

Ministère
de la Sécurité
publique

POLITIQUE MINISTÉRIELLE

SUR LA PROTECTION DES
RENSEIGNEMENTS PERSONNELS

Ce document a été préparé par la Direction de la gestion intégrée des documents et des relations avec les citoyens du ministère de la Sécurité publique.

Nous remercions pour leur éclairage chacune des personnes ayant contribué aux réflexions indispensables à la production de la version définitive de ce document d'orientation.

Version – Décembre 2023

© Gouvernement du Québec

Table des matières

1. INTRODUCTION	5
2. OBJECTIFS DE LA POLITIQUE.....	5
3. CHAMP D'APPLICATION.....	5
4. DÉFINITIONS	5
5. PRINCIPES DIRECTEURS DE LA POLITIQUE	7
6. RÔLES ET RESPONSABILITÉS	8
7. ÉTAPES DU CYCLE DE VIE D'UN RENSEIGNEMENT PERSONNEL	9
8. SONDAGE	11
9. INCIDENT DE CONFIDENTIALITÉ IMPLIQUANT UN RENSEIGNEMENT PERSONNEL	11
10. DROITS DE LA PERSONNE CONCERNÉE PAR UN RENSEIGNEMENT PERSONNEL	12
11. RÉVISION DE LA POLITIQUE.....	12
12. ENTRÉE EN VIGUEUR	12
ANNEXE 1 : HISTORIQUE DES MODIFICATIONS.....	13

1. Introduction

Le ministère de la Sécurité publique (ci-après désigné comme « le MSP ») est responsable d'assurer la protection des renseignements personnels qu'il détient sur sa clientèle et ses employés. Cette responsabilité s'étend peu importe que la collecte, l'utilisation, la communication, la conservation ou la destruction soit assurée par le MSP ou un tiers.

2. Objectifs de la politique

La présente politique a pour objectif de définir les règles et les principes généraux encadrant sa gouvernance à l'égard des renseignements personnels en application de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*¹ (ci-après la « *Loi sur l'accès* ») et des autres dispositions légales applicables.

3. Champ d'application

La présente politique s'applique à l'ensemble du personnel du MSP ainsi qu'à toute personne morale ou physique qui, par engagement contractuel ou autrement, a accès aux renseignements personnels collectés et détenus par le MSP, et ce, dans le cadre de l'exercice de ses fonctions ou d'un mandat.

En outre, elle s'applique à l'ensemble des activités du MSP qui nécessitent la collecte, l'utilisation, la communication, la conservation et la destruction de renseignements personnels, quel que soit leur support.

4. Définitions

Biométrie

Elle permet d'identifier ou d'authentifier une personne grâce à ses caractéristiques uniques. Il existe trois types de biométrie :

- Morphologique : basée sur l'identification de traits physiques particuliers (reconnaissance des empreintes digitales, de la forme de la main, du visage, de la rétine et de l'iris de l'œil);
- Comportementale : basée sur l'analyse de certains comportements d'une personne (tracé de sa signature, sa voix, sa démarche, sa façon de taper sur un clavier, etc.);
- Biologique : basée sur l'analyse des traces biologiques d'une personne (l'ADN, le sang, la salive, l'urine, les odeurs).

¹ RLRQ, c. A-2.1.

Critère de nécessité

L'objectif du critère de nécessité est de réduire les atteintes à la vie privée. Un renseignement personnel est nécessaire si l'atteinte à la vie privée par sa collecte est proportionnelle à une finalité légitime et importante. Ce critère doit donc être évalué lors des étapes de collecte, d'utilisation et de communication des renseignements personnels. Le résultat de cette évaluation doit permettre d'affirmer que le besoin de l'organisme est supérieur à l'atteinte à la vie privée pour la personne concernée. L'organisme est en mesure de démontrer qu'il n'a pas d'autre moyen pour atteindre ses objectifs. Le consentement d'une personne ne peut permettre de déroger au critère de nécessité.

Évaluation des facteurs relatifs à la vie privée

Elle 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'impact. 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.

Incident de confidentialité impliquant un renseignement personnel

L'accès non autorisé par la loi à un renseignement personnel, ou l'utilisation ou la communication non autorisée par la loi d'un tel renseignement, ainsi que sa perte ou toute autre atteinte à sa protection.

Renseignement anonymisé

Un renseignement personnel est anonymisé quand il est, en tout temps, raisonnable de prévoir dans les circonstances qu'il ne permet plus, de façon irréversible, d'identifier directement ou indirectement la personne concernée.

