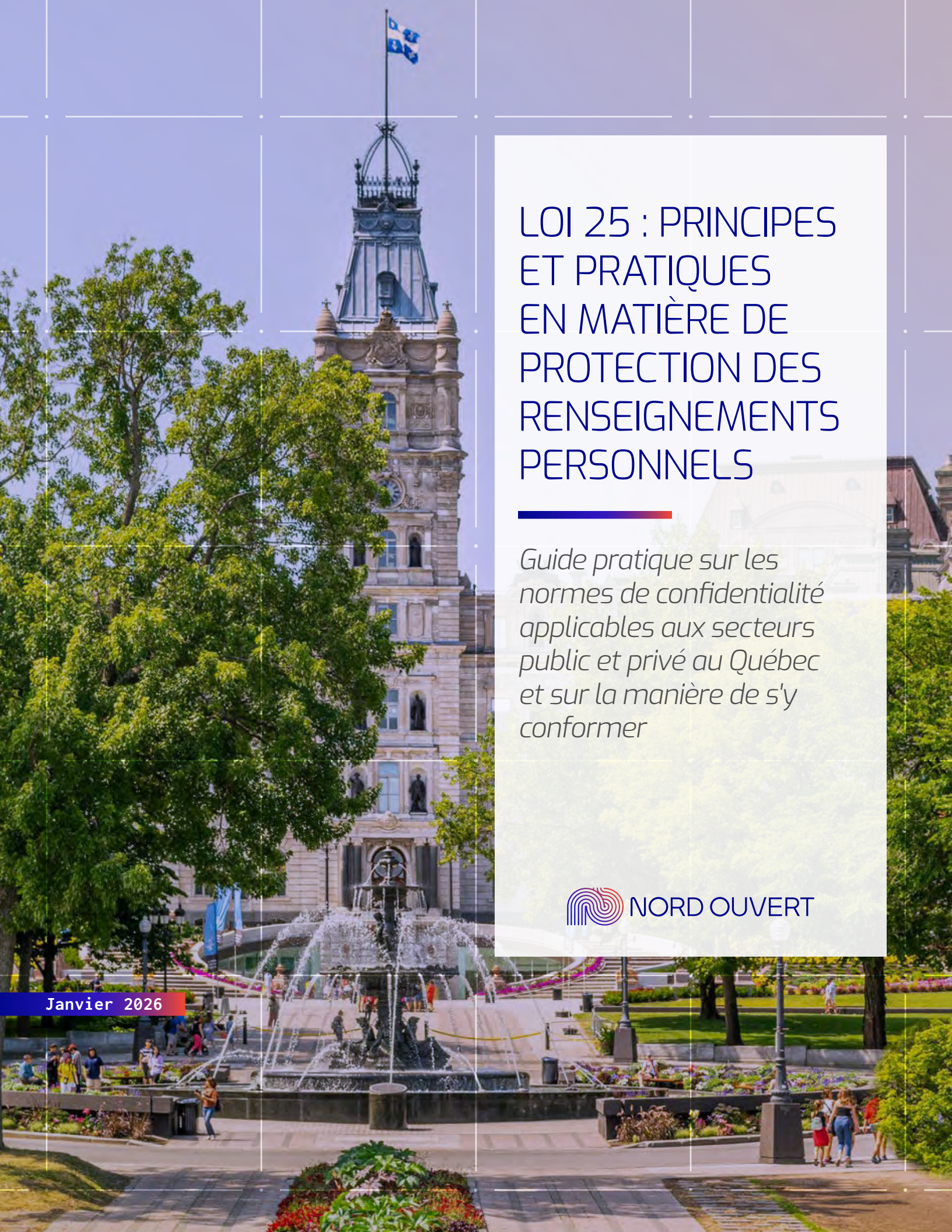




LOI 25 : PRINCIPES ET PRATIQUES EN MATIÈRE DE PROTECTION DES RENSEIGNEMENTS PERSONNELS

*Guide pratique sur les
normes de confidentialité
applicables aux secteurs
public et privé au Québec
et sur la manière de s'y
conformer*

