

GUIDE SUR L'ACCÈS AUX DOCUMENTS ET SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

**SERVICE DE POLICE DE
L'AGGLOMÉRATION DE LONGUEUIL**

Septembre 2022



Service de police
AGGLOMÉRATION DE LONGUEUIL

longueuil

TABLE DES MATIÈRES

Section 1 – L'accès aux documents	3
1. Qu'est-ce que le droit d'accès aux documents des organismes publics?	3
2. Quel est le rôle de l'équipe – Loi d'accès aux documents?	3
3. Quels sont les impacts de la Loi sur l'exercice de vos fonctions?	4
Section 2 – La protection des renseignements personnels	5
1. Qu'est-ce qu'un renseignement personnel?	5
2. Qu'est-ce qu'un incident de confidentialité?	5
3. Comment prévenir les incidents de confidentialité?	5
4. Quelques exemples d'un incident de confidentialité	6
5. Comment signaler un incident de confidentialité?	7
6. Comment se déroule le signalement des incidents?	7
7. J'ai des questions, à qui puis-je m'adresser?	7
8. En conclusion	7

SECTION 1 - L'ACCÈS AUX DOCUMENTS

1. Qu'est-ce que le droit d'accès aux documents des organismes publics?

À titre de corps de police, le Service de police de l'agglomération de Longueuil (ci-après « le SPAL ») est un organisme public soumis à la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (RLRQ, c. A-2.1) (ci-après « la Loi »). Les dispositions de cette loi s'appliquent aux documents détenus par un organisme public dans l'exercice de ses fonctions, que leur conservation soit assurée par l'organisme lui-même ou par un tiers.

La Loi s'applique, quelle que soit la forme de ces documents :

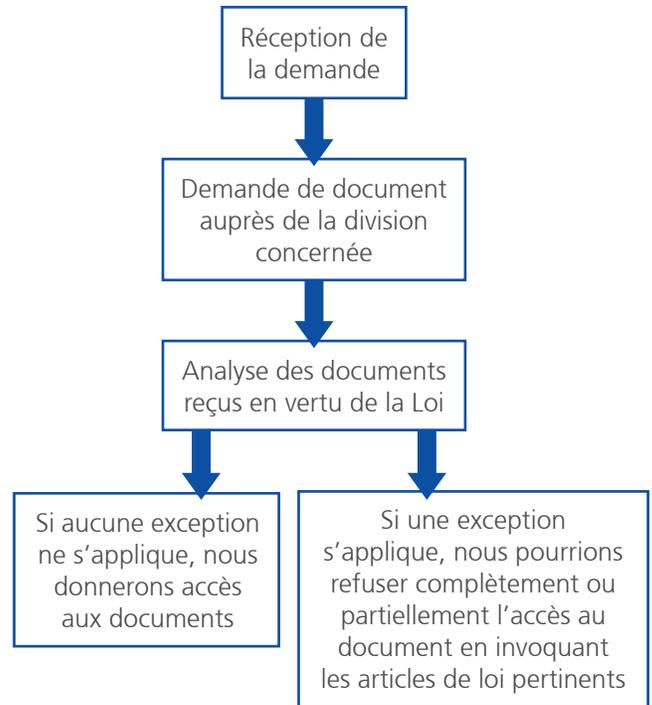
- Écrite;
- Graphique;
- Sonore;
- Visuelle;
- Informatisée;
- Autre.

En vertu de l'article 9 de la Loi, toute personne qui en fait la demande a droit d'accès aux documents d'un organisme public. C'est le premier objectif de la Loi. Ce droit n'est pas absolu, la Loi prévoit certaines exceptions. Cependant, partons du principe que tout est public.

2. Quel est le rôle de l'équipe – Loi d'accès aux documents?

Voici le processus d'une demande d'accès à l'information :

1. L'équipe – Loi d'accès reçoit les demandes d'accès aux documents. Un délai de 20 jours (non ouvrables) est prévu à la Loi pour y répondre.
2. L'équipe communique avec la direction, la section, l'équipe ou le service concerné afin d'obtenir les documents visés par la demande.
3. Une fois reçus, les documents sont analysés en vertu de la Loi. C'est alors qu'il sera décidé si le document peut être transmis ou non et si des renseignements doivent être caviardés.



Il est important de ne pas induire le requérant en erreur en l'informant que l'équipe – Loi d'accès lui fournira la documentation demandée. Il faut plutôt référer le requérant vers l'équipe – Loi d'accès en l'informant qu'une analyse sera faite suivant sa demande afin de déterminer si le SPAL détient la documentation et si elle est accessible, en tout ou en partie.