Renseignement dépersonnalisé

Un renseignement personnel est dépersonnalisé lorsqu'il ne permet plus d'identifier directement la personne concernée. La dépersonnalisation consiste à retirer tous les renseignements qui permettent l'identification directe de la personne concernée.

Renseignement personnel

Tout renseignement qui concerne une personne physique qui permet, directement ou indirectement, de l'identifier.

Renseignement personnel sensible

Un renseignement personnel est sensible lorsque, par sa nature 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 (ex. : renseignements médicaux, biométriques, convictions religieuses, origine ethnique).

5. Principes directeurs de la politique

Dans l'objectif d'assumer pleinement ses responsabilités en matière de protection des renseignements personnels, les règles encadrant la gouvernance ministérielle s'appuient sur les principes suivants :

- **PRINCIPE 1 – Être transparent à l'égard des personnes concernées**

Le MSP respecte les renseignements personnels qu'il détient. Il permet aux personnes concernées de bien comprendre leurs droits en matière de vie privée, pourquoi leurs renseignements sont collectés, comment ils sont utilisés et à quelles fins. Le MSP traite toute plainte relative à la protection des renseignements personnels de manière objective et transparente sur la base de ses engagements de la Déclaration de services aux citoyennes et citoyens².

- **PRINCIPE 2 – Former et sensibiliser les employés**

Le MSP accompagne ses employés afin qu'ils comprennent leurs responsabilités et qu'ils puissent assurer la protection des renseignements personnels nécessaires à l'exercice de leurs fonctions. À cet effet, il offre des activités de sensibilisation et de formation en continu. De plus, il met en place divers outils à la disposition des employés.

- **PRINCIPE 3 – Intégrer la protection des renseignements personnels au tout début des projets**

Dès le début d'un projet, le MSP tient compte de la protection des renseignements personnels. Lorsque cela est requis en vertu de la *Loi sur l'accès*, une évaluation des facteurs relatifs à la vie privée est réalisée.

- **PRINCIPE 4 – S'assurer de la conformité des consentements des personnes concernées**

Le MSP s'assure que les huit critères de validité d'un consentement sont respectés :

- Manifeste : évident, qui démontre une volonté réelle;
- Libre : volontaire, sans contrainte ou pression;
- Éclairé : la personne doit comprendre ce à quoi elle consent;
- Spécifique : pour une fin précise;
- Granulaire : doit être demandé pour chacune des fins visées;
- Compréhensible : en termes simples et clairs;
- Temporaire : pour une durée limitée;
- Distinct : séparé des autres informations.

² <https://www.quebec.ca/gouvernement/ministere/securite-publique/declarations-de-services>

6. Rôles et responsabilités

Le MSP considère que la protection des renseignements personnels est une responsabilité stratégique et horizontale impliquant l'ensemble de ses employés.

- **Le Comité sur l'accès à l'information et la protection des renseignements personnels**

Le Comité sur l'accès à l'information et la protection des renseignements personnels (CAIPRP) est chargé de soutenir le sous-ministre dans l'exercice de ses responsabilités et dans l'exécution de ses obligations en vertu de la *Loi sur l'accès*. En plus d'assumer certaines autres responsabilités prévues par la loi, le CAIPRP exerce un rôle de leadership et contribue à la promotion d'une culture organisationnelle qui renforce la protection des renseignements personnels et favorise la transparence. Par sa composition multisectorielle, ses travaux permettent une consultation horizontale pour suggérer des mesures particulières de protection relativement aux différents projets impliquant des renseignements personnels. Il propose également des orientations stratégiques et opérationnelles en matière de protection des renseignements personnels.

- **Le responsable de la protection des renseignements personnels**

Le responsable de la protection des renseignements personnels (RPRP) exerce une fonction stratégique dans le respect du droit à la vie privée reconnu par la *Charte des droits et libertés de la personne*³. Pour ce faire, il conseille le sous-ministre, la haute direction et le CAIPRP sur l'adoption d'un cadre de gouvernance de la protection des renseignements personnels. Il conseille et soutient les unités opérationnelles dans la mise en œuvre des orientations et des stratégies du MSP en matière de protection des renseignements personnels et sur l'exercice de leurs rôles et responsabilités à cet égard.