 NORD OUVERT

Janvier 2026

TABLE DES MATIÈRES

Termes clés	1
Qu'est-ce que la Loi 25 ?	2
Pourquoi est-il important de se conformer à la Loi 25 ?	3
Dix principes de confidentialité : un cadre fondamental pour la protection des renseignements personnels au Canada	4
Responsabilité : assumer la responsabilité de la protection des données	5
Déterminer les fins de collecte : être transparent quant aux raisons pour lesquelles vous collectez des renseignements	5
Consentement : obtenir l'autorisation de manière appropriée	5
Limiter la collecte : ne collecter que ce qui vous est nécessaire	6
Limiter l'utilisation, la divulgation et la conservation : respecter les limites de l'information	6
Exactitude : maintenir des données exactes et à jour	6
Mesures de sécurité : mettre en œuvre des mesures de sécurité pour protéger les données	7
Transparence : faire preuve de transparence quant à vos pratiques en matière de confidentialité	7
Accès aux renseignements personnels : donner aux personnes les moyens de contrôler leurs données personnelles	7
Contester la conformité : proposer un recours en cas de problème	8
Les principes de confidentialité comme point de départ d'une bonne gouvernance des données	8
Protection des renseignements personnels au Québec : exigences applicables aux secteurs privé et public en vertu de la Loi 25	9
Une conversation autour d'un café entre collègues	9

Évaluation rapide de la conformité à la Loi 25	20
Exigences communes (secteurs privé et public)	20
Exigences supplémentaires pour le secteur public	21
Exigences supplémentaires pour le secteur privé	21
Commencez dès aujourd'hui	21
À propos de Nord Ouvert	22
À propos du Défi des villes intelligentes et de Montréal en commun	22

TERMES CLÉS

Avant de commencer, voici quelques définitions des termes clés que vous trouverez tout au long de ce guide :

TERME	DÉFINITION
Loi 25	Loi visant à moderniser les dispositions législatives en matière de protection des renseignements personnels, mise en œuvre progressivement entre 2021 et 2024 au Québec.
Droit à la vie privée	Droit fondamental des personnes à contrôler la manière dont leurs renseignements personnels sont recueillis, utilisés, communiqués et conservés par les organisations.
Renseignements personnels	Données concernant une personne identifiable (par exemple, numéro de téléphone, adresse, âge, sexe, origine ethnique).
Renseignements personnels sensibles	Renseignements personnels qui nécessitent une protection accrue de la vie privée, tels que les données relatives à la santé, aux finances, à la race, aux opinions politiques, à l'orientation sexuelle, aux croyances religieuses et aux données génétiques. (Remarque : ce qui est considéré comme sensible peut varier d'un individu à l'autre).
Commission d'accès à l'information (CAI)	Organisme public indépendant du Québec chargé de superviser et d'appliquer la Loi 25 pour les organisations des secteurs public et privé.
Consentement	Autorisation donnée par une personne pour la collecte, l'utilisation ou la divulgation de ses renseignements personnels.
Incident de confidentialité	Tout événement impliquant la perte, l'accès, l'utilisation ou la communication non autorisés de renseignements personnels nécessitant une documentation et éventuellement, une notification à la CAI et aux personnes concernées.
Anonymisation	Processus technique qui modifie de manière irréversible les renseignements personnels afin qu'il ne soit plus raisonnablement possible d'identifier une personne, conformément aux exigences réglementaires spécifiques du Québec.

QU'EST-CE QUE LA LOI 25 ?

La Loi 25, officiellement intitulée « **Loi modernisant des dispositions législatives en matière de protection des renseignements personnels** », a été progressivement mise en œuvre entre 2021 et 2024 dans la province canadienne du Québec. Il s'agit d'une législation complète qui modernise les lois sur la protection de la vie privée dans les secteurs privé et public et introduit plusieurs nouvelles exigences en matière de conformité juridique.

La Loi 25 est considérée comme l'équivalent du règlement général sur la protection des données (RGPD) de l'Union européenne et constitue la loi sur la protection de la vie privée la plus exigeante en Amérique du Nord. La législation établit des exigences strictes concernant la manière dont les organisations collectent, utilisent, stockent et protègent les renseignements personnels, avec des pénalités pouvant atteindre 25 millions de dollars ou 4 % du chiffre d'affaires mondial en cas de non-conformité, ainsi que des amendes pour les entreprises et les gouvernements, et des sanctions pénales pour les particuliers.



POURQUOI EST-IL IMPORTANT DE SE CONFORMER À LA LOI 25 ?

