GOUVERNANCE ET GESTION DES RENSEIGNEMENTS PERSONNELS

AVEC VOUS POUR VOUS

TABLE DES MATIÈRES

1. Introduction

Dans l'exercice de sa mission policière et de ses activités de gestion, la Sûreté du Québec (Sûreté) recueille et traite des renseignements personnels, tant des citoyens que de ses employés.

Le présent document énonce les règles qui guident les pratiques de la Sûreté dans la gestion des renseignements personnels qu'elle détient, pendant tout leur cycle de vie, ainsi que les rôles et responsabilités de ses membres pour assurer leur protection.

2. Cadre législatif et réglementaire

Le cadre de gouvernance à l'égard des renseignements personnels de la Sûreté s'appuie sur :

- ✓ la Charte des droits et libertés de la personne;
- ✓ le Code civil du Québec;
- ✓ la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, ci-après désignée *Loi sur l'accès*;
- ✓ le Règlement sur la diffusion de l'information et sur la protection des renseignements personnels, ci-après désigné *Règlement sur la diffusion*;
- ✓ le Règlement sur les incidents de confidentialité;
- ✓ le Règlement sur les politiques de confidentialité des organismes publics recueillant des renseignements personnels par un moyen technologique;
- ✓ la Loi sur la police;
- ✓ le Règlement sur la discipline interne des membres de la Sûreté du Québec;
- ✓ le Code de déontologie des policiers du Québec;
- ✓ la Loi sur les archives;
- ✓ le Règlement sur le calendrier de conservation, le versement, le dépôt et l'élimination des archives publiques;
- ✓ la Loi sur la fonction publique;
- ✓ le Règlement sur l'éthique et la discipline dans la fonction publique;
- ✓ la Loi concernant le cadre juridique des technologies de l'information.

3. Principes directeurs

Les règles de gouvernance en vigueur à l'égard des renseignements personnels reposent sur les principes de responsabilité, de transparence, de nécessité et de confidentialité énoncés, notamment, dans la *Loi sur l'accès*.

Prenant différentes formes (politiques, instructions, procédures, guides, sections de l'Intranet, etc.), elles s'adressent à tous les employés civils et policiers de la Sûreté, quel que soit le statut ou la catégorie d'emploi qu'ils occupent, de même qu'à toute personne morale ou physique qui, par engagement contractuel ou autrement, a accès aux informations de la Sûreté.

Les règles de gouvernance s'appliquent à tous les renseignements personnels détenus par la Sûreté, incluant ceux dont la conservation est assurée par un tiers, quel que soit le support sur lequel ils sont conservés, et ce, de leur collecte à leur destruction. Elles s'appliquent également à toute personne à qui la Sûreté confie ce type de renseignements.

4. Biométrie

Dans l'exercice de sa mission policière, la Sûreté collecte, utilise et conserve des données biométriques des citoyens (ex. : images captées dans le cadre d'une enquête criminelle, ADN, empreintes digitales, photographies et autres mensurations inscrites dans les fiches signalétiques), avec ou sans leur consentement, en conformité avec plusieurs lois fédérales et provinciales, notamment :

- ✓ le Code criminel;
- ✓ la Loi sur l'identification des criminels;
- ✓ la Loi sur le casier judiciaire;
- ✓ la Loi sur la police;
- ✓ le Règlement sur les services policiers que les corps de police municipaux et la Sûreté du Québec doivent fournir selon leur niveau de compétence;
- ✓ la Loi sur les coroners;
- ✓ la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels;
- ✓ la Loi sur les archives.

La Sûreté collecte aussi certaines données biométriques (empreintes digitales et photographies) dans le cadre des vérifications de sécurité visant à assurer la fiabilité de ses employés ou des personnes qui travaillent dans ses locaux ou à

l'exécution d'un contrat auprès d'elle, ainsi que dans le cadre des vérifications ou enquêtes de sécurité effectuées pour différents ministères et organismes en application d'une loi.

S'appuyant sur le cadre légal en vigueur, plusieurs politiques internes encadrent le traitement des données biométriques et leur protection, compte tenu de leur plus haut degré de confidentialité.

En aucun cas ces données ne sont utilisées aux fins de reconnaissance faciale, c'est-à-dire pour l'identification d'un individu, ni pour réaliser des recherches automatisées auprès de la population en général.

5. Comité sur l'accès à l'information et la protection des renseignements personnels

En conformité avec la *Loi sur l'accès*, la Sûreté a mis en place un comité sur l'accès à l'information et la protection des renseignements personnels (CAIPRP), qui relève de la personne ayant la plus haute autorité au sein de l'organisation, soit la directrice générale.

La mission première du CAIPRP est de soutenir l'organisation dans l'exécution de ses obligations énoncées dans la loi et de promouvoir une culture organisationnelle qui renforce la protection des renseignements personnels et qui favorise la transparence.

