, sur les convictions religieuses, les opinions politiques ainsi que l'origine ethnique ou raciale.

Un consentement est manifesté de façon expresse lorsqu'il est explicitement exprimé par un geste ou une déclaration (orale ou écrite) témoignant de l'acceptation par la personne concernée. Un consentement exprès ne laisse aucun doute sur la volonté réelle de la personne.

La personne doit pouvoir décider librement si elle consent ou non et le Ministère conserve une preuve du consentement.

Un consentement est sans effet s'il n'est pas donné conformément aux critères exposés ci-dessus.

2. Utilisation

Le Ministère n'utilise les renseignements personnels qu'aux fins pour lesquelles ils ont été recueillis, à moins du consentement de la personne concernée, et pour la durée prévue en tenant compte du calendrier de conservation du Ministère.

La Loi prévoit cependant des cas d'utilisation à des fins autres que celles pour lesquels un renseignement a été recueilli.

Utilisation à d'autres fins

Le Ministère peut utiliser un renseignement personnel à une autre fin, sans le consentement de la personne concernée, uniquement lorsque l'utilisation est :

- 1° À des fins compatibles avec celles pour lesquelles le renseignement a été recueilli. Pour qu'une fin soit compatible, il doit y avoir un lien pertinent et direct avec les fins pour lesquelles le renseignement a été recueilli;
- 2° Manifestement au bénéfice de la personne concernée;
- 3° Nécessaire à l'application d'une loi au Québec, que cette utilisation soit ou non prévue expressément par la Loi;
- 4° Nécessaire à des fins d'étude, de recherche ou de production de statistiques et qu'il est dépersonnalisé. Un renseignement est dépersonnalisé lorsque ce renseignement ne permet plus d'identifier directement la personne concernée. Un organisme public qui utilise des renseignements dépersonnalisés doit prendre les mesures raisonnables afin de limiter les risques que quiconque procède à l'identification d'une personne physique à partir de renseignements dépersonnalisés.

Ces utilisations requièrent l'obtention d'un avis PRP favorable du responsable de l'accès à l'information et de la protection des renseignements personnels (responsable AIPRP).

Ces utilisations sont consignées dans le Registre des utilisations et communications sans consentement. Toute personne qui en fait la demande a le droit d'accéder au registre, sauf pour obtenir un renseignement dont la confirmation de l'existence ou la communication peut être refusée en vertu de la Loi.

Utilisation pour une décision fondée sur un traitement automatisé

Dans l'éventualité où le Ministère utilise des renseignements personnels afin que soit rendue une décision fondée exclusivement sur un traitement automatisé de ceux-ci, il informe la personne concernée du mode de décision au plus tard lorsque la décision est communiquée à cette personne.

De plus, si la personne en fait la demande, le Ministère l'informe :

- des renseignements personnels utilisés pour rendre la décision;
- des raisons et principaux facteurs ayant mené à la décision;
- de son droit de faire rectifier les renseignements personnels utilisés pour rendre la décision.

Le Ministère donne à la personne concernée la possibilité de présenter ses observations à un membre du personnel qui est en mesure, le cas échéant, de réviser la décision.

Utilisation dans l'exercice des fonctions d'une personne à l'emploi du Ministère

Le Ministère s'assure que l'accès aux renseignements personnels est limité aux seules personnes ayant qualité pour les recevoir au sein du Ministère, lorsque ces renseignements sont nécessaires à l'exercice de leurs fonctions.

Chacune de ces personnes fait partie d'une catégorie autorisée à accéder à un fichier de renseignements donné et chaque personne y est autorisée individuellement par son supérieur.

3. Communication

Le Ministère ne peut communiquer un renseignement de la personne concernée à un organisme public ou à un tiers que s'il a préalablement obtenu le consentement de cette personne.

Certaines exceptions et situations particulières permettant la communication de renseignements personnels sans consentement sont prévues par la Loi. Malgré ces exceptions, le Ministère privilégiera, dans la mesure du possible, l'obtention du consentement.