Au-delà des obligations légales et des répercussions financières, le respect de la Loi 25 est essentiel pour les raisons suivantes :

- › **Instaurer la confiance** : les organisations qui font preuve de pratiques rigoureuses en matière de protection de la vie privée gagnent la confiance des citoyens, des clients, des membres et des bénéficiaires. À l'ère numérique, la confiance est un avantage concurrentiel qui a un impact direct sur les relations avec la communauté et sur la réussite des organisations;
- › **Viser l'excellence opérationnelle** : de bonnes pratiques en matière de confidentialité permettent une meilleure gouvernance des données, des opérations plus efficaces et une réduction des risques liés à la cybersécurité. Les organisations disposant de processus clairs de gestion des données font face à moins d'incidents et fonctionnent plus efficacement;
- › **Préparer l'avenir** : alors que les attentes en matière de respect de la vie privée continuent d'évoluer à l'échelle mondiale, les organisations dotées de cadres de confidentialité solides sont mieux placées pour s'adapter aux futurs changements réglementaires et évolutions technologiques.
- › **Protéger la réputation** : les violations de la vie privée et la non-conformité peuvent entraîner une atteinte importante à la réputation, une couverture médiatique négative et une perte de confiance du public. Cette dernière pourrait prendre plusieurs années à reconstruire.

Ce guide compare les exigences du secteur public et du secteur privé en vertu de la Loi 25 et fournit des conseils pratiques sur la manière de s'y conformer. Que vous soyez au service de citoyens, de clients, de membres ou de bénéficiaires, il est essentiel de comprendre comment traiter correctement les renseignements personnels afin de protéger à la fois votre organisation et les personnes qui vous font confiance.



DIX PRINCIPES DE CONFIDENTIALITÉ : UN CADRE FONDAMENTAL POUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS AU CANADA

Il est essentiel de comprendre les 10 principes énumérés ci-dessous pour appréhender les normes et la législation en matière de protection de la vie privée au Canada, y compris au Québec. Ces principes, élaborés par l'Association canadienne de normalisation, constituent le fondement de la Loi 25 et fournissent un cadre complet pour un traitement responsable des données personnelles.

Les 10 principes de protection de la vie privée sont les suivants :

1. **Responsabilité** — assumer la responsabilité de la protection des données;
2. **Détermination des fins de la collecte des renseignements** — être transparent quant aux raisons pour lesquelles vous collectez des renseignements personnels;
3. **Consentement** — obtenir l'autorisation de manière appropriée;
4. **Limitation de la collecte** — ne collecter que ce qui vous est nécessaire;
5. **Limitation de l'utilisation, de la communication et de la conservation** — respecter les restrictions relatives aux données;
6. **Exactitude** — maintenir des données exactes et à jour;
7. **Mesures de sécurité** — mettre en œuvre des mesures de sécurité pour protéger les données;
8. **Transparence** — faire preuve de transparence quant à vos pratiques en matière de confidentialité;
9. **Accès aux renseignements personnels** — donner aux personnes les moyens de contrôler leurs données personnelles;
10. **Possibilité de porter plainte à l'égard du non-respect des principes** — Proposer un recours en cas de problème.

En comprenant ces principes, vous saisissez l'essence même des normes et des lois en matière de protection de la vie privée au Canada, y compris la Loi 25 du Québec. Les sections ci-dessous examinent chaque principe en détail.

1

Responsabilité : assumer la responsabilité de la protection des données

Ce que cela signifie

Votre organisation doit assumer l'entière responsabilité de tous les renseignements personnels sous son contrôle, y compris les informations traitées par des tiers en votre nom.

En pratique

Cela signifie qu'il vous faut désigner un référent pour la protection de la vie privée au sein de votre organisation. Cette personne sera chargée de veiller à la confidentialité des données et au respect des normes en vigueur. Il peut s'agir du directeur général, d'un responsable administratif ou d'un coordonnateur dédié, selon la taille et la structure de votre organisation.

Exemple

Lorsqu'une organisation passe un contrat avec un prestataire de services tiers pour traiter les paiements en ligne ou gérer les bases de données des membres, elle reste responsable de la protection de ces données personnelles, même si le traitement est effectué ailleurs.

En pratique

Chaque formulaire, demande ou processus de collecte de données doit avoir un objectif clair et légitime que vous pouvez expliquer à la personne qui fournit ses renseignements personnels.

Exemple

Lorsque des individus s'inscrivent à un programme ou à un service, expliquez-leur clairement que vous avez besoin de leurs coordonnées pour leur communiquer des informations, de leur adresse dans le cadre de la prestation de services (le cas échéant) et des coordonnées de leur contact d'urgence à des fins de sécurité.

3

Consentement : obtenir l'autorisation de manière appropriée

Ce que cela signifie

Vous devez obtenir le consentement éclairé des personnes avant de collecter, d'utiliser ou de partager leurs renseignements personnels, sauf dans des circonstances spécifiques où la loi autorise le contraire.

