Guide de l'employé en matière de protection des renseignements personnels – Municipalité de Nantes

(le « Guide »)

Table des matières

Préface

Objet du Guide. Le Guide vise à établir les bonnes pratiques en matière de protection des renseignements personnels (tels que ci-après définis) pour tous les employés de la Municipalité ayant accès à de tels renseignements personnels dans le cadre de l'exercice de leurs fonctions au sein de la Municipalité (les « **Employés** »).

Responsable de l'application de Guide. Pour toute question ou tout commentaire en lien avec le Guide et son contenu, les Employés sont invités à communiquer directement avec le responsable de la protection des renseignements personnels au sein de la Municipalité, à savoir le directeur général (le « **Responsable** »).

Nature du Guide. Le Guide constitue une directive administrative entérinée par le conseil municipal. Toute conduite d'un Employé qui s'avère dérogatoire aux bonnes pratiques consacrées dans le Guide est susceptible de mener à l'infliction de sanctions disciplinaires à l'Employé concerné.

Importance de la protection des renseignements personnels. La Municipalité est responsable de la protection des renseignements personnels qui lui sont confiés dans le cadre de l'exercice de ses fonctions. La Municipalité compte sur la discipline et la rigueur des Employés pour protéger ces renseignements personnels et ainsi éviter les sanctions importantes prévues par la législation applicable en cas de manquement, lesquelles peuvent prendre la forme de pénalités pécuniaires significatives pour la Municipalité.

1. Comment reconnaître un renseignement personnel ?

Définition. Un renseignement personnel est un renseignement qui permet, seul ou conjointement avec d'autres renseignements, d'identifier une personne physique (un particulier) de façon directe ou indirecte. Par exemple sont des renseignements personnels : le prénom, le nom, les adresses civiques, les adresses électroniques, les numéros de téléphone, l'âge, l'origine ethnique, l'état matrimonial, les numéros de cartes de crédit et le numéro d'assurance sociale d'une personne physique donnée. Un renseignement personnel peut être recueilli directement auprès de la personne concernée (ex : à l'occasion d'un appel téléphonique ou en remplissant un formulaire sur un site web), créé (ex : la Municipalité attribue un numéro d'identification unique à un client) ou inféré.

Renseignement personnel « sensible ». Un renseignement personnel peut être considéré « sensible ». Un renseignement personnel est dit « sensible » s'il « suscite un haut degré d'attente raisonnable en matière de vie privée. » Un renseignement personnel peut être sensible par sa nature même ou en raison d'un contexte particulier (ex : dossier de la DPJ, informations sur le divorce, garde partagée…). Les renseignements de santé (ex. dossier médical, handicap, diagnostics…), biométriques (ex. l'iris, la paume de la main, des empreintes digitales…), financiers (ex. salaire, numéro de compte en banque…) et le numéro d'assurance sociale sont généralement considérés comme étant sensibles par leur nature même. Tel qu'il sera démontré, les renseignements dits « sensibles » méritent d'être davantage sécurisés

2. Bonnes pratiques en matière de collecte de renseignements personnels

2.1. Collecte de renseignements personnels

Définition. Un Employé recueille des renseignements personnels au bénéfice de la Municipalité lorsqu'il :

- Procède à la collecte directe auprès de la personne concernée (par exemple, lors d'un entretien téléphonique ou d'un échange de courriels);
- Procède à la collecte indirecte auprès d'une personne autre que la personne concernée (par exemple, lorsqu'un tiers communique des documents contenant des renseignements personnels à un Employé);
- Crée un renseignement personnel à l'égard d'une personne concernée (par exemple, lorsqu'un Employé attribue un numéro exclusif à une personne concernée afin de l'identifier au sein d'une base de données de la Municipalité); ou
- Infère un renseignement personnel d'une personne concernée à partir d'autres renseignements de cette personne (par exemple, un rapport d'inspection ou la confirmation que des plaintes ont été reçues peut permettre d'inférer qu'un propriétaire est non conforme).

Lignes directrices en matière de collecte. Avant de procéder à toute collecte de renseignements personnels, un Employé doit :

- Déterminer les fins de la collecte ;
- Limiter sa collecte aux renseignements personnels nécessaires à celles-ci ; et
- obtenir le consentement des personnes concernées.