Communication sans consentement

Une communication sans consentement peut être effectuée dans les cas suivants :

- Communication en raison d'un événement ayant fait l'objet d'un rapport de police ou d'un rapport similaire, lors d'une situation d'urgence mettant en danger la vie, la santé ou la sécurité, ou dans les cas de prévention d'actes de violence;
- Communication au Directeur des poursuites criminelles et pénales si le renseignement est nécessaire aux fins d'une poursuite pour une infraction à une loi applicable au Québec, ou au procureur général si le renseignement est nécessaire aux fins d'une autre procédure judiciaire;

- Communication de documents ou de renseignements exigés par le Protecteur du citoyen ou par assignation, citation à comparaître, mandat ou ordonnance d'une personne ou d'un organisme ayant le pouvoir de contraindre à leur communication;
- Utilisation nécessaire à l'application d'une loi au Québec, que cette communication soit ou non prévue par la Loi;
- Exercice d'un mandat ou exécution d'un contrat de services ou d'entreprise confié par le Ministère;
- Application d'une convention collective, d'un décret, d'un arrêté, d'une directive ou d'un règlement qui établissent des conditions de travail;
- Communication à une personne ou à un organisme aux fins d'étude, de recherche ou de production de statistiques, auquel cas une EFVP et une entente sont nécessaires;
- Communication à un organisme public ou à un organisme d'un autre gouvernement, aux fins de prestation de programmes ou de services de l'organisme receveur lorsque la communication est nettement au bénéfice de la personne concernée, ou encore à une personne ou un organisme lorsque des circonstances exceptionnelles le justifient.

Toute communication sans consentement d'un renseignement personnel nécessite un avis PRP et, dans certains cas, une EFVP, une décision du Comité AIPRP ainsi qu'une entente avec un organisme demandeur.

De plus, toute communication sans consentement est consignée dans le Registre des utilisations et communications sans consentement. Toute personne qui en fait la demande a droit d'accès au registre, sauf pour certains cas où la confirmation de l'existence d'un renseignement peut être refusée en vertu de la Loi.

4. Conservation

La conservation est la période durant laquelle un organisme garde des renseignements personnels, sous quelque forme que ce soit, et ce, peu importe que les renseignements soient activement utilisés ou non.

Les renseignements personnels sont conservés tant et aussi longtemps qu'ils sont nécessaires pour réaliser les activités et offrir les services, en tenant compte de la période prévue au calendrier de conservation du Ministère.

Le Ministère applique les mesures technologiques, physiques et organisationnelles de sécurité de l'information qui sont nécessaires et raisonnables.

À chaque étape du cycle de vie, le Ministère s'assure de :

- veiller à ce que les renseignements personnels qu'il détient soient à jour et exacts au moment où il les utilise pour prendre une décision relative à la personne concernée;
- catégoriser les types de support pour leur associer les méthodes de conservation et de destruction appropriées, par exemple : support numérique, vidéo, enregistrement vocal, papier, ou bac sécurisé;
- prendre les mesures propres à assurer la sécurité des renseignements personnels conservés, notamment : protection contre les attaques extérieures, les pertes, le vol, l'accès non autorisé et la divulgation, la copie, l'utilisation ou la modification non autorisée. Seuls les membres du personnel dont l'accès aux renseignements personnels est nécessaire dans le cadre de leurs fonctions sont autorisés à y accéder.

De plus, tout contrat avec un tiers incorpore les obligations découlant des dispositions de la Loi en matière de protection des renseignements personnels.

Inventaire des fichiers de renseignements personnels

La fonction de conservation des renseignements personnels comprend la mise à jour des fichiers et l'inventaire des fichiers détenus.

À cette fin, le Ministère s'assure de constituer en fichiers les renseignements personnels qu'il détient et de maintenir un inventaire des fichiers à jour.

Cet inventaire est accessible sur la page [Protection des renseignements personnels | Gouvernement du Québec](#).

5. Demande d'accès ou de rectification

Accès

Toute personne qui en fait la demande a un droit d'accès aux renseignements personnels la concernant, pendant tout le cycle de vie de ses renseignements, sous réserve des exceptions prévues par la Loi.

Une demande ne peut être considérée que si elle est faite par écrit par une personne physique justifiant de son identité à titre de personne concernée ou à titre de personne représentante autorisée, avec documents à l'appui. Cette demande doit être adressée au responsable AIPRP.

La demande doit fournir suffisamment d'information pour en permettre le traitement. Le responsable AIPRP accuse réception de la demande auprès de la personne requérante.