En pratique

Le consentement doit être éclairé (les personnes comprennent ce à quoi elles consentent), volontaire (sans contrainte) et spécifique (explicite quant aux utilisations prévues). La forme du consentement peut varier en fonction du niveau de sensibilité des données.

Exemple

Lorsque des individus s'inscrivent à un service, ils peuvent donner leur consentement général dans le cadre de l'administration du programme, mais vous devez également obtenir leur consentement explicite et distinct afin d'utiliser leurs photos dans des supports promotionnels ou partager leurs données avec des organisations partenaires. Les formulaires d'inscription doivent comporter des cases distinctes pour chaque objectif et celles-ci ne doivent pas être préalablement cochées.

2

Déterminer les fins de collecte : être transparent quant aux raisons pour lesquelles vous collectez des renseignements

Ce que cela signifie

Vous devez identifier et documenter les raisons pour lesquelles vous collectez des renseignements personnels avant ou au moment où vous les collectez.

4

Limiter la collecte : ne collecter que ce qui vous est nécessaire

Ce que cela signifie

Ne collectez que les renseignements personnels nécessaires aux fins que vous avez identifiées.

En pratique

Remettez en question chaque champ de vos formulaires et chaque donnée que vous collectez régulièrement. Si vous ne pouvez pas établir de lien direct avec l'objectif que vous avez annoncé, demandez-vous si vous en avez vraiment besoin.

Exemple

Pour l'inscription à un programme, vous pouvez avoir besoin du nom et des coordonnées des participants afin de communiquer avec eux, ainsi que des coordonnées des personnes à contacter en cas d'urgence pour des raisons de sécurité. Vous n'avez probablement pas besoin de connaître leur profession, leur niveau de revenu ou des informations détaillées sur leur famille, sauf si cela est directement lié au service spécifique fourni.

et respectez ces délais. N'utilisez pas les informations collectées à une fin donnée pour des activités complètement différentes sans obtenir un nouveau consentement.

Exemple

Les coordonnées recueillies pour les notifications relatives aux programmes ne peuvent pas être automatiquement utilisées pour des campagnes de collecte de fonds sans consentement spécifique. Les dossiers des clients peuvent être conservés à des fins de prestation de services, mais ils doivent être détruits de manière sécurisée après la période de conservation requise, conformément aux exigences légales et aux besoins opérationnels.

6

Exactitude : maintenir des données exactes et à jour

Ce que cela signifie

Les renseignements personnels doivent être aussi exacts, complets et à jour que nécessaire pour les fins auxquelles ils sont utilisés.

En pratique

Mettez en place des processus pour vérifier l'exactitude des informations au moment de leur collecte et les mettre à jour lorsque vous constatez des changements ou des erreurs.

Exemple

Vérifiez régulièrement que les coordonnées sont à jour et exactes, en particulier les contacts d'urgence et les adresses nécessaires pour la prestation de services. Proposez aux utilisateurs des moyens simples de signaler et de corriger les erreurs dans leurs dossiers. Si la situation d'une personne change, facilitez-lui la mise à jour de ses informations.

5

Limiter l'utilisation, la divulgation et la conservation : respecter les limites de l'information

Ce que cela signifie

Les renseignements personnels ne doivent être utilisés ou partagés qu'aux fins pour lesquelles ils ont été collectés, et ne doivent pas être conservés plus longtemps que nécessaire.

En pratique

Établissez des politiques claires concernant la durée de conservation des différents types d'informations

7

Mesures de sécurité : mettre en œuvre des mesures de sécurité pour protéger les données

Ce que cela signifie

Protégez les renseignements personnels à l'aide de mesures de sécurité adaptées au niveau de sensibilité des données.

En pratique

Mettez en place des mesures de sécurité physiques (armoires verrouillées, installations sécurisées), des mesures techniques (mots de passe, cryptage, réseaux sécurisés) et des mesures organisationnelles (formation, politiques). Le niveau de protection doit être adapté à la sensibilité des données.

Exemple

Les données personnelles sensibles telles que les dossiers médicaux ou les informations financières nécessitent une protection plus stricte que les listes de contacts générales. Cela peut inclure des armoires à dossiers verrouillées, des ordinateurs protégés par mot de passe, le cryptage des fichiers numériques et la limitation de l'accès au personnel autorisé uniquement. Même les données de base doivent être protégées contre tout accès non autorisé.

En pratique

Élaborez des politiques de confidentialité claires en utilisant un langage simple et rendez-les facilement accessibles. Soyez prêt à répondre aux questions sur la manière dont vous traitez les données personnelles.