Il oriente et suggère des mesures afin d'assurer la protection des renseignements personnels et le respect des obligations légales dans le cadre des différents projets. De plus, il sensibilise l'ensemble des employés sur les bonnes pratiques en matière de protection des renseignements personnels. Il s'assure également du traitement des plaintes relatives à la protection des renseignements personnels.

- **Le responsable de la sécurité de l'information**

Le responsable de la sécurité de l'information (RSI) exerce un leadership et une fonction stratégique pour assurer une approche intégrée de la sécurité applicable aux renseignements personnels, et ce, tout au long de leur cycle de vie. Au MSP, le rôle du RSI est associé au rôle du directeur général adjoint de la sécurité de l'information. Il s'assure que la stratégie et les mesures de sécurité de l'information s'inscrivent dans les principes et les orientations en matière de protection des renseignements personnels recommandés par le RPRP.

³ RLRQ, c. C-12.

- **Le responsable de la gestion documentaire**

Le responsable de la gestion documentaire élabore et tient à jour un plan de classification des documents ainsi qu'un calendrier de conservation. Il collabore avec les différents secteurs afin de rédiger les règles de conservation applicables à leurs documents. De plus, il veille au respect de celles-ci par différentes méthodes et différents systèmes. Il exerce un rôle-conseil auprès des différents secteurs du MSP. Il collabore avec le RPRP afin d'assurer le respect des exigences gouvernementales relativement à la protection des renseignements personnels. Enfin, il contribue aux travaux du CAIPRP et soulève les enjeux, les problèmes et les préoccupations liant la gestion documentaire et la protection des renseignements personnels.

- **Le gestionnaire**

Le gestionnaire doit transmettre aux employés qui relèvent de lui les orientations et les obligations concernant la protection des renseignements personnels applicables à leurs activités opérationnelles. Il s'assure que ces orientations et ces obligations sont intégrées dans leurs pratiques et leurs relations avec les clientèles, le cas échéant. Il veille au respect des délais de conservation des renseignements personnels en s'assurant de leur destruction aux moments prévus, y compris les courriels le cas échéant.

- **L'employé**

L'employé du MSP contribue au respect de ses obligations et de ses engagements à l'égard des renseignements personnels en respectant la présente politique. Il s'assure de signaler à son gestionnaire, sans délai, tout incident de confidentialité constaté en application de la procédure de gestion des incidents de confidentialité.

7. Étapes du cycle de vie d'un renseignement personnel

Collecte ou création

La collecte est la première étape du cycle de vie d'un renseignement. Elle consiste à recueillir le renseignement directement auprès de la personne concernée ou auprès d'un tiers. La collecte peut se faire directement par le ministère, par un contractant ou par un mandataire.

La création est l'action de créer un renseignement associé à une personne physique qui permet directement ou indirectement de l'identifier, par exemple un identifiant.

Le MSP ne collecte que les renseignements personnels qui sont nécessaires à l'exercice de ses attributions ou à la mise en œuvre d'un programme dont il a la gestion, sous réserve des exceptions prévues par la *Loi sur l'accès*. De plus, les mesures de sécurité et les procédures de gestion des renseignements personnels doivent être prévues avant la collecte.

Lorsque le MSP collecte des renseignements personnels auprès de la personne concernée, il l'informe des obligations prévues par la *Loi sur l'accès*, notamment :

- du nom de l'organisme public au nom de qui la collecte est réalisée;

- des fins auxquelles ces renseignements sont recueillis;
- des moyens par lesquels les renseignements sont recueillis;
- du caractère obligatoire ou facultatif de la demande;
- des conséquences pour la personne concernée ou, selon le cas, pour le tiers, d'un refus de répondre à la demande ou, le cas échéant, d'un retrait de son consentement à la communication ou à l'utilisation des renseignements recueillis suivant une demande facultative;
- des droits d'accès et de rectification prévus par la loi.

Utilisation

L'utilisation est la période pendant laquelle le renseignement personnel est utilisé par les personnes autorisées en raison du fait qu'il est nécessaire à l'exercice de leurs fonctions au sein du MSP. Il ne peut être utilisé qu'aux fins pour lesquelles il a été recueilli, sauf en cas de consentement de la personne concernée ou dans les situations prévues à la *Loi sur l'accès*.

Le MSP privilégie l'utilisation de renseignements personnels dépersonnalisés.

Communication

La communication est l'action de communiquer un renseignement personnel dans le cadre des situations prévues par la loi et aux conditions qu'elle prescrit. Cette communication peut être ponctuelle ou s'étendre sur une période en fonction de la nécessité.