Lorsque l'équipe – Loi d'accès vous demande un document, **vous avez l'obligation de le fournir, et ce, peu importe la nature du document.** Vous devez informer l'équipe des incidences possibles de la divulgation du document selon votre connaissance. C'est le responsable qui fera l'analyse légale permettant de conclure si le document est accessible ou non, après vous avoir consulté.

L'équipe – Loi d'accès ne traite pas les demandes d'information. La réponse à une demande consiste à fournir les documents existants, dans la mesure où leur transmission est autorisée par la Loi.

3. Quels sont les impacts de la Loi sur l'exercice de vos fonctions?

En tant qu'employé d'un organisme public, il est important de comprendre les impacts de cette loi.

- La Loi ne prévoit pas de notion de document interne, confidentiel ou protégé. Une mention en ce sens sur un document vise à restreindre sa communication au sein du SPAL mais ne le soustrait pas à l'application de la Loi.
 - Dès qu'un document est créé, il est susceptible d'être accessible au public. Vos courriels, échanges Teams et toutes autres communications peuvent être accessibles. **Il faut donc être prudent.**
 - Lorsque vous discutez avec un requérant, il ne faut jamais divulguer de renseignements personnels d'un tiers.
 - En tant qu'employé du SPAL, vous avez accès à des documents contenant des informations et des renseignements sensibles. Toute transmission de documents à un tiers doit passer par l'équipe – Loi d'accès. En cas de doute, n'hésitez pas à communiquer avec l'équipe.
 - Vous n'avez pas à créer de document ni à procéder à des calculs ou à des comparaisons de renseignements pour répondre à une demande d'accès. Ainsi, si l'information n'est pas disponible dans un document existant ou si des calculs sont nécessaires pour l'obtenir, veuillez en informer l'équipe – Loi d'accès, qui pourra alors refuser la demande.
 - Le fait d'extraire des données d'un système informatique afin de récupérer les renseignements ne constitue pas la création d'un document. Le droit d'accès oblige l'organisme à extraire les données visées (ex. : statistiques) qui sont détenues dans une base de données lorsque l'opération nécessite une simple extraction.
 - Vous devez respecter le délai de 10 jours calendrier pour fournir les documents suite à une demande de repérage, afin qu'une réponse puisse être transmise au requérant avant l'expiration du délai de 20 jours prévu à la Loi. Le défaut de répondre dans le délai est réputé être un refus d'accès, ce qui donne ouverture au recours en révision devant la Commission d'accès à l'information (CAI).
- Lorsqu'un requérant conteste la décision du responsable d'accès, le dossier sera entendu devant la CAI. Vous pourriez alors être appelé à témoigner. Conservez des traces des démarches effectuées pour le repérage des documents.

SECTION 2 - LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

1. Qu'est-ce qu'un renseignement personnel?

Les renseignements personnels sont ceux qui portent sur une personne physique et qui permettent de l'identifier, directement ou indirectement. Ils sont confidentiels. Sauf exception, ils ne peuvent être communiqués sans le consentement de la personne concernée.

Les organismes publics ont des obligations à respecter à chaque étape du cycle de gestion d'un renseignement personnel :

- **À la collecte ou à la création** : Recueillir les renseignements personnels nécessaires et informer la personne concernée des fins auxquelles les renseignements sont recueillis;
- **À l'utilisation** : Utiliser les renseignements personnels seulement aux fins pour lesquelles ils ont été recueillis et prendre connaissance des renseignements personnels que lorsqu'ils sont nécessaires aux fonctions exercées;
- **À la communication** : Ne communiquer les renseignements personnels qu'avec le consentement de la personne concernée ou lorsque permis par la Loi;
- **À la conservation** : Conserver les renseignements personnels à jour, exacts et complets pour servir aux fins auxquelles ils ont été recueillis et utilisés;
- **À la destruction** : Détruire les renseignements personnels lorsque les fins ont été accomplies sous réserve de la Loi sur les archives (calendrier de conservation);
- **En tout temps**, prendre les mesures de sécurité propres à assurer la protection des renseignements personnels.

2. Qu'est-ce qu'un incident de confidentialité?

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

Cela vise toute divulgation illégale de renseignements personnels ou leur accès par une personne non autorisée, peu importe le support sur lequel les renseignements se trouvent (papier, électronique, etc.). Cet incident peut être intentionnel ou accidentel, et peut être le fait d'un employé de l'organisme ou de toute autre personne. Une divulgation non autorisée par la Loi ou par la personne concernée constitue une divulgation illégale.

*Se référer à la définition de renseignements personnels dans le guide.