Exemple

Publiez sur votre site web une politique claire en matière de renseignements personnels, expliquant comment ceux-ci sont collectés, utilisés et protégés. Indiquez les coordonnées à contacter pour toute question relative à la confidentialité et affichez ces informations au sein de vos bureaux. La politique doit être rédigée dans un langage simple et compréhensible par votre public.

9

Accès aux renseignements personnels : donner aux personnes les moyens de contrôler leurs données personnelles

Ce que cela signifie

Sur demande, les personnes doivent être informées des données personnelles que vous détenez à leur sujet et de la manière dont elles sont utilisées. De plus, les individus doivent avoir accès à leurs propres données.

En pratique

Établissez des procédures afin de traiter les demandes d'accès, notamment en vérifiant l'identité des demandeurs et en fournissant les données dans un format clair et compréhensible dans des délais raisonnables.

Exemple

Les individus doivent pouvoir demander des copies de leurs propres informations, demandes d'inscription à des programmes ou autres données personnelles que vous détenez. Établissez des procédures claires et des délais raisonnables pour ces demandes. Si une personne estime que ses données sont incorrectes, elle doit pouvoir demander des corrections.

8

Transparence : faire preuve de transparence quant à vos pratiques en matière de confidentialité

Ce que cela signifie

Il est nécessaire de rendre les informations relatives à vos politiques et pratiques en matière de confidentialité facilement accessibles au public.

10

Contester la conformité : proposer un recours en cas de problème

Ce que cela signifie

Les individus doivent pouvoir contester la conformité de votre organisation à l'égard du non-respect de ces principes de confidentialité et voir leurs préoccupations prises en compte.

En pratique

Établissez une procédure claire pour traiter les plaintes relatives à la confidentialité, examinez les plaintes de manière équitable et prenez des mesures correctives si nécessaire.

Exemple

Créez une procédure permettant aux personnes de déposer des plaintes relatives à la confidentialité, que ce soit par l'intermédiaire d'un référent désigné ou d'une procédure officielle. Examinez rapidement les plaintes et informez les plaignants des résultats et des mesures correctives prises. Soyez ouvert aux commentaires et disposé à améliorer vos pratiques.

Les principes de confidentialité comme point de départ d'une bonne gouvernance des données

Que vous soyez au service du public, de clients, de membres ou de bénéficiaires, la protection des renseignements personnels est fondamentale pour une bonne gouvernance des données et des pratiques responsables au sein de toute organisation. Les dix principes équitables de l'Association canadienne de normalisation fournissent un cadre éprouvé pour instaurer la confiance, réduire les risques et garantir que les renseignements personnels sont traités avec le soin et le respect qu'ils méritent. En adoptant ces dix principes, les organisations du Québec peuvent établir des relations plus solides avec leurs communautés tout en protégeant les renseignements personnels qui leur sont confiés.

Dans les sections suivantes, nous verrons comment les lois québécoises sur la protection des renseignements personnels reflètent ces dix principes au sein des organisations publiques et privées.

PROTECTION DES RENSEIGNEMENTS PERSONNELS AU QUÉBEC : EXIGENCES APPLICABLES AUX SECTEURS PRIVÉ ET PUBLIC EN VERTU DE LA LOI 25

Une conversation autour d'un café entre collègues

Anna, directrice générale d'un organisme sans but lucratif, et Robert, secrétaire municipal, se rencontrent autour d'un café pour discuter de leurs défis respectifs liés à la Loi 25. Tous deux sont référents de la protection des renseignements personnels au sein de leurs organisations respectives. L'organisation d'Anna est soumise aux exigences du secteur privé, tandis que la municipalité de Robert suit les règles du secteur public. Robert et Anna collaborent dans le cadre d'un atelier visant à aider d'autres municipalités et organisations non gouvernementales à s'y retrouver dans les exigences du Québec en matière de protection des renseignements personnels. Ils essaient de comprendre en quoi leurs exigences légales se recoupent et en quoi elles diffèrent.

Anna: Robert, je suis encore en train d'essayer de comprendre la Loi 25. Mon conseil d'administration ne cesse de me poser des questions sur la conformité, d'autant plus que nous travaillons avec des populations vulnérables. Pouvons-nous discuter de la manière dont tout cela est lié aux 10 principes de protection de la vie privée que nous présenterons lors de notre atelier ?



Robert: Absolument ! La bonne nouvelle, c'est que la Loi 25 reprend essentiellement ces 10 principes canadiens en matière de protection de la vie privée et les rend juridiquement contraignants au Québec. Passons-les en revue un par un et voyons comment ils s'appliquent à nous deux.