Il est composé des membres de la Sûreté qui occupent les fonctions suivantes :

- Responsable de l'accès aux documents et de la protection des renseignements personnels;
- Responsable de la gestion documentaire;
- Responsable de la sécurité de l'information.

Selon les besoins, le CAIPRP peut solliciter la collaboration d'autres membres de l'organisation pour la réalisation de certaines activités ou de certains mandats les concernant.

Un suivi des activités du comité est périodiquement effectué auprès de la directrice générale afin qu'elle puisse réaliser les interventions nécessaires si l'occasion se présente.

Les responsabilités du CAIPRP, enchâssées dans la *Loi sur l'accès* et dans le *Règlement sur la diffusion*, sont les suivantes :

1. Soutenir la directrice générale dans l'exercice de ses responsabilités et dans l'exécution de ses obligations en vertu de la *Loi sur l'accès*.
2. Approuver les règles de la Sûreté encadrant la gouvernance à l'égard des renseignements personnels, dont celles en matière de sondages, et les publier.

3. Évaluer le processus interne de gestion des incidents de confidentialité, en faire le bilan et émettre des recommandations sur les incidents présentant des enjeux particuliers et sur ceux déclarés à la Commission d'accès à l'information.
4. Veiller à la sensibilisation et à la formation des membres du personnel au sujet des obligations et des pratiques en matière d'accès à l'information et de protection des renseignements personnels.
5. S'assurer que tout projet d'acquisition, de développement ou de refonte d'un système d'information ou de prestation électronique de services ou d'une technologie de vidéosurveillance impliquant la collecte, l'utilisation, la communication, la conservation ou la destruction de renseignements personnels est soumis, dès le début, à une évaluation des facteurs relatifs à la vie privée proportionnée à la confidentialité des renseignements concernés, à la finalité de leur utilisation, à leur quantité, à leur répartition et à leur support et suggérer, le cas échéant, des mesures particulières de protection.
6. Recommander la mise en place de mesures relatives à la diffusion de l'information et à la protection des renseignements personnels encadrant les activités de la Sûreté, en conformité avec les lois et règlements applicables.

6. Consentement

Toute unité de la Sûreté qui souhaite collecter, communiquer ou utiliser des renseignements personnels dans le cadre de ses activités ou de l'exécution d'un mandat ou d'un projet précis doit s'assurer d'obtenir un consentement valide de la personne concernée lorsque la *Loi sur l'accès* l'exige. Plus précisément, elle doit :

- ✓ s'assurer que la collecte est nécessaire aux fins de l'exercice des attributions de l'organisation ou de la mise en œuvre d'un programme dont elle a la gestion;
- ✓ s'assurer de la nécessité d'utiliser les renseignements personnels, car ils ont un caractère confidentiel selon la loi;
- ✓ obtenir le consentement de la personne concernée, de son représentant ou d'un tiers, sauf si la loi prévoit une exception à cette obligation;
- ✓ s'assurer que le consentement fourni est conforme aux critères de validité énoncés par la loi;
- ✓ s'assurer de rédiger le consentement conformément aux critères de validité énoncés par la loi lorsqu'il n'est pas fourni par la personne concernée ou son représentant;

- ✓ prêter assistance à la personne donnant son consentement pour l'aider à comprendre sa portée, lorsque requis;
- ✓ déclarer toute consultation, utilisation ou communication de renseignements personnels sans le consentement valide de la personne concernée, dans les cas où les lois en vigueur ne prévoient pas d'exception à cette exigence.

7. Droits de la personne concernée par un renseignement personnel

7.1 Droit d'accès

La Sûreté reconnaît le droit de toute personne d'accéder aux renseignements personnels que nous détenons à son sujet, dans la mesure prévue par la Loi sur l'accès.

La Sûreté peut, selon les motifs prévus à la Loi sur l'accès, refuser de confirmer l'existence d'un renseignement personnel concernant une personne ou en refuser l'accès en totalité ou en partie.

7.2 Droit de rectification

La Sûreté reconnaît également le droit de toute personne qui reçoit confirmation de l'existence, dans un document ou un fichier, d'un renseignement personnel la concernant, d'exiger sa rectification s'il est inexact, incomplet ou ambigu, ou si sa collecte, sa communication ou sa conservation ne sont pas autorisées par la Loi sur l'accès.

La Sûreté publie toute l'information nécessaire pour permettre à une personne de formuler une demande d'accès ou de rectification de renseignements personnels dans la section Accès à l'information de son site Web.

7.3 Droit à la portabilité

Une personne peut demander l'accès à ses renseignements personnels informatisés qu'elle a fournis directement à la Sûreté dans un format technologique structuré et couramment utilisé. Les renseignements personnels recueillis en format papier ne sont pas visés.