Les sections 2.1.1 à 2.1.3 ci-après contiennent des explications sur chacune des lignes directrices susmentionnées.

2.1.1. Déterminer les fins de la collecte

Définition. Avant toute collecte de renseignements personnels, un Employé doit indiquer de façon claire à la personne concernée les raisons pour lesquelles de tels renseignements personnels doivent être recueillis par la Municipalité.

Exemple pratique. La Municipalité doit recueillir et conserver le numéro d'assurance sociale d'un nouvel employé pour permettre à ce dernier d'accéder à certains programmes et prestations gouvernementaux, entre autres. Les fins de la collecte du numéro d'assurance sociale sont donc clairement établies : cette collecte est dictée par la loi et elle permet au nouvel employé de bénéficier de programmes et prestations gouvernementales. En

conséquence, les Employés du département des ressources humaines de la Municipalité seraient justifiés de procéder à la collecte d'un tel renseignement personnel auprès d'un nouvel employé.

Identifier et documenter les fins. Les fins de la collecte de **chaque type** de renseignement personnel doivent être identifiées et **documentées** par les Employés avant que de tels renseignements personnels puissent être collectés, car celles-ci ont une incidence sur :

- La légalité de la collecte des renseignements personnels ;
- Les informations devant être communiquées à la personne concernée lors de la collecte ;
- La validité du consentement à la collecte des renseignements personnels ;
- L'utilisation que l'organisation pourra effectuer des renseignements personnels ; et
- Le délai de conservation des renseignements personnels.

Un tableau résumant (i) les différents types de renseignements personnels qu'un Employé est autorisé à recueillir au bénéfice de la Municipalité et (ii) les fins primaires inhérentes à la collecte de chaque type de renseignement personnel, est joint au Guide à titre d'Annexe « A » pour en faire partie intégrante.

Utilisation et communication. Les Employés doivent utiliser les renseignements personnels détenus par la Municipalité aux seules fins requises pour exécuter leur prestation de travail au bénéfice de cette dernière, sous la supervision ou selon les instructions de leur supérieur immédiat ou du Responsable. **Les Employés ne sont autorisés à procéder à aucune communication de renseignements personnels, à moins d'avoir obtenu le consentement préalable écrit du Responsable ou de la personne déléguée, le cas échéant.**

Exemple pratique. Un Employé reçoit un appel téléphonique d'une personne qui prétend être un ami de l'un de ses collègues. Cette personne demande à l'Employé de lui fournir des renseignements relatifs à l'horaire de travail de son collègue au cours la semaine prochaine, sous le prétexte de l'organisation d'une fête surprise. L'Employé ne doit pas donner suite à la demande en question et référer son interlocuteur au courriel du Responsable.

2.1.2. Limiter la collecte aux renseignements personnels nécessaires pour les fins identifiées

Les Employés doivent garder à l'esprit que toute collecte de renseignements personnels doit être **nécessaire** à l'accomplissement des fins identifiées. **La loi ne permet pas de recueillir un renseignement personnel qui n'est pas nécessaire à l'exercice des fonctions de la Municipalité, même si la personne concernée consent à cette collecte**.

Plus qu'utile, mais moins qu'essentiel. La collecte d'un renseignement personnel ne doit pas forcément s'avérer essentielle aux activités de la Municipalité. En revanche, la collecte doit s'avérer plus que simplement utile à ces activités. Ainsi, les Employés doivent faire preuve de prudence et diligence dans leur utilisation. Informer convenablement les personnes concernées

Informations à communiquer. Au moment de la collecte de renseignements personnels auprès d'une personne concernée, les Employés doivent communiquer à celle-ci les informations suivantes, et ce, en termes simples et clairs :

1. Les fins auxquelles les renseignements personnels sont recueillis ;
2. Les moyens par lesquels les renseignements personnels sont recueillis ;
3. Le nom du tiers pour qui la collecte est faite, le cas échéant ;
4. Le nom des catégories de tiers à qui il est nécessaire de communiquer les renseignements personnels au regard des fins pour lesquelles ceux-ci sont recueillis, le cas échéant ;

Droit de la personne concernée. Toute personne concernée par des renseignements personnels détenus par la Municipalité bénéficie du droit d'obtenir les informations suivantes :

1. Tous les renseignements personnels qui la concernent, sauf exceptions prévues par la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (ci-après : la « **Loi** ») ;
2. Les catégories de personnes qui ont accès à ces renseignements au sein de la Municipalité ;
3. La durée de conservation de ces renseignements personnels ; et
4. Les coordonnées du Responsable.