1

Principe de responsabilité dans la Loi 25

Robert: Le premier principe est celui de la **responsabilité**. En vertu de la Loi 25, nous devons tous deux désigner un responsable de la protection des renseignements personnels et publier ses coordonnées sur nos sites web.



Anna: D'accord, je me suis donc désignée comme référente de la protection des renseignements personnels, puisque je suis la directrice générale. Mais que se passe-t-il si je suis trop occupée par d'autres responsabilités ?



Robert: Vous pouvez déléguer cette fonction à quelqu'un d'autre, par exemple à responsable administratif ou à un autre membre du personnel. L'important est de trouver une personne qui connaît la loi et qui peut consacrer du temps aux problématiques de protection de la vie privée. Dans notre municipalité, nous avons nommé notre coordonnatrice informatique car elle a une bonne compréhension à la fois des aspects techniques et des aspects juridiques.



Anna: C'est logique. Et nous avons tous les deux besoin de politiques de gouvernance claires, n'est-ce pas ? C'est grâce à ces politiques que les gens sauront comment procéder.



Robert: Exactement ! Des politiques claires, accessibles et compréhensibles par tous.



2

Principe d'identification des fins de collecte dans la Loi 25

Anna: Le deuxième principe est l'**identification des finalités de collecte**. Je suppose que cela signifie que nous devons expliquer clairement pourquoi nous collectons des renseignements personnels ?



Robert: Exactement ! La Loi 25 exige que nous indiquions de manière transparente pourquoi nous collectons des données personnelles avant ou au moment de les collecter. Par exemple, lorsque ma municipalité procède à des évaluations foncières, nous expliquons que nous avons besoin de ces informations à des fins fiscales et d'urbanisme.

Anna: Donc, pour les inscriptions à nos programmes, je dois expliquer que nous collectons les coordonnées pour communiquer sur les programmes, les adresses pour la prestation des services et les contacts d'urgence pour des raisons de sécurité. Mais je ne peux pas simplement collecter des informations au hasard « au cas où » ?



Robert: Exactement ! Ne recueillez que ce dont vous avez réellement besoin pour remplir l'objectif que vous avez déclaré.



3

Principe du consentement dans la Loi 25

Anna: C'est là que je ne comprends plus très bien. Ai-je besoin d'un **consentement** explicite pour chaque objectif ?



Robert: C'est là que nos secteurs diffèrent considérablement. Dans le secteur privé, vous devez généralement obtenir le consentement explicite des personnes pour collecter et utiliser leurs renseignements personnels. Le consentement doit être éclairé, libre, spécifique et présenté séparément du reste des informations.

Anna: Que voulez-vous dire par « séparément » ? N'est-il pas suffisant d'avoir une seule et même déclaration de consentement pour tous les objectifs ?



Robert: Vous ne pouvez pas noyer la mention du consentement dans un long texte. Dans votre cas, chaque demande de consentement doit faire l'objet d'une case à cocher distincte. Par exemple :

- ☐ « J'accepte de fournir mes données personnelles pour le service fourni » et, séparément,
- ☐ « J'accepte de recevoir les mises à jour du programme par e-mail ».

Anna: Oh, je vois souvent cela sur de nombreux sites web. Et pour vous, dans le secteur public ?



Robert: Nous pouvons collecter des renseignements personnels sans consentement si cela est nécessaire dans le cadre de notre mandat légal, par exemple pour l'évaluation foncière, les demandes de permis ou la facturation des services municipaux. Mais si nous voulons utiliser ces données à d'autres fins, comme l'envoi de courriels marketing à propos d'autres services municipaux, nous devons obtenir le consentement des personnes concernées.



4

Principe de limitation de la collecte dans la Loi 25

Robert: Le quatrième principe est celui de la **limitation de la collecte**. La Loi 25 impose cette exigence de manière très stricte.



Anna: Si je comprends bien, pour le camp d'été de nos enfants, je n'ai pas vraiment besoin du numéro d'assurance maladie de l'enfant simplement pour les inscrire à des activités artistiques et manuelles, n'est-ce pas ?



Robert: Probablement pas ! Vous avez besoin des coordonnées des personnes à contacter en cas d'urgence et peut-être d'informations sur les allergies, mais le numéro d'assurance maladie pourrait être excessif, sauf s'il s'agit d'une activité spécifique liée à la santé.



Anna: Cela va m'obliger à revoir tous nos formulaires et à justifier chaque champ.



Robert: Idem pour moi. Nous passons en revue toutes les demandes de permis et tous les formulaires de demande de service.