Le traitement de ce type de demande se fait conformément aux exigences de la Loi *sur l'accès* et des instructions internes.

8. Évaluations des facteurs relatifs à la vie privée

Afin de se conformer aux exigences de la *Loi sur l'accès,* la Sûreté a mis en place plusieurs processus internes qui prévoient la réalisation d'une évaluation des facteurs relatifs à la vie privée de tout projet organisationnel visant:

- ✓ l'acquisition, le développement et la refonte d'un système d'information ou de prestation électronique de services qui impliquent des renseignements personnels ou d'une technologie de vidéosurveillance;
- ✓ la collecte des renseignements personnels nécessaires à l'exercice des attributions ou à la mise en œuvre d'un programme de l'organisme public avec lequel la Sûreté collabore pour la prestation de services ou pour la réalisation d'une mission commune;
- ✓ la communication de renseignements personnels, sans le consentement des personnes concernées, à une personne ou à un organisme qui souhaite utiliser ces renseignements à des fins d'étude, de recherche ou de production de statistiques;
- ✓ la communication de renseignements personnels, sans le consentement des personnes concernées, conformément à l'article 68 de la *Loi sur l'accès*, soit :
  - à un organisme public ou à un organisme d'un autre gouvernement lorsque cette communication est nécessaire à l'exercice des attributions de l'organisme receveur ou à la mise en œuvre d'un programme dont cet organisme a la gestion,
  - à un organisme public ou à un organisme d'un autre gouvernement lorsque la communication est manifestement au bénéfice de la personne concernée,
  - à une personne ou à un organisme lorsque des circonstances exceptionnelles le justifient,
  - 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;
- ✓ la communication de renseignements personnels à une personne ou à un organisme à l'extérieur du Québec.

La responsabilité d'évaluer les projets organisationnels impliquant des renseignements personnels relève du CAIPRP et du Service de l'accès et de la protection de l'information.

9. Formation et sensibilisation des employés

L'aspect humain est l'une des pierres angulaires de la sécurité de l'information et de la protection des renseignements personnels.

C'est pourquoi la Sûreté offre à ses employés des activités de formation et de sensibilisation au sujet des obligations de l'organisation en matière de respect de la vie privée, d'accès et protection de l'information, des conséquences d'une atteinte à la sécurité de l'information et des rôles et responsabilités de chacun.

Ces activités revêtent différentes formes, selon le contexte et l'objectif : formation d'accueil lors de l'entrée en poste d'un nouvel employé, formations d'appoint et activités de sensibilisation diverses telles de présentations, webinaires, capsules d'information, infolettres, ateliers et rencontres d'équipes, informations sur l'intranet, etc.

10. Incidents de confidentialité

La Sûreté prend les mesures de sécurité nécessaires pour assurer la protection des renseignements personnels qu'elle détient pendant tout leur cycle de vie, soit de leur collecte jusqu'à leur destruction.

Toutefois, malgré l'adoption de mesures de sécurité adéquates, des incidents mettant en cause la confidentialité des renseignements personnels peuvent survenir (ex. : cyberattaques à nos infrastructures technologiques, erreur humaine, etc.). Afin de mitiger de tels risques pouvant causer des préjudices tant aux personnes concernées qu'à l'organisation, des mesures d'atténuation des impacts potentiels sont mises en place.

À cet effet, tous les membres de la Sûreté ont l'obligation de déclarer, avec diligence, tout incident de confidentialité impliquant des renseignements personnels, quel que soit le moment où celui-ci est survenu et que la personne en soit ou non l'auteure.

La gestion des incidents de confidentialité se fait conformément aux instructions internes qui ont été mises en place pour se conformer au Règlement sur les incidents de confidentialité.

11. Registres

Conformément à la *Loi sur l'accès*, la Sûreté tient à jour les registres suivants :

- ✓ Registre des incidents de confidentialité;
- ✓ Registre des communications de renseignements personnels, sans le consentement de la personne concernée, lorsque la Sûreté communique :

- l'identité d'une personne concernée à une personne ou à un organisme privé afin de recueillir des renseignements déjà colligés par ces derniers,
- des renseignements personnels nécessaires à l'application d'une loi au Québec, que cette communication soit ou non expressément prévue par la loi,
- des renseignements personnels nécessaires à l'application d'une convention collective, d'un décret, d'une ordonnance, d'une directive ou d'un règlement qui établit les conditions de travail,
- des renseignements personnels à un mandataire ou à un fournisseur de services dans le cadre d'un mandat ou d'un contrat de service,
- des renseignements personnels à des fins d'étude, de recherche ou de statistique,
- des renseignements personnels dans les cas visés par l'article 68 et après avoir effectué une évaluation des facteurs relatifs à la vie privée.

