gestar
Experts en gouvernance documentaire



Nathalie Levesque
Vice-présidente

Après la Loi 25 : comment passer du cadre de gouvernance à son application concrète ?

Depuis l'entrée en vigueur des différentes dispositions de la Loi 25, la majorité des municipalités québécoises ont accompli un travail considérable. Responsabilités liées à la protection des renseignements personnels désignés, politiques adoptées et diffusées, comités formés lorsque requis : les fondations de la gouvernance sont désormais en place. Pourtant, un défi de taille demeure : comment transformer ces exigences administratives en application quotidienne par les employés ? La conformité ne repose pas uniquement sur des politiques, elle dépend surtout de la capacité de chaque employé à reconnaître un renseignement personnel, à identifier son niveau de confidentialité et à appliquer des mesures de protection efficaces et adaptées tout au long de son cycle de vie. C'est souvent à cette étape de mise en œuvre que les municipalités rencontrent les plus grands défis.

Incorporer la protection dans la pratique quotidienne

La responsabilité de la protection des renseignements personnels ne repose pas uniquement sur le responsable désigné, elle concerne tous les employés qui produisent, consultent, transmettent ou conservent des documents dans le cadre de leurs fonctions.

Selon le rapport Verizon DBIR 2025, un élément humain est impliqué dans près de 60 % des atteintes à la sécurité et à la confidentialité. Cela inclut l'envoi d'un document au mauvais destinataire, une configuration de permissions erronée ou une utilisation inadéquate des données. Toujours selon ce rapport, seules 20 % des brèches sont liées à l'exploitation de failles techniques non corrigées. Au-delà, donc, de la mise en place d'une cybersécurité solide par le responsable des TI, l'établissement d'une méthodologie claire, complète et contrôlée à l'intention du personnel est impératif.

Développer des procédures et des outils complémentaires

Les politiques de gouvernance ne suffisent généralement pas à guider les opérations quotidiennes. Les municipalités gagnent à élaborer des procédures et des outils simples et accessibles portant notamment sur le traitement des demandes d'accès, la gestion des incidents de confidentialité, l'utilisation sécuritaire du courriel, le partage de documents avec des organisations externes ou encore la fermeture des accès lors du départ d'un employé.

Les registres obligatoires et l'inventaire des fichiers de renseignements personnels doivent être à jour.

L'importance des niveaux de confidentialité

L'attribution de niveaux de confidentialité aux documents permet aux employés de connaître immédiatement le degré de sensibilité de ce qu'ils manutentionnent et de lier cette information aux mesures de protection qui doivent être appliquées.

Voici un exemple de classification simple qui peut être mise en place :

Public – Information destinée à être diffusée sans restriction, comme les règlements municipaux adoptés ou les procès-verbaux publics.

Protégé A – Renseignements personnels ou autres informations confidentielles dont la divulgation pourrait causer un préjudice limité à une personne ou à une organisation, par exemple : un curriculum vitae, des coordonnées d'urgence.

Protégé B – Renseignements dont la divulgation pourrait entraîner un préjudice sérieux, notamment les dossiers de ressources humaines, certaines plaintes citoyennes ou les informations financières confidentielles.

Pour certaines organisations, des niveaux de confidentialité encore plus élevés pourraient être définis, par exemple, s'ils détiennent des informations dont la divulgation menacerait la sécurité nationale ou la sécurité publique. On ne parle pas, ici, de renseignements personnels, mais plutôt de renseignements à garder secrets, comme les mesures de sécurité d'un événement impliquant des dignitaires fédéraux.

Adapter les mesures aux niveaux de confidentialité et aux supports

Les spécialistes s'entendent sur le fait que les documents papier contenant des renseignements personnels devraient être conservés dans des espaces à accès contrôlé, tandis que les documents technologiques devraient faire l'objet de permissions adaptées aux besoins réels des utilisateurs et à leur degré d'accréditation.

Des mesures additionnelles peuvent être ajoutées selon le niveau de confidentialité. Les documents papier à contenu très sensible pourraient, par exemple, être consultés sous caméra de surveillance. Les documents technologiques pourraient être visés par des mesures sécurisées de transmission, de l'encryptage ou des mots de passe à même le fichier.

La sauvegarde, la consultation, la transmission, la conservation et la destruction de ces documents doivent être encadrées par des mesures précises et définies par niveau de confidentialité et par support.

Le niveau de protection doit être facilement identifiable à même le document (certains organismes inscrivent la cote de confidentialité directement sur celui-ci).

Appliquer le calendrier de conservation

La *Loi sur les archives* exige l'établissement et la tenue à jour du calendrier de conservation déterminant les périodes de conservation ainsi que le sort final des documents. Or, plusieurs organisations considèrent encore le calendrier comme un simple outil archivistique. En réalité, il joue un rôle central dans la protection des renseignements personnels. L'application des règles est obligatoire et renforcée par l'article 73 de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*.

Conserver des renseignements personnels au-delà de leur durée utile augmente les risques de fuite d'information et d'incident de confidentialité ainsi que les coûts de stockage. C'est pourquoi les opérations de déclassement, de transfert et de destruction prévues au calendrier devraient être réalisées de façon systématique au moins une fois par an.

Former et sensibiliser le personnel

Finalement, aucune politique ne peut remplacer le jugement des employés. La conformité durable repose sur leur sensibilisation continue. Les organisations les plus efficaces ne se limitent pas à une formation unique, elles multiplient les rappels pratiques sous diverses formes : capsules, guides et aide-mémoire, modèles de documents, procédures, séances d'information ciblées selon les fonctions.

Contrôler l'application des mesures

Tout ce qui peut être automatisé devrait l'être. Les contrôles de cybersécurité sont de précieux alliés.

Cependant, comme il y a toujours des tâches qui ne sont pas automatisables, les exigences de protection des renseignements personnels doivent faire l'objet d'un contrôle administratif, par exemple, via un audit interne périodique. Un tel exercice permet de déceler rapidement les imprécisions, les failles d'application et les autres points à corriger afin de garder l'ensemble du système efficient et sécuritaire au fil des ans.

Passer de la conformité à la maturité

La Loi 25 a permis d'accélérer la mise en place d'une gouvernance structurée des renseignements personnels au sein des municipalités québécoises. Toutefois, la véritable conformité commence après l'adoption des politiques.

Les organisations les plus résilientes sont celles qui, non seulement, mettent en place toute la documentation exigée, mais réussissent aussi à intégrer la protection des renseignements personnels à leurs pratiques courantes de gestion documentaire : création de documents, classification de l'information, gestion des accès, procédures opérationnelles, formation continue et application rigoureuse du calendrier de conservation.

En somme, la protection des renseignements personnels ne devrait pas être perçue comme une obligation parallèle à la gestion documentaire, car elle en est, aujourd'hui, l'une des composantes essentielles. Une municipalité qui sait identifier ses informations sensibles, les protéger adéquatement et les détruire au moment opportun est non seulement conforme à la Loi 25, mais également mieux préparée à répondre aux attentes grandissantes des citoyens en matière de confiance et de transparence.

Bibliographie et références :

Loi sur les archives, RLRQ, c. A-21.1.

Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, RLRQ, c. A-2.1.

2025 Data Breach Investigations Report (DBIR), Verizon Business, New York, 2025.