Un Employé qui reçoit une demande d'informations en lien aux points 1 à 4 menant à une communication de renseignements personnels détenus par la Municipalité à la personne concernée doit acheminer cette demande sans délai au Responsable. **Pour fins de précision, seul le Responsable de l'accès aux documents et à la protection des renseignements personnels est autorisé à traiter une telle demande.**

2.1.3. Obtenir le consentement des personnes concernées

2.1.3.1. Validité du consentement

Consentements requis pour l'utilisation et la communication. Toute utilisation et communication de renseignements personnels doit faire l'objet d'un consentement valide de la part de la personne concernée.

Critères de validité du consentement. Pour être valide, un consentement doit respecter les critères suivants :

- Le consentement doit être **manifeste ;**
- Le consentement doit être **libre ;**
- Le consentement doit être **éclairé ;**
- Le consentement doit être **granulaire ;**
- Le consentement doit être **compréhensible ;**
- Le consentement doit être **distinct ;**
- Le consentement doit être donné **à des fins spécifiques ; et**
- Le consentement ne vaut que pour une **durée spécifique.**

Manifeste : Le consentement doit être évident, certain et indiscutable et il ne doit laisser aucun doute quant à la volonté qui y est exprimée.

Libre : Le consentement doit être donné sans contrainte. Ce critère ne serait pas satisfait si, par exemple, le consentement résultait d'une pression exercée sur la personne concernée.

Éclairé : Les informations transmises à la personne concernée doivent lui permettre de donner son consentement en toute connaissance de cause. Par exemple, dans le contexte d'une demande de consentement à la communication de renseignements personnels, un organisme public doit notamment informer la personne concernée :

- Des renseignements personnels qui seront communiqués ;
- Des personnes et des organismes à qui ces renseignements seront communiqués ;
- Des fins pour lesquelles ces renseignements sont requis ;
- Des conséquences d'une telle communication ou d'un refus de donner son consentement.

Granulaire : Le consentement doit être demandé pour chacune des fins visées. S'il y a plusieurs finalités, le consentement doit être demandé séparément pour chacune d'elles. Cette granularité permet à la personne concernée de manifester sa volonté clairement, car elle peut accepter ou refuser chaque finalité spécifique.

Compréhensif : La demande de consentement doit être présentée en des termes simples et clairs, tant pour les informations fournies que pour la question ou l'énoncé d'acceptation ou de refus. Les propos devraient être concis, c'est-à-dire exprimés avec un minimum de mots.

Ils devraient utiliser un vocabulaire courant, sans jargon juridique ou organisationnel. Ils devraient utiliser les termes les plus directs possibles.

Distinct : La demande de consentement doit être séparée des conditions d'utilisation, des politiques de confidentialité, des signatures, etc. Elle doit avoir sa propre section ou sa propre interface facilement accessible par la personne concernée.

Donné à des fins spécifiques : Le consentement doit être demandé pour chacune de ces fins. Il ne peut donc pas être général ni englober plusieurs fins. La personne concernée doit être en mesure de comprendre et de choisir les fins pour lesquelles elle donne ou non son consentement, par exemple en cochant des cases dans un formulaire électronique.

Exemple d'application pratique de ce critère. Lors de l'embauche d'un nouvel employé, ce dernier est informé que la Municipalité recueille son adresse électronique personnelle afin de lui acheminer des informations et de la documentation en lien avec son emploi. Dans la mesure où la Municipalité désire désormais utiliser ce renseignement personnel à une autre fin (ex : communiquer des informations et de la documentation n'ayant pas de lien avec son emploi), un nouveau consentement manifeste, libre et éclairé devra être obtenu à cette fin pour une durée spécifique.

Durée variable : Le consentement ne vaut que pour la durée nécessaire à la réalisation des fins auxquelles il a été demandé. Ce consentement s'évalue donc au cas par cas. Cette durée peut être un nombre de jours, de mois ou d'années, ou alors faire référence à un événement déterminé ou à une situation précise.