Ce registre, qui est publié sur le site Internet de la Sûreté, contient également :

- les ententes de collecte conclues aux fins de l'exercice des fonctions ou de la mise en œuvre d'un programme d'un organisme public avec lequel la Sûreté collabore pour la prestation de services ou la réalisation d'une mission commune;
- les utilisations de renseignements personnels au sein de la Sûreté à d'autres fins et sans le consentement de la personne concernée lorsque cette utilisation est compatible avec les fins pour lesquelles ils ont été recueillis, qu'elle est manifestement à l'avantage de la personne concernée ou qu'elle est nécessaire à l'application d'une loi au Québec.

12. Plaintes relatives à la protection des renseignements personnels

Si vous considérez que les renseignements personnels vous concernant ont été traités par notre organisation de façon non conforme à la législation applicable, nous vous invitons à nous en informer par écrit.

Adresse courriel : accesdocuments@surete.qc.ca

Adresse postale :
Service de l'accès et de la protection de l'information (UO 3210)
600, rue Fullum, bureau 1.100
Montréal (Québec) H2K 3L6

Un responsable de l'accès aux documents et de la protection des renseignements personnels (responsable de l'accès) assurera le traitement de votre plainte.

Recevabilité d'une plainte

Une plainte est recevable si :

- ✓ elle est formulée par une personne physique;
- ✓ elle concerne une insatisfaction relative à une pratique, une action ou l'inaction de la Sûreté quant à la gestion ou la protection des renseignements personnels qu'elle détient au sujet de son auteur;
- ✓ elle contient les éléments suivants :
  - Nom, prénom et coordonnées de la personne plaignante,
  - Une description suffisamment précise de la situation problématique,
  - La ou les mesures correctrices souhaitées.

Une plainte n'est pas recevable si elle :

- ✓ est anonyme;
- ✓ est abusive, frivole ou manifestement faite de mauvaise foi;
- ✓ contient des propos à caractère haineux ou diffamatoire;
- ✓ ne contient pas les informations nécessaires à son traitement (même après que des précisions ont été demandées);
- ✓ concerne une insatisfaction relative à un sujet autre que la protection des renseignements personnels.

Si une plainte est jugée non recevable par le responsable de l'accès, il informera la personne plaignante par écrit des motifs de sa décision, et ce, dans un délai maximal de 30 jours.

Si une plainte est jugée recevable, le responsable de l'accès recueillera l'ensemble des faits pertinents, procédera à son analyse, déterminera si elle est fondée ou non et, le cas échéant, décidera si des mesures correctrices ou des interventions doivent être réalisées.

13. Responsable de l'accès aux documents et de la protection des renseignements personnels

En vertu des pouvoirs et fonctions qui lui sont délégués par la directrice générale, le responsable de l'accès aux documents et de la protection des renseignements personnels de la Sûreté a la responsabilité de :

- ✓ traiter les demandes provenant des citoyens, de leurs représentants ou des médias visant l'accès à des documents organisationnels, à des renseignements personnels ou la rectification de renseignements personnels en toute autonomie et conformément aux exigences de la *Loi sur l'accès* et aux autres lois applicables;
- ✓ porter assistance à toute personne ayant effectué une demande d'accès à l'information pour l'aider à comprendre la teneur de la décision reçue;
- ✓ représenter l'organisation lors des audiences devant la Commission d'accès à l'information;
- ✓ veiller au respect des droits et obligations de la Sûreté en matière de collecte, d'utilisation, de conservation, de communication et de destruction des renseignements personnels et confidentiels;
- ✓ assurer la mise en œuvre du *Règlement sur la diffusion*.

Les noms et coordonnées des responsables de l'accès aux documents et de la protection des renseignements personnels sont disponibles dans la section Accès à l'information du site Web de la Sûreté.

14. Sécurité de l'information

L'information détenue par la Sûreté est essentielle à sa mission et à ses activités courantes. C'est pourquoi elle doit faire l'objet d'une utilisation et d'une protection adéquate durant tout son cycle de vie.

Puisque la sécurité de l'information est la responsabilité collective des individus utilisant les informations de la Sûreté ou y ayant accès, incluant ses fournisseurs et partenaires, l'organisation s'est dotée d'une politique-cadre sur la sécurité de l'information.

Cette politique précise les règles internes et les exigences en matière de gestion de la sécurité de l'information, qui comprend l'accès et la protection des renseignements personnels, la sécurité physique des personnes et des ressources informationnelles, ainsi que la continuité du service et de la gestion documentaire.