La communication d'un renseignement personnel s'effectue avec le consentement de la personne concernée ou dans les cas autorisés par la *Loi sur l'accès*. Cette communication est faite de manière sécuritaire, par exemple au moyen d'une plateforme d'échange ou d'un courriel sécurisé.

De plus, lorsque cela est requis par la *Loi sur l'accès* :

- la communication est inscrite dans le registre approprié;
- une évaluation des facteurs relatifs à la vie privée doit être réalisée avant d'effectuer certaines communications sans consentement;
- une entente écrite qui prévoit les mesures de sécurité applicables aux renseignements personnels est conclue avec l'organisme receveur;
- un contrat écrit stipulant les exigences à respecter pour assurer la protection des renseignements personnels visés doit être signé.

Conservation

La conservation est la période durant laquelle le MSP conserve des renseignements personnels, sous quelque forme que ce soit, et ce, peu importe qu'ils soient activement utilisés ou non. Le MSP applique les règles de conservation approuvées par Bibliothèque et Archives nationales du Québec. De plus, il veille à ce que ces renseignements soient à jour, exacts et complets pour servir aux fins pour lesquelles ils ont été collectés.

Le MSP applique les mesures de sécurité de l'information établies par le gouvernement du Québec afin de protéger les renseignements personnels qu'il détient, pendant toute la durée de leur conservation, en s'assurant qu'elles sont raisonnables, compte tenu notamment de leur sensibilité et du contexte de leur utilisation.

Destruction

Lorsque les fins pour lesquelles un renseignement personnel a été recueilli ou utilisé sont accomplies, le MSP détruit ce renseignement. La destruction des renseignements personnels doit être sécuritaire et irréversible.

Toutefois, l'anonymisation d'un tel renseignement est possible si l'utilisation prévue par le MSP est à des fins d'intérêt public.

Le cycle de vie d'un renseignement personnel prend fin avec sa destruction.

8. Sondage

La collecte et l'utilisation de renseignements personnels dans le cadre d'un sondage doivent faire l'objet de mesures de protection particulières. Une évaluation de la nécessité de recourir au sondage doit être effectuée par le RPRP en collaboration avec le secteur visé. De plus, une évaluation de l'aspect éthique par le répondant en éthique doit être effectuée. Enfin, le secteur visé doit également présenter son projet de sondage au CAIPRP.

9. Incident de confidentialité impliquant un renseignement personnel

Lorsque le MSP a des motifs de croire que s'est produit un incident de confidentialité impliquant un renseignement personnel qu'il détient, il 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.

Après analyse de la situation, si l'incident présente un risque qu'un préjudice sérieux soit causé, le MSP doit, conformément au *Règlement sur les incidents de confidentialité*⁴ :

- aviser la Commission d'accès à l'information;
- aviser toute personne dont un renseignement personnel est concerné par l'incident;
- tenir un registre des incidents de confidentialité impliquant un renseignement personnel.

⁴ RLRQ, c. A-2.1, r. 3.1.

10. Droits de la personne concernée par un renseignement personnel

- **Droit d'accès**

Toute personne qui en fait la demande a le droit d'accéder aux renseignements personnels la concernant détenus par le MSP, sous réserve des exceptions prévues par la *Loi sur l'accès*.

- **Droit de rectification**

Toute personne qui reçoit confirmation de l'existence dans un fichier d'un renseignement personnel la concernant peut, s'il est inexact, incomplet ou équivoque, ou si sa collecte, sa communication ou sa conservation ne sont pas autorisées par la *Loi sur l'accès*, exiger que le fichier soit rectifié.

Procédure

Toute demande d'accès à des renseignements personnels et de rectification ne peut être considérée que si elle est transmise par écrit, par une personne physique autorisée par la *Loi sur l'accès*, justifiant de son identité.

Cette demande doit être adressée au RPRP du MSP à l'adresse courriel accs-info@msp.gouv.qc.ca.

11. Révision de la politique

Le MSP procède à la révision de sa politique tous les trois ans ou lors de changements significatifs qui pourraient l'affecter.

12. Entrée en vigueur

La présente politique entre en vigueur à la date de son approbation.

Original signé

Monsieur Marc Croteau
Sous-ministre

Date

Annexe 1 : Historique des modifications

PAGE	DESCRIPTION	INSTANCE	DATE
	Adoption de la politique sur la protection des renseignements personnels	GDIDRC	2023-12-18