Exemple d'application pratique de ce critère. Lors de l'inscription d'un enfant au camp de jour, les parents de ce dernier sont informés que la Municipalité doit recueillir des informations sur différents enjeux de santé afin d'assurer sa sécurité lors de sa présence au camp de jour. Dans la mesure où l'enfant n'est palus inscrit au camp de jour, la Municipalité devra procéder à la destruction de ces renseignements personnels conformément à son calendrier de conservation.

Ceci dit, en ce qui concerne les municipalités, les renseignements personnels compris dans les dossiers d'un immeuble (notamment en matière d'urbanisme et taxation) doivent y demeurer

2.1.3.2. L'obtention d'un consentement dit « exprès »

Le consentement exprès. Une organisation doit privilégier l'obtention d'un consentement exprès des personnes concernées (aussi appelé « consentement explicite »)[1].

[1] Commission d'accès à l'information, 16 mai 2023, *Lignes directrices 2023-1 sur les critères de validité du consentement.*

Notez qu'il est **toujours requis** de **toujours s'assurer** d'obtenir un consentement exprès lorsque l'on demande à une personne concernée de pouvoir utiliser ou communiquer ses renseignements personnels sensibles.

Définition. Une personne consent expressément à une utilisation ou à une communication de ses renseignements personnels lorsqu'elle manifeste son acceptation par un **geste positif** ou par une déclaration.

Méthodes. Plusieurs méthodes permettent d'obtenir un consentement exprès. Par exemple, il est possible de :

1. Demander à la personne concernée d'apposer sa signature écrite à un document ;
2. Demander à la personne concernée d'activer une case sur une plateforme web ;
3. Demander à la personne concernée de cliquer sur un bouton « accepter » alors qu'il visite un site web (à condition qu'un bouton « je refuse » soit mis en valeur de la même façon)[2] ; ou de
4. demander à un client de répondre à l'affirmative à une demande orale de consentement et le documenter.

Exemple pratique. Lors du dépôt d'une demande de permis, les Employés du département de l'urbanisme de la Municipalité expliquent au propriétaire que celui-ci doit entre autres transmettre une description de son projet, la valeur estimée des travaux de même les coordonnées auxquelles il peut être rejoint. La remise et la signature de la demande de permis dûment complétée et signée permet de présumer le consentement du demandeur de permis. Par précaution, les Employés du service de l'urbanisme pourraient demander au moment de la complétion de la demande de permis de signer, un formulaire écrit de consentement. Ce faisant, le propriétaire donne un consentement exprès à la collecte des renseignements personnels contenus dans la demande de permis.

Une telle demande de consentement peut être ajouté au formulaire de demande de permis de façon à systématiser les collectes de renseignements personnels plus fréquentes.

[2] Commission d'accès à l'information, 16 mai 2023, *Lignes directrices 2023-1 sur les critères de validité du consentement*, p. 17.

3. Bonnes pratiques en matière de conservation et de destruction de renseignements personnels

3.1. Conservation de renseignements personnels

Définition. La conservation fait référence à la période durant laquelle la Municipalité continue de détenir des renseignements personnels après leur collecte, sous quelque format que ce soit et sans égard au fait que ces renseignements personnels soient activement utilisés ou non. Ainsi, un formulaire écrit composé de renseignements personnels qui est oublié dans le tiroir du bureau d'un Employé constitue une conservation des renseignements personnels dans le formulaire, au même titre que la présence de renseignements personnels dans un fichier numérique quelconque enregistré sur le disque dur d'un appareil technologique d'un Employé dans le cadre de son emploi. Lorsqu'elle conserve des renseignements personnels, la Municipalité doit :

1. Assurer la qualité des renseignements personnels en veillant à ce que ceux-ci soient exacts au moment où elle les utilise pour prendre une décision relative à la personne concernée ;

2. Mettre en place des mesures de sécurité permettant d'assurer la protection du caractère confidentiel des renseignements personnels ; et

3. Assurer la destruction des renseignements personnels une fois les fins de sa collecte accomplies, à moins qu'une loi applicable prévoie un délai de conservation spécifique.