En vertu de cette politique-cadre :

- ✓ Toute entente ou tout contrat signé par la Sûreté doit comprendre une clause obligeant un fournisseur ou un tiers à s'engager à respecter les exigences organisationnelles en matière de sécurité de l'information.
- ✓ Les détenteurs d'information et des processus d'affaires sont responsables de la sécurité de ces informations lors de leur utilisation par les personnes autorisées à y accéder et de l'application des mesures de contrôle afférentes.

- ✓ Les gestionnaires concernés sont tenus d'évaluer la mise en place de contrôles afin d'assurer la protection des données. Il en résulte un suivi et des recommandations pour assurer une saine gestion des activités organisationnelles.
- ✓ La Sûreté doit maintenir l'intégrité de tout document ayant une valeur juridique nonobstant l'interchangeabilité de son support afin de préserver son admissibilité éventuelle devant les tribunaux. À cette fin, les processus, procédés et mécanismes qui encadrent la copie, le classement, la saisie, la conservation, la transmission ou le transfert de support d'un document doivent assurer le maintien de son intégrité et de sa valeur probante.
- ✓ Toute information doit être accessible et utilisable en temps voulu par une personne autorisée tout au long du cycle de vie de l'information.

Tout employé de la Sûreté a l'obligation de signaler sans tarder tout acte susceptible de représenter une violation réelle ou présumée des règles de sécurité, telle que le vol, l'intrusion dans un réseau ou un système, les dommages délibérés, l'utilisation abusive, la fraude, etc.

Suivant le processus en vigueur, chaque incident est pris en charge par l'autorité concernée afin que celle-ci y apporte les correctifs et les améliorations appropriés.

Afin de réduire les risques de commission d'un incident de sécurité, tous les membres de notre organisation ont l'obligation de participer aux activités de formation et de sensibilisation offertes en la matière.

15. Sondages impliquant des renseignements personnels

La Sûreté réalise des sondages auprès des citoyens et des employés dans différents contextes liés à sa mission et à ses activités.

Dans certains cas, les sondages peuvent impliquer la collecte de renseignements personnels des personnes qui seront sondées.

Pour assurer le respect de nos obligations en matière de protection des renseignements personnels énoncées dans la *Loi sur l'accès*, tout projet de sondage impliquant ce type de renseignements est évalué pour déterminer :

- ✓ la nécessité de la collecte de renseignements personnels dans le cadre du sondage, eu égard de à l'exercice des attributions de l'organisation ou à la mise en œuvre d'un programme qu'elle gère et, le cas échéant, de la communication de renseignements personnels à un prestataire de services;

- ✓ l'aspect éthique du sondage compte tenu, notamment, de la confidentialité des renseignements personnels recueillis et de la finalité de leur utilisation.

S'il est conclu, après cette évaluation, que la collecte de renseignements personnels est nécessaire à l'atteinte des objectifs du sondage, l'unité porteuse doit :

- ✓ privilégier l'obtention du consentement des personnes qui seront sondées;
- ✓ informer les personnes visées :
  - des fins pour lesquelles leurs renseignements personnels sont recueillis,
  - des catégories de personnes qui y auront accès,
  - du caractère volontaire de la participation au sondage,
  - des conséquences d'un refus d'y répondre;
- ✓ mettre en place les mesures de protection nécessaires pour préserver la confidentialité des participants et de leurs renseignements, même lorsque le sondage est confié à un prestataire de service.

Dans certains cas, les sondages ne visent pas la collecte de nouveaux renseignements personnels, mais la réutilisation de renseignements personnels qui ont déjà été colligés par la Sûreté dans d'autres contextes.

16. Traitement des renseignements personnels

Les renseignements personnels détenus par la Sûreté sont confidentiels et sont soumis aux règles de protection prévues par la *Loi sur l'accès* tout au long de leur cycle de vie, soit de leur collecte jusqu'à leur destruction.

16.1 Collecte de renseignements personnels

La Sûreté ne collecte que les renseignements personnels nécessaires à l'exercice de ses attributions ou à la mise en œuvre de programmes dont elle a la responsabilité.

Sauf dans les cas d'exception prévus par la loi, elle informe la personne concernée des buts poursuivis par cette collecte, de l'utilisation qui sera faite de ses renseignements personnels et de plusieurs autres éléments requis par la loi.

En cas de collecte par un moyen technologique, ces informations sont incluses dans sa politique de confidentialité.

La collecte de renseignements personnels se fait principalement dans les contextes suivants :

16.1.1 Gestion des ressources humaines

Aux fins de l'embauche du personnel civil et policier, le personnel des ressources humaines de la Sûreté ne recueille que les renseignements personnels nécessaires au traitement de l'évaluation des candidatures. Il s'agit généralement des renseignements transmis par les candidats.