5

Principe de limitation de l'utilisation, de la divulgation et de la conservation dans la Loi 25

Anna: Le cinquième principe concerne la **limitation de l'utilisation, de la divulgation et de la conservation**. Ainsi, les renseignements personnels collectés dans un but précis ne peuvent pas être automatiquement utilisés à d'autres fins ?



Robert: Exactement ! Si vous collectez des adresses courriel pour communiquer sur un programme, vous ne pouvez pas ajouter ces utilisateurs automatiquement à votre infolettre sur vos activités de collecte de fonds sans obtenir un consentement complémentaire.

Anna: Qu'en est-il de la conservation ? Combien de temps devons-nous conserver les renseignements personnels dans nos systèmes ?



Robert: La Loi 25 exige la destruction ou l'anonymisation des données une fois les objectifs atteints, mais nous devons également concilier cela avec nos obligations de conservation prévues par la Loi sur les archives.

Anna: Pour nous, cela peut signifier conserver les dossiers du programme à des fins d'assurance, puis les détruire de manière sécurisée lorsqu'ils ne sont plus nécessaires.



6

Principe d'exactitude dans la Loi 25

Robert: Le principe d'**exactitude** exige que les données soient à jour et correctes. La Loi 25 renforce fortement cette exigence.

Anna: Donc, si quelqu'un déménage ou change de contact d'urgence, nous avons besoin de systèmes pour mettre à jour ces informations ?



Robert: Oui, et vous devez également permettre aux personnes de signaler et de corriger facilement les erreurs dans leurs dossiers. Les deux secteurs ont la même obligation à cet égard.



7

Principe de sécurité dans la Loi 25

Anna: Les **mesures de sécurité** concernent la protection des renseignements, n'est-ce pas ? Qu'exige la Loi 25 ?



Robert: Il s'agit essentiellement de trois niveaux de mesures de sécurité : **physique** (armoires de classement verrouillées), **technique** (mots de passe, cryptage) et **organisationnel** (formation du personnel, politiques). Le niveau de protection doit correspondre à la sensibilité des données.



Anna: Oh, je vais peut-être avoir besoin d'un budget supplémentaire pour cela. Les informations financières de nos donateurs doivent-elles bénéficier d'une protection plus forte que notre liste de diffusion générale ?



Robert: Tout à fait ! Et si nous utilisons des services tiers, tels que le stockage en nuage ou des processeurs de paiement, nous avons besoin de contrats qui les obligent à protéger ces données également.



8

Principe d'ouverture dans la Loi 25

Robert: Le principe **d'ouverture** signifie être transparent. La Loi 25 nous oblige à publier des politiques de confidentialité claires sur nos sites web.

Anna: Dans un langage simple que les gens peuvent réellement comprendre ?



Robert: Oui ! Sans jargon juridique. Les gens doivent pouvoir lire votre politique et comprendre ce que vous faites de leurs renseignements personnels.



9

Principe d'accès individuel dans la Loi 25

Anna: L'accès individuel, cela signifie que les personnes peuvent obtenir des copies de leurs propres données ?



Robert: Exactement ! En vertu de la Loi 25, les individus peuvent exercer leur droit d'accès et de rectification, retirer leur consentement ou même exiger que nous cessions de partager leurs renseignements dans certains cas. Nous disposons d'un délai de 30 jours pour donner suite à ces requêtes.

Anna: Existe-t-il un « droit à l'oubli » dans la Loi 25, comme dans le RGPD de l'Union européenne ?



Robert: En quelque sorte. Il existe un droit à la « désindexation » : les gens peuvent demander que nous cessions de diffuser leurs renseignements ou que nous retirions les hyperliens qui y mènent si cela leur porte préjudice. Mais pour nous, dans le secteur public, cela devient complexe en raison des exigences de transparence et de conservation des documents publics.

Anna: Cela semble complexe sur le plan juridique.



Robert: Ça l'est ! C'est pourquoi nous avons besoin de conseils juridiques pour ces demandes.



10

Principe de contestation à respecter dans la Loi 25

Robert: Le dernier principe est **la contestation de la conformité**, qui consiste à offrir un recours en cas de problème.

Anna: Nous avons donc besoin d'une procédure de plainte officielle ?



Robert: Oui, et des procédures d'intervention en cas d'incident. En cas de violation des données, nous devons évaluer le risque et, s'il est grave, en informer à la fois la Commission d'accès à l'information (CAI) et les personnes concernées.

Anna: Mais qu'est-ce qui est considéré comme « grave » ?



Robert: Si la violation peut entraîner un vol d'identité, une fraude financière ou un préjudice important pour les personnes concernées. La Loi 25 exige que nous tenions un registre de tous les incidents, même mineurs.