3.2. Mesures de sécurité

Mesures raisonnables. La Municipalité est responsable de la mise en place de mesures de sécurité « raisonnables » pour assurer la protection du caractère confidentiel des renseignements personnels qu'elle conserve. Le caractère raisonnable des mesures mises en place s'évalue en tenant compte, notamment, de la sensibilité des renseignements personnels conservés, de la finalité de leur utilisation, de leur quantité, de leur répartition et de leur support[3].

Exemples de mesures de sécurité :

1. **Centralisation des renseignements personnels.** Les Employés sont la courroie principale de la Municipalité en matière d'entrée et de sortie de renseignements personnels. En ce sens, il est impératif que les Employés utilisent exclusivement les infrastructures et les outils technologiques mis à leur disposition par la Municipalité pour recueillir, utiliser, communiquer et conserver ces renseignements personnels. Par exemple, un Employé ne doit pas utiliser sa boîte à courrier électronique

[3] *Loi sur la protection des renseignements personnels dans le secteur privé*, RLRQ, c. P-39.1, art. 10.

personnelle pour recevoir ou transmettre des documents de travail pouvant contenir des renseignements personnels, et ce, même si ceux-ci ont été dépersonnalisés.

2. **Mesure d'authentification mises en place.** Les Employés doivent respecter les procédures d'authentification mise en place par la Municipalité le cas échéant, préalablement à tout accès à des logiciels ou plateformes renfermant des renseignements personnels.

3. **Mots de passe forts.** Les Employés doivent créer des mots de passe dits « forts » pour accéder aux logiciels ou plateformes renfermant des renseignements personnels. Un mot de passe est considéré « fort » dans la mesure où il est composé :

    - d'au moins douze (12) caractère ;
    - d'au moins un caractère spécial (ex : !, @, #, $, %, ^, &, *, (,), -, +, =, {, }, [,], :, ;, « , », ‘, , ?, /, , et |) ;
    - d'au moins un chiffre (ex : 1, 2, 3, 4, 5, 6, 7, 8, 9 et 0) ;
    - d'au moins une lettre majuscule (ex : A, B, C, D, E, F, G, H,I…) ; et
    - d'au moins une lettre minuscule (ex : a, b, c, d, e, f, g, h…).

4. **Formations.** Les Employés doivent participer assidument à toute activité de formation offerte par la Municipalité en matière de protection des renseignements personnels.

5. **Utilisation des infrastructures technologiques.** Les Employés doivent utiliser les infrastructures et outils technologiques mis à leur disposition par la Municipalité, notamment :

    - utiliser un réseau privé virtuel (« VPN ») rendu accessible par la Municipalité en cas de télétravail ;
    - Ne jamais déplacer de renseignements personnels en format physique en dehors des locaux de la Municipalité, même en situation de télétravail ;
    - Ne jamais connecter un appareil technologique à un réseau public ou inconnu ;
    - Ne jamais enregistrer de documents contenant des renseignements personnels sur un support de stockage mobile ou non-autorisé par le Responsable.
    - La vérification continue des adresses électroniques des personnes qui communiquent un courriel afin d'identifier qu'il s'agit bien d'une personne connue et réviser l'adresse du destinateur afin de vérifier s'il s'agit bel et bien de l'adresse de cette personne;
    - Être méfiant à l'égard des courriels qui inspirent un sentiment d'urgence ou qui contiennent des requêtes qui sortiraient de l'ordinaire;

- Se méfier des hyperliens transmis par courriel et des courriels contenant des hyperliens intégrés à même le texte ou à une image. Si le courriel semble légitime, placer son curseur par-dessus le courriel afin de vérifier si la véritable adresse attachée au lien est suspecte ;

- Ne jamais cliquer sur un hyperlien suspect ou ouvrir une pièce jointe transmise par un courriel suspect ;

- Détruire immédiatement tout courriel suspect ; et

- En cas de doutes sur la légitimité du courriel, effectuer une capture d'écran et communiquer celle-ci au Responsable.

6. **Réceptivité aux incidents de confidentialité.** Un Employé qui constate la survenance d'un incident de confidentialité, ou qui a des raisons de croire à la survenance d'un incident de confidentialité, doit en informer sans délai le Responsable. La section 0 du Guide contient des informations relatives aux incidents de confidentialité.