Rectification

Toute personne qui reçoit la confirmation de l'existence d'un renseignement personnel la concernant peut exiger que le fichier soit rectifié, s'il est inexact, incomplet ou ambigu, ou si sa collecte, sa communication ou sa conservation ne lui semble pas autorisée par la Loi.

Une personne physique qui justifie de son identité à titre de personne concernée ou à titre de personne représentante autorisée peut formuler, par écrit, une demande de communication ou de rectification en écrivant à accès@environnement.gouv.qc.ca et en fournissant suffisamment d'indications précises pour en permettre le traitement. Lorsqu'il accorde une demande de rectification, le Ministère délivre à la personne à l'origine de la demande une copie de tout renseignement personnel modifié ou ajouté, ou, selon le cas, une attestation du retrait.

6. Destruction ou anonymisation

Le cycle de vie du renseignement personnel se termine lors de sa destruction.

Le Ministère détruit de façon sécuritaire les renseignements personnels lorsque les fins pour lesquelles ils ont été collectés sont atteintes, sous réserve des lois applicables quant à leur conservation.

À cette fin, le Ministère :

- choisit une méthode de destruction adaptée, par exemple le formatage, le déchiquetage numérique ou la destruction physique, et conserve une trace des dossiers qui ont été détruits;
- peut conclure, avec un tiers, un contrat prévoyant les procédés de destruction, l'obligation de confidentialité, l'entreposage, l'accès aux locaux, la reddition de comptes, les mesures de sécurité, la gestion des incidents de sécurité et les règles applicables à ses employés et sous-traitants.

RÔLES ET RESPONSABILITÉS

Sous-ministre

En tant que personne détenant la plus haute autorité au Ministère, la sous-ministre veille à y assurer le respect et la mise en œuvre de la Loi.

La sous-ministre préside le Comité AIPRP.

Elle délègue la fonction de responsable AIPRP à un membre du personnel de direction.

Elle prévoit les ressources nécessaires à la réalisation des tâches et responsabilités relatives à la protection des renseignements personnels.

Comité sur l'accès et la protection des renseignements personnels (Comité AIPRP)

Constitué en vertu de la Loi, le Comité AIPRP est chargé de soutenir le Ministère dans la mise en œuvre des dispositions de la Loi et des règles qui en découlent.

Le Comité AIPRP relève de la sous-ministre et se compose de la personne responsable de l'accès au document et de la protection des renseignements personnels, du directeur général des technologies de l'information, du sous-ministre adjoint au soutien et à la transformation organisationnelle, de la secrétaire générale, de la directrice de l'expérience client et de la gestion documentaire ainsi que de la directrice de l'audit interne et de la gestion des risques.

Le Comité AIPRP peut s'adjoindre toute autre personne qu'il juge utile.

Le Comité AIPRP doit notamment approuver :

- les politiques et règles encadrant la gouvernance et la confidentialité à l'égard des renseignements personnels, de même que les directives ou guides;
- tout projet lié à l'acquisition, au développement ou à la refonte de systèmes d'information ou de prestation électronique de services et les mesures de protection des renseignements personnels applicables à ces projets. Cela inclut, notamment, les moyens technologiques permettant la cueillette de renseignements et comportant des fonctions de localisation ou de profilage de la personne, de même que tout projet de vidéosurveillance ou de collecte de données biométriques;
- un programme de sensibilisation et de formation sur la protection des renseignements personnels.

Responsable de l'accès à l'information et de la protection des renseignements personnels (responsable AIPRP)

Le responsable AIPRP doit notamment :

- coordonner et supporter les travaux du Comité AIPRP;
- rédiger et réviser les politiques et les règles en matière de protection des renseignements personnels qu'il présente au Comité AIPRP;
- promouvoir le développement d'une culture de protection de la vie privée au sein du Ministère.