The consequences of non-Compliance

Anna: Cela fait beaucoup à gérer, mais le fait de suivre ces 10 principes permet de mieux s'organiser. Que se passe-t-il si nous ne nous y conformons pas ?



Robert: Les sanctions sont lourdes. Pour les organisations privées comme la vôtre, les amendes peuvent atteindre 25 millions de dollars ou 4 % du chiffre d'affaires mondial. Pour les organisations publiques comme la mienne, les sanctions financières sont moins sévères, mais la surveillance est plus stricte. De plus, les particuliers peuvent désormais poursuivre directement les organisations en justice pour violation de la vie privée.

Anna: Voilà une motivation sérieuse pour bien faire les choses ! Au moins, nous avons le même organisme de surveillance, le CAI, qui contrôle les deux secteurs.



Robert: En effet. Et les 10 principes nous servent de feuille de route. Si nous les suivons systématiquement, nous serons en bonne voie pour nous conformer à la Loi 25.



Sur la base de la conversation entre Anna et Robert, voyons dans quelle mesure votre organisation répond à ces exigences.

ÉVALUATION RAPIDE DE LA CONFORMITÉ À LA LOI 25

Exigences communes (secteurs privé et public)

Responsabilité : Avez-vous désigné un référent de la protection de la vie privée et avez-vous publié ses coordonnées ?

Identification des fins de collecte : Disposez-vous d'un inventaire documenté de toutes les données à caractère personnel collectées et des finalités de cette collecte ?

Consentement : Existe-t-il un processus permettant d'obtenir le consentement explicite des personnes avant de collecter leurs renseignements personnels (secteur privé) ou pour des utilisations secondaires (secteur public) ?

Limitation de la collecte : Vous assurez-vous que la collecte de données à caractère personnel est limitée à ce qui est nécessaire pour la finalité déclarée ?

Limitation de l'utilisation et de la divulgation : Utilisez-vous les données uniquement aux fins initiales, sauf si vous avez obtenu un consentement supplémentaire pour de nouvelles utilisations ?

Conservation des données : Disposez-vous de procédures pour éliminer ou anonymiser en toute sécurité les données à caractère personnel qui ne sont plus nécessaires ?

Exactitude : avez-vous mis en place des procédures pour maintenir les informations à jour et correctes et traiter les demandes de correction ?

Mesures de protection : Votre organisation dispose-t-elle d'une politique de sécurité complète comprenant des mesures physiques, techniques et organisationnelles proportionnées à la sensibilité des données que vous traitez ?

Transparence : Votre politique de confidentialité est-elle rédigée dans un langage simple et accessible au public ?

Accès individuel : Avez-vous mis en place des procédures pour répondre aux demandes d'accès, de rectification et de portabilité des données dans les délais légaux (30 jours pour le secteur privé, 20 jours pour le secteur public) ?

Contestation de la conformité : Disposez-vous d'un processus de plainte officiel et de réponse aux incidents ?

Confidentialité par défaut : Vos produits/services technologiques sont-ils configurés par défaut avec les paramètres de confidentialité les plus élevés ?

Évaluations d'impact sur la vie privée (EIVP) : Effectuez-vous des évaluations d'impact sur la vie privée dans le cadre de la mise en place de nouveaux systèmes d'information et de transferts transfrontaliers de données ?

Registre des incidents : Tenez-vous un registre de tous les incidents liés à la confidentialité, comme l'exige la Loi 25 ?

Contrats avec des tiers : Avez-vous établi des contrats avec des prestataires de services garantissant qu'ils respectent les exigences de la Loi 25 ?

Prise de décision automatisée : Informez-vous les personnes concernées lorsqu'elles font l'objet d'une prise de décision automatisée ou d'un profilage ?

Exigences supplémentaires pour le secteur public

Mise en place d'un comité obligatoire : Avez-vous mis en place un « comité sur l'accès à l'information et la protection des renseignements personnels » ?

Réponse dans les 20 jours : Êtes-vous en mesure de répondre aux demandes d'accès dans un délai de 20 jours (prolongeable à 30 jours) ?

Intégration des archives : Vos pratiques de conservation sont-elles conformes aux exigences des archives provinciales ?

Notification à la CAI : Avez-vous officiellement informé la CAI de la nomination de votre référent de la protection de la vie privée ?

Exigences supplémentaires pour le secteur privé

Consentement explicite : Obtenez-vous un consentement explicite et détaillé pour les données sensibles et les utilisations secondaires à l