Le personnel des ressources humaines recueille les renseignements nécessaires à la gestion du dossier du personnel de la Sûreté, notamment :

- les informations relatives à son emploi;
- ses coordonnées;
- son assiduité;
- les événements liés à la formation et au développement professionnel, à la santé et sécurité au travail, à sa performance et à sa rémunération.

16.1.2 Opérations et enquêtes policières

La Sûreté collecte des renseignements personnels dans le cadre de certaines activités liées directement à la mission policière, telles que les enquêtes criminelles, les interpellations policières ou les interceptions routières, qui sont prévues et encadrées par plusieurs lois fédérales et provinciales (ex. : *Code de la sécurité routière*, *Loi sur l'identification des criminels*, *Loi sur le casier judiciaire*, *Loi sur la police*, *Code criminel*, etc.).

16.1.3 Traitement des demandes reçues par l'entremise du site Internet de la Sûreté

La Sûreté permet aux citoyens de faire des demandes d'information, de services en ligne, d'assistance ou de soutien à partir de son site Internet (ex. : obtenir de l'information sur l'organisation, demander un permis d'explosifs, déposer une plainte à la suite d'un événement afin que la Sûreté en fasse enquête, etc.).

Le personnel concerné recueille les renseignements nécessaires pour prêter le service ou le soutien demandé. Il s'agit généralement des renseignements d'identification (nom, date de naissance, coordonnées), de l'objet de la demande et des informations concernant une situation ou un événement précis.

16.1.4 Traitement des demandes d'accès à l'information

La Sûreté collecte les renseignements personnels transmis par toute personne qui adresse une demande d'accès à l'information.

Il s'agit généralement de ses coordonnées, de sa date de naissance, l'objet de la demande, des informations concernant le contexte de l'intervention

policière ou de la demande d'accès et d'une pièce d'identité avec photo et signature.

La reproduction de la pièce d'identité qui accompagne une demande d'accès est détruite une fois que l'identité de la personne a été vérifiée.

Le nom d'une personne physique qui a transmis une demande d'accès à la Sûreté est un renseignement personnel qui est accessible seulement aux personnes impliquées dans le traitement de la demande.

16.1.5 Traitement des plaintes relatives à la qualité des services et à la protection des renseignements personnels

La Sûreté collecte les renseignements personnels transmis par les plaignants pour le traitement d'une plainte relative à la qualité des services offerts et à la protection de leurs renseignements personnels. Il s'agit généralement des renseignements tels que leurs coordonnées, l'objet de leur plainte, etc.

16.2 Utilisation des renseignements personnels

La Sûreté s'assure que les renseignements personnels qu'elle détient sont à jour, exacts et complets pour servir aux fins pour lesquelles ils sont recueillis.

Ces renseignements ne sont utilisés que pour les fins indiquées lors de leur collecte.

Pour toute autre utilisation, le consentement de la personne concernée est demandé, sauf dans les cas d'exception prévus par la *Loi sur l'accès*.

Chaque membre de la Sûreté :

- ✓ accède à l'information exclusivement selon les droits d'accès mis à sa disposition et dans l'exercice de ses fonctions;
- ✓ catégorise et applique le niveau de confidentialité à toute information mise à sa disposition ou dont il dispose, tout en prenant les moyens de sécurité nécessaires;
- ✓ limite l'utilisation de l'actif informationnel aux fins pour lesquelles il est destiné;
- ✓ signale à son supérieur immédiat toute atteinte ou toute tentative d'atteinte à la sécurité de l'information dont il a connaissance;
- ✓ participe aux activités de sensibilisation de la sécurité de l'information établies par la Sûreté.

Les gestionnaires de la Sûreté ont la responsabilité de gérer et de valider les droits d'accès de son personnel aux locaux, aux systèmes, aux bases de données, aux courriels, aux collecticiels, aux services d'Internet et à l'Intranet

en fonction des tâches de celui-ci et conformément aux autorisations accordées par les détenteurs.

16.3 Communication des renseignements personnels

Avec le consentement des personnes concernées

Dans le cadre de sa mission policière, la Sûreté est appelée à communiquer à d'autres personnes ou organismes des renseignements personnels qu'elle détient avec le consentement des personnes concernées, par exemple, dans le cadre des enquêtes de sécurité des personnes candidates pour un poste au sein d'un organisme public ou du traitement d'une demande d'accès à l'information.

Cette communication se fait uniquement lorsque le consentement de la personne est jugé conforme aux exigences de la *Loi sur l'accès* (voir la section sur le consentement).

Sans le consentement des personnes concernées

La Sûreté traite un grand nombre de demandes provenant d'autres organismes visant l'obtention de renseignements personnels (ex. : rapports d'événement ou d'enquête). Dans la plupart des cas, ces demandes ne sont pas accompagnées du consentement de la personne concernée et sont faites dans le cadre d'application d'une loi au Québec.