À toutes les étapes du cycle de vie d'un renseignement personnel, le responsable AIPRP doit :

- réaliser les EFVP en collaboration avec les unités administratives à l'origine de tout projet nécessitant une EFVP;
- produire un avis écrit (l'avis PRP) portant sur toute initiative ou mesure, en cours ou nouvelle, visant la collecte, l'utilisation, la communication, la conservation et la destruction ou l'anonymisation d'un renseignement personnel;
- évaluer la conformité de toute utilisation ou communication de renseignements personnels à des fins autres que celles envisagées initialement;
- commenter ou appuyer la rédaction des ententes de communication de renseignements personnels à d'autres organismes publics ou à l'extérieur du Québec, formuler des avis en la matière et, après l'approbation des ententes, les soumettre à la Commission;

- coordonner la mise à jour des fichiers de renseignements personnels de même que l'inventaire des fichiers du Ministère;
- recevoir et traiter les demandes d'accès et de rectification;
- recevoir et traiter les incidents de confidentialité en fonction des règles en matière de protection des renseignements personnels et de sécurité de l'information;
- recevoir les plaintes qui mettent en cause la protection des renseignements personnels et les traiter en fonction des règles en matière de protection des renseignements personnels et de sécurité de l'information;
- tenir à jour le Registre des utilisations et communications sans consentement, le Registre des ententes de collecte de renseignements et le Registre des incidents de confidentialité.

Direction générale des technologies de l'information (DGTI)

La DGTI doit :

- informer le responsable AIPRP dès le début de tout projet de système d'information ou de prestation électronique de services utilisant des renseignements personnels;
- collaborer avec l'unité administrative concernée ainsi qu'avec le responsable AIPRP à la réalisation d'une EFVP pour tout projet de système d'information ou de prestation électronique de services;
- maintenir à jour la politique et les mesures de sécurité relatives aux systèmes d'information ou de prestation électronique de services et les déposer au Comité AIPRP;
- appliquer les mesures appropriées à toute menace et tout incident de sécurité lorsque les circonstances l'exigent;
- assurer le fonctionnement du processus de gestion des accès selon les mécanismes mis en place.

Direction générale des ressources financières et matérielles (DGRFM)

La DGRFM doit :

- concevoir et mettre en œuvre les mesures de protection physique contre les sinistres, les pertes, les dommages, le vol ainsi que l'interruption des activités pouvant compromettre des renseignements personnels;
- sécuriser et contrôler les accès physiques aux locaux du Ministère;
- faire approuver par le responsable AIPRP les exigences contractuelles visant la protection des renseignements personnels pour tout contrat avec un fournisseur ou un prestataire de services.

Direction générale des ressources humaines

La Direction générale des ressources humaines doit :

- informer la DGTI et la DRFM d'une embauche, d'un changement de fonction et de la fin d'emploi d'une personne, afin de mettre à jour les accès aux actifs informationnels de même qu'aux locaux du Ministère;

- communiquer, dans le dossier d'accueil de tout nouvel employé, ses obligations découlant de la Politique et de tout cadre normatif qui en découle;
- intervenir auprès des membres du personnel concernés en cas d'atteinte à la confidentialité et à la protection des renseignements personnels, en collaboration avec le gestionnaire concerné, le responsable AIPRP et les autres parties prenantes.

Responsable de la gestion documentaire

Le responsable de la gestion documentaire doit :

- participer à l'analyse et à la planification des besoins et des actions concernant la gestion des documents et des archives qui impliquent la protection de renseignements personnels;
- appuyer les unités administratives responsables dans la conservation des renseignements personnels et dans la gestion des accès pour les catégories de personnes à l'emploi du Ministère autorisées à y accéder pour l'exercice de leurs fonctions;
- s'assurer que les délais de conservation des renseignements personnels prévus au calendrier de conservation du Ministère respectent les normes en la matière;
- conserver les fichiers et l'inventaire des fichiers de renseignements personnels, en collaboration avec les unités administratives concernées et la Direction principale des renseignements, de l'accès à l'information, de l'éthique et des plaintes;
- s'assurer que les moyens utilisés pour la destruction des renseignements personnels sont sécuritaires et protègent leur caractère confidentiel.

Gestionnaire

Chaque gestionnaire est responsable de veiller à la protection des renseignements personnels détenus par l'unité administrative qu'il dirige. Il doit notamment :

- informer et sensibiliser les membres du personnel relevant de son autorité à propos des dispositions de la Politique et des directives ou règles pouvant en découler, et s'assurer de leur application;
- demander un avis écrit au responsable AIPRP sur la légitimité et la nécessité de toute initiative, en cours ou nouvelle, visant la collecte, l'utilisation, la communication, la conservation et la destruction ou l'anonymisation d'un renseignement personnel;
- collaborer, avec le responsable AIPRP, à l'élaboration de l'EFVP requise pour toute communication de renseignements à un autre organisme ou à l'extérieur du Québec; tout projet de système d'information ou de prestation électronique de services; tout projet permettant d'identifier, de localiser ou d'effectuer un profilage et tout projet de vidéosurveillance et de mesure biométrique. Dans le cas d'un système d'information ou de prestation électronique, le gestionnaire s'assure de la collaboration de la Direction générale des technologies de l'information;
- s'assurer que le personnel sous sa responsabilité participe aux formations relatives à la protection des renseignements personnels offertes par le Ministère;

- prendre les mesures appropriées en cas de manquement à la présente politique ou aux règles de protection des renseignements personnels par un membre du personnel sous sa responsabilité.