3. Comment prévenir les incidents de confidentialité?

Des moyens administratifs et technologiques sont mis en place pour que le traitement des renseignements personnels se fasse dans le respect des lois applicables. Malgré ces moyens, le risque d'un bris de confidentialité demeure. En effet, aucune mesure de prévention ou de sécurité ne saurait garantir une étanchéité exempte de toute erreur ou de malversation (ex. : erreur lors de l'envoi de courrier ou par courriel, piratage informatique, perte ou vol de documents ou d'un ordinateur portable).

Nous avons donc adopté une stratégie d'intervention en cas d'incident de confidentialité dans le but de limiter les conséquences fâcheuses ou préjudiciables pour la personne concernée. Le but est également d'instaurer immédiatement des mesures correctives afin d'éviter qu'une situation se généralise ou se répète.

4. Quelques exemples d'un incident de confidentialité

Obligation légale non respectée	Incident
Accès non autorisé à un renseignement personnel	<p>Employé du SPAL qui utilise le CRPQ (Centre de renseignements policiers du Québec) à des fins personnelles.</p> <p>Employé du SPAL qui consulte un dossier opérationnel à des fins personnelles ou par curiosité.</p> <p>Employé du SPAL qui ne respecte pas le délai d'accès concernant le dossier d'un mineur en vertu de la LSJPA (article 118 de la Loi sur le système de justice pénale pour les adolescents).</p>
Utilisation non autorisée d'un renseignement personnel	<p>Policier qui utilise une adresse courriel prise dans un rapport d'événement à d'autres fins que celles pour laquelle le renseignement a été recueilli (ex. : infolettre pour de la sensibilisation).</p>
Communication non autorisée d'un renseignement personnel	<p>Policier qui juge qu'un individu a besoin d'aide et qui prend la décision de communiquer avec son médecin, sans qu'il y ait danger pour lui-même et pour autrui et sans le consentement de l'individu.</p> <p>Employé qui transmet de l'information sur les démarches effectuées dans le cadre d'une enquête en cours à un assureur, et ce, sans le consentement de l'assuré.</p> <p>Employé qui transmet par erreur un courriel à un mauvais destinataire et dans lequel il y avait une pièce jointe (ex. : résultat d'une vérification des antécédents judiciaires, billet médical, documents de retraite, etc.).</p>
Perte d'un renseignement personnel ou autre	<p>Employé qui oublie son porte-document avec des comptes-rendus d'enquête dans un endroit public ou chez un ami.</p> <p>Policier qui va à la cour et qui oublie son rapport d'enquête sur un banc du Palais de justice.</p> <p>Employé qui s'aperçoit que son ordinateur est victime d'une cyberattaque.</p>

SECTION 2 - LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

5. Comment signaler un incident de confidentialité?

Deux méthodes sont en place pour le signalement des incidents :

- Par courriel à l'adresse incident.confidentialite@longueuil.quebec
- Par téléphone au 7111 si un système informatique est en cause

Dans tous les cas, le signalement de l'incident parviendra à la Responsable de l'accès et de la protection des renseignements personnels du SPAL, madame Mélanie Coutu.

Lors du signalement d'un incident de confidentialité, veuillez indiquer le plus de détails possible pour nous permettre de gérer adéquatement l'incident. Au besoin, nous communiquerons avec vous.

Important - Tout incident de confidentialité doit obligatoirement être signalé.

6. Comment se déroule le signalement d'un incident?

Certains incidents de confidentialité seront détectés par les outils informatiques (ou équipes TI) et d'autres seront détectés par les employés, les fournisseurs de services, etc. Nous avons donc besoin de la collaboration de tout un chacun afin que les incidents soient signalés dès qu'une personne en a connaissance.

Il faut se référer à la définition d'un incident de confidentialité pour déterminer s'il s'agit d'un incident au sens de la Loi : il faut conclure que des renseignements personnels sont impliqués dans l'incident, ce qui sera parfois impossible à affirmer au jour 1. Dans le doute, faites le signalement.

7. J'ai des questions, à qui puis-je m'adresser?

Madame Mélanie Coutu
Responsable de l'accès et de la protection des renseignements personnels du SPAL

Par courriel : # police loi d'accès aip@longueuil.quebec
Par courriel à melanie.coutu@longueuil.quebec
Par téléphone au 450 463-7100, poste 2701

8. En conclusion

La gestion et le signalement des incidents de confidentialité sont une nouvelle obligation introduite dans la Loi sur l'accès. Il est donc essentiel que la Ville ainsi que tous les employés s'y conforme, car en cas de non-respect de la Loi, des amendes et des sanctions pénales sévères pourraient être appliquées.

Notre objectif est d'agir de façon préventive pour faire cesser l'incident ou corriger une pratique inadéquate pour nous améliorer et mieux encadrer la protection des renseignements personnels et non pas dans un but de répression.