La Sûreté met à la disposition des demandeurs toute l'information nécessaire pour formuler une demande de renseignements aux fins d'application d'une loi au Québec afin qu'elle puisse être traitée conformément aux exigences de la *Loi sur l'accès* et autres lois sectorielles. Cette information est disponible dans la section Accès à l'information du site Web de la Sûreté.

Bien que l'obtention du consentement de la personne concernée demeure l'option privilégiée pour procéder à une communication de renseignements personnels à un tiers, certains cas d'exception prévus par la loi permettent à la Sûreté de le faire sans le consentement de la personne, notamment les suivants :

16.3.1 Dans le cadre d'une équipe mixte

La Sûreté collabore avec diverses organisations dans le but d'atteindre des objectifs communs. Dans un tel contexte, le partage de renseignements personnels s'avère parfois nécessaire.

Notre organisation s'assure que l'échange de renseignements personnels des personnes visées par les interventions des équipes mixtes (Sûreté et autres organismes) se fait dans le respect du cadre légal applicable et que les intervenants impliqués sont sensibilisés aux différents aspects des droits fondamentaux en matière de vie privée.

16.3.2 Dans le cadre d'une entente

D'autres contextes opérationnels impliquant l'échange de renseignements entre la Sûreté et d'autres organismes peuvent justifier le recours à une entente de communication de renseignements personnels.

Avant de signer ce type d'entente, la Sûreté s'assure que la communication des renseignements visés est nécessaire pour que les parties signataires puissent se conformer aux lois applicables et atteindre un objectif légitime, important et plus utile à l'organisation que préjudiciable aux personnes concernées.

Lorsque le critère de nécessité est satisfait, la Sûreté veille à ce que l'entente respecte toutes les exigences légales en matière de protection des renseignements personnels et à ce que celles-ci soient connues et appliquées par les acteurs concernés au sein de l'organisation.

16.3.3 Dans le cadre d'un mandat ou d'un contrat de biens ou de services

La Sûreté communique à certaines personnes ou à certains organismes des renseignements personnels qu'elle détient, sans le consentement des personnes concernées, pour leur permettre de réaliser un mandat ou d'exécuter un contrat de biens ou de services.

Tout mandat ou contrat confié à un tiers inclut des exigences concernant la protection des renseignements personnels, dont des clauses prévoyant l'obligation de déclarer toute violation ou tentative de violation d'une obligation relative à la confidentialité des données en jeu.

16.3.4 Dans une situation d'urgence ou afin de prévenir un acte de violence

Dans certaines situations d'urgence mettant en danger la vie, la santé ou la sécurité d'une personne, les policiers de la Sûreté peuvent juger nécessaire de communiquer à un tiers des renseignements personnels la concernant, sans son consentement.

Notre organisation offre à ses membres des outils pour les aider à identifier dans quelles situations il est approprié de procéder à cette communication et à déterminer quoi faire en cas de doute.

16.3.5 À des fins d'étude, de recherche ou de production de statistiques

La Sûreté encourage l'avancement de la connaissance en matière d'administration et d'opérations policières en participant à des projets de recherche, tant externes qu'internes. Dans certains cas, les projets impliquent la communication de renseignements personnels détenus par notre organisation, sans le consentement des personnes concernées.

Étant donné que ces renseignements sont confidentiels selon la *Loi sur l'accès,* leur communication à cette fin est conditionnelle à l'obtention d'une évaluation favorable des facteurs relatifs à la vie privée.

La Sûreté encourage toutefois les chercheurs à collecter des renseignements personnels anonymisés ou dépersonnalisés pour diminuer les risques d'atteinte à la vie privée des personnes concernées.

Lorsque cela n'est pas possible, la communication des renseignements personnels est encadrée par une entente écrite qui prévoit les mesures à mettre en place pour assurer leur protection. Cette entente est transmise à la Commission d'accès à l'information avant son entrée en vigueur.

Les étapes à suivre pour déposer une demande de projet de recherche à la Sûreté ainsi que les objectifs et les principes sous-jacents au déploiement des activités de recherche au sein de l'organisation sont détaillés dans le document Dépôt d'une demande de projet de recherche à la Sûreté du Québec.

Les études et recherches réalisées par des membres de notre organisation sont publiées dans la section Publications du site Web de la Sûreté.

La Sûreté inscrit au Registre des communications de renseignements personnels tous ces types de communications.

La Sûreté s'assure également de former et de sensibiliser ses membres au sujet de l'importance de connaître les précautions à prendre pour s'assurer d'une communication de renseignements personnels conforme au cadre légal et aux instructions internes en vigueur.

16.4 Conservation des renseignements personnels

La Sûreté reconnaît à l'information sa pleine valeur en tant que ressource essentielle pour l'organisation, permettant d'optimiser le processus décisionnel au même titre que les ressources humaines, financières ou matérielles.