En matière de collecte et d'utilisation de renseignements personnels, le gestionnaire doit notamment :

- recenser les renseignements personnels que son unité administrative utilise, détient ou envisage de recueillir et déterminer les finalités précises de tout nouveau projet ou de toute nouvelle activité nécessitant des renseignements personnels;
- demander un avis écrit au responsable AIPRP portant sur l'utilisation de tout formulaire, de cueillette, d'information et de consentement, en usage ou proposé;
- tenir à jour les fichiers de renseignements personnels et l'inventaire des fichiers pour lesquels son unité administrative assume la responsabilité;
- apporter les révisions ou modifications nécessaires à tout fichier de renseignements personnels détenu par son unité administrative et notifier toute révision ou modification au Responsable AIPRP. En l'absence de changement nécessitant la modification d'un fichier ou de l'inventaire, aviser de l'absence de changement une fois par exercice annuel, dans le but de confirmer que l'inventaire requis par la Loi est à jour;
- autoriser, réviser ou révoquer les accès des personnes de son unité administrative devant utiliser les renseignements personnels dans l'exercice de leurs fonctions. Notifier toute modification au responsable AIPRP. En l'absence de modifications, notifier la liste des accès autorisés au moins une fois par exercice annuel dans le but de confirmer que la liste des accès autorisés est à jour;
- veiller à ce que les renseignements personnels dont son unité administrative est détentrice soient à jour, exacts et utilisés uniquement pour les fins déterminées lors de leur collecte.

En matière de communication de renseignements personnels, le gestionnaire doit notamment :

- obtenir l'autorisation du responsable AIPRP avant de communiquer des renseignements personnels à une personne ou à un organisme, étant entendu qu'une telle communication est soumise à un avis PRP ou une EFVP et à une entente avec la personne ou l'organisme, entente qui peut entrer en vigueur 30 jours après sa réception à la Commission;
- conclure avec tout fournisseur ou prestataire de services un contrat comportant les dispositions de protection de renseignements personnels conformes à la Loi ainsi qu'un engagement de confidentialité signé par tout employé impliqué dans la fourniture de biens ou services ou dans l'exécution du contrat, et s'assurer de la conservation de ces contrats et engagements signés dans le fichier des communications de renseignements personnels;
- obtenir, au terme d'un contrat avec tout fournisseur ou prestataire de services pour la destruction de renseignements, une attestation de destruction des renseignements personnels, et mettre à jour le fichier et l'inventaire des fichiers des renseignements personnels détenus par son unité administrative.

En matière de conservation des renseignements, le gestionnaire doit :

- mettre en place les mesures nécessaires pour assurer la conservation sécuritaire des renseignements détenus par son unité administrative, en collaboration avec le responsable de la gestion documentaire;
- mettre en place les mesures nécessaires pour s'assurer du respect des règles de conservation des renseignements détenus;

- autoriser la destruction de renseignements personnels ou leur anonymisation.

Personne à l'emploi du Ministère

Toute personne à l'emploi du Ministère doit :

- prendre connaissance de la présente politique et en respecter l'esprit, les dispositions et les règles ou directives qui en découlent;
- utiliser des moyens conformes aux mesures de sécurité du Ministère, pour recueillir, utiliser, conserver, communiquer ou détruire des renseignements personnels;
- n'accéder qu'aux renseignements personnels nécessaires à l'exercice de ses fonctions;
- utiliser les renseignements personnels auxquels elle a accès uniquement pour les fins prévues lors de leur collecte;
- s'assurer que les renseignements personnels qu'elle utilise sont complets, à jour et exacts pour servir aux fins pour lesquelles le Ministère les recueille ou les utilise;
- s'assurer d'être autorisée à communiquer des renseignements personnels avant de le faire;
- s'adresser à son gestionnaire en cas de doute quant à la confidentialité d'un renseignement ou de question au sujet de la gestion des renseignements personnels;
- obtenir l'autorisation de son gestionnaire avant de détruire tout renseignement personnel;
- informer son gestionnaire de tout incident qui pourrait compromettre la protection des renseignements personnels détenus par le Ministère;
- participer aux activités de sensibilisation et de formation à la protection des renseignements personnels mis à sa disposition par le Ministère.