3.3. Incidents de confidentialité et devoir de signaler

Définition d' « incident de confidentialité ». Un « incident de confidentialité » correspond à tout accès, utilisation ou communication non autorisés d'un renseignement personnel, de même qu'à la perte d'un renseignement personnel ou à toute autre atteinte à sa protection. Par exemple, un incident de confidentialité pourrait se produire lorsque :

- Un employé de la Municipalité consulte des renseignements personnels sans autorisation;

- Un Employé communique des renseignements personnels au mauvais destinataire, par erreur ou autrement;

- La Municipalité est victime d'une cyberattaque, quelle qu'en soit la source (hameçonnage, rançongiciel, etc.).

Obligations en lien avec les incidents de confidentialité. Un Employé qui constate la survenance d'un incident de confidentialité, ou qui a des raisons de croire à la survenance d'un incident de confidentialité, **aussi mineur puisse-t-il sembler**, doit en informer sans délai le Responsable et collaborer activement avec ce dernier afin de limiter tout préjudice pouvant découler d'un tel incident de confidentialité. **La transparence et la collaboration des Employés est essentielle pour permettre à la Municipalité de s'acquitter de ses obligations en cas de survenance d'un incident de confidentialité**.

3.4. Obligation de détruire les renseignements personnels

Fins accomplies. Lorsque les fins auxquelles un renseignement personnel a été recueilli sont accomplies, la Municipalité doit procéder à sa destruction, sous réserve d'un délai de

conservation prévu par une loi ou un règlement. Les délais de conservation pour chaque type de renseignements personnels recueillis par la Municipalité sont indiqués dans le **Calendrier de conservation** de la Municipalité. Malgré ce qui précède, aucun **Employé n'est autorisé à procéder à la destruction d'un renseignement personnel sans l'autorisation préalable écrite du Responsable**. De même, un Employé qui reçoit une demande dont l'objet est la destruction de renseignements personnels détenus par la Municipalité doit acheminer cette demande au Responsable, sans délai.

Méthodes de destruction. La Commission d'accès à l'information propose différentes méthodes de destruction selon le support de conservation des renseignements personnels[4].

ACCEPTATION

Je soussigné, _____, reconnaissant avoir lu l'intégralité du Guide, de même qu'avoir obtenu toute explication jugée opportune à l'égard de son contenu, signe à l'endroit et à la date indiqués ci-après :

Signé à _____, ce _____e jour de _____ 20__.

_____
Signature

_____
Nom et Prénom

[4] Conservation et... | Commission d'accès à l'information du Québec, consulté le 12 février 2025

Annexe « A » - Tableau récapitulatif des fins poursuivies par la collecte de chaque type de renseignements personnels

Type de renseignements personnels	Fins poursuivies par la collecte
Renseignements d'identification Par exemple : adresse électronique et postale, numéro de téléphone, sexe, âge, numéro d'assurance sociale, numéro d'assurance maladie, identifiant numérique, photographie, enregistrement vidéo ou audio d'une personne, etc.	**Traitement des différentes demandes de contribuables :** Demande de permis ou autres demandes ou actes posées en liens avec l'urbanisme; Demandes déposées en conformité avec différents programmes mis en place par la Municipalité; Taxation et comptes à recevoir/payables; Services de sécurité incendies – Prévention et intervention; Inscription à différents services – Camps de jour, loisirs, bibliothèque etc.
Renseignements de santé Par exemple : diagnostic, consultation d'une professionnelle ou d'un professionnel de la santé, allergie, médicament, etc.	Camp de jours; Dossiers employés;
Renseignements financiers Exemples : revenu d'une personne, numéro de compte bancaire, biens possédés, numéros de cartes de crédit, etc.	Taxation et comptes à recevoir/payables Inscription à différents services – camp de jour, loisirs, bibliothèques etc. Service de paie
Renseignements relatifs au travail Exemples : motifs d'absence, dates de vacances, salaire, heures d'entrée et de sortie liées au lieu de travail, etc.	Ressources humaines

Renseignements sur les préférences de communication et la consommation de services Exemples : informations sur les abonnements aux communications, informations sur les services utilisés, réponses aux sondages ou aux études, etc.	Amélioration des services municipaux; Consultations citoyennes.