Chaque unité de la Sûreté est propriétaire de l'information créée ou reçue dans le cadre de ses activités et en est pleinement responsable jusqu'à sa destruction ou son versement à Bibliothèque et Archives nationales du Québec (BAnQ).

Chaque employé est responsable de gérer, protéger, classifier et classer judicieusement l'information en fonction de sa nature, de ses caractéristiques et de sa valeur.

Afin de respecter ses obligations légales en matière de gestion des documents découlant notamment de la *Loi sur les archives* et de la *Loi sur l'accès*, l'actif documentaire administratif de la Sûreté est coordonné à l'échelle de l'organisation à travers une méthode de gestion intégrée des documents (GID).

Le système de GID est un système qui garantit la disponibilité, l'intégrité, la confidentialité, l'authenticité et l'irrévocabilité des documents tout au long de leur cycle de vie en dictant des méthodes et des techniques précises de classification, d'identification, de classement et déclassement, d'entreposage et de destruction ou versement.

Pour atteindre ces objectifs, la Sûreté s'est dotée d'un plan de classification et d'un calendrier de conservation.

Le Service de l'accès et de la protection de l'information, également responsable de la gestion des documents, fait la promotion des pratiques normalisées en gestion des documents auprès des responsables des différentes unités de l'organisation.

16.5 Destruction des renseignements personnels

La Sûreté s'assure de détruire de manière sécuritaire les renseignements personnels qu'elle détient lorsque les finalités pour lesquelles ils ont été collectés sont atteintes, sous réserve des délais prévus à son calendrier de conservation.

Les documents dont le mode de disposition prévu au calendrier de conservation est la destruction doivent être détruits le plus tôt possible après l'expiration du délai prévu au calendrier de conservation et dans le respect des instructions en vigueur.

Dans tous les cas, la destruction doit toujours être réalisée ou supervisée par un employé de la Sûreté.

Les documents en attente de destruction doivent être entreposés de manière sécuritaire, de façon à ce que leur accès soit restreint aux personnes autorisées.

17. Vérification interne

À la Sûreté, l'unité responsable de la vérification interne effectue notamment des examens sur l'efficacité des contrôles présents dans les activités de l'organisation, y compris la protection de l'information et des renseignements personnels. Plus précisément, l'unité responsable de la vérification interne :

- ✓ exerce un rôle stratégique dans la reddition de comptes en matière d'accès et de protection d'information, plus particulièrement en regard de l'identification, de l'évaluation et de la gestion des risques d'atteinte à la protection des renseignements personnels;
- ✓ procède périodiquement à une vérification des mesures de sécurité de l'information, dont celles visant la protection des renseignements personnels, afin de s'assurer de leur efficacité;

- ✓ formule des recommandations aux autorités de la Sûreté en matière de protection des renseignements personnels et de sécurité physique, opérationnelle et documentaire afin de protéger les ressources informationnelles;
- ✓ effectue le suivi des recommandations et des mesures correctives retenues.

18. Vidéosurveillance

Consciente des enjeux en matière de respect de la vie privée liés à la vidéosurveillance, la Sûreté limite son utilisation aux fins de lutte contre la criminalité et le terrorisme ainsi que de protection des personnes, des biens et de l'information confidentielle, et ce, dans le respect des lois fédérales et provinciales en vigueur (ex. : *Charte des droits et libertés de la personne*, *Code civil du Québec*, *Code criminel*, *Loi sur l'identification des criminels*, *Loi sur le casier judiciaire*, *Loi sur la police*, *Loi sur l'accès*, etc.). Dans la plupart des cas, la surveillance vidéo se fait avec l'autorisation d'un juge.

La Sûreté ne fait pas de surveillance générale et systématique des personnes qui se trouvent dans les lieux publics.

La Sûreté du Québec collecte des images des citoyens à l'aide des caméras portatives qui sont utilisées par les policiers qui desservent les municipalités régionales de comté de Rimouski-Neigette, de La Vallée-de-l'Or, de Beauharnois-Salaberry et de Drummond. Ces caméras ont été déployées dans le cadre du projet pilote sur l'utilisation des caméras portatives, approuvé par le ministère de la Sécurité publique.

Toute communication de renseignements recueillis par un système de vidéosurveillance doit être faite conformément aux exigences des lois qui s'appliquent, dont la *Loi sur l'accès*.

Les images collectées sont conservées dans un environnement protégé à accès restreint et pendant la durée prévue au calendrier de conservation en vigueur à la Sûreté selon le contexte et la finalité de leur collecte.

SÛRETÉ DU QUÉBEC
POLICE
SERVICE INTÉGRITÉ JUSTICE

AVEC VOUS
POUR VOUS