En outre, toute personne à l'emploi du Ministère doit, pour les accès physiques, s'assurer au quotidien de :

- verrouiller ses filières;
- éviter de laisser à la vue des dossiers contenant des renseignements personnels;
- privilégier l'utilisation de bacs sécurisés comme moyen de destruction de documents personnels sur papier, en tenant compte du calendrier de conservation du Ministère et en ayant obtenu les autorisations nécessaires;
- faire preuve de discrétion lorsqu'elle discute d'un dossier contenant des renseignements personnels;
- verrouiller sa session de travail lorsqu'elle quitte son poste de travail, même pour de courtes périodes;
- utiliser des moyens de communication et de transmission sécuritaires, conformes aux règles de sécurité.

SENSIBILISATION ET FORMATION DU PERSONNEL

Le Ministère rendra disponibles des formations sur mesure et des outils d'information visant la protection des renseignements personnels pour toute personne à son emploi et ayant pour but de :

- présenter un aperçu de la Loi et sensibiliser à son importance en matière de protection de la vie privée;
- faire comprendre les principes qui sous-tendent les règles qui en découlent;
- présenter les règles applicables à chaque étape du cycle de vie d'un renseignement personnel, avec pour objectif qu'elles constituent un repère facilement utilisable dans le travail quotidien;
- présenter les rôles et responsabilités découlant de la Loi;
- bien faire comprendre le processus s'appliquant à d'éventuels incidents de confidentialité.

Cet éventail d'outils sera notamment constitué de :

- Capsules de sensibilisation sur des thèmes précis;
- Articles et messages internes dans l'intranet;
- Webinaires, présentations;
- Présentations ciblées aux équipes.

PLAINTES EN MATIÈRE DE RENSEIGNEMENTS PERSONNELS

Dans un souci d'améliorer constamment la qualité de ses services, le Ministère accorde une grande importance aux commentaires, suggestions et plaintes des citoyens.

Quiconque considère que le Ministère ne respecte pas ses droits en matière de protection des renseignements personnels peut transmettre une plainte par écrit, au responsable AIPRP.

Déposer une plainte

Toute plainte en matière de renseignements personnels est traitée selon la procédure de traitement d'une plainte du Ministère, accessible à la page [Plaintes | Gouvernement du Québec \(quebec.ca\)](#)

Une plainte peut être déposée à l'adresse suivante :

Responsable de la gestion des plaintes
Direction principale des renseignements, de l'accès à l'information, de l'éthique et des plaintes,
ministère de l'Environnement, de la Lutte contre les changements climatiques,
de la Faune et des Parcs
675, boulevard René-Lévesque Est, 29^e étage
Québec (Québec) G1R 5V7
418 521-3858, poste 4980
plaintes@environnement.gouv.qc.ca

À consulter aussi : [Politique de gestion des plaintes sur la qualité des services](#)

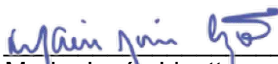
ENTRÉE EN VIGUEUR ET RÉVISION

La présente politique en matière de protection des renseignements personnels et les règles qu'elle comporte sont approuvées par le Comité sur l'accès à l'information et la protection des renseignements personnels (Comité AIPRP).

La politique entre en vigueur à la date de son approbation par le Comité AIPRP. Elle demeure en application tant et aussi longtemps qu'elle n'est pas abrogée, modifiée ou remplacée par un autre cadre de gouvernance.

Elle est régulièrement réévaluée par le Comité AIPRP, notamment en ce qui a trait à la pertinence de ses énoncés à l'égard des nouveaux enjeux de protection des renseignements personnels.

Date : 2025-01-17

Approuvé par : 
Marie-Josée Lizotte,
Sous-ministre



**Environnement,
Lutte contre
les changements
climatiques,
Faune et Parcs**

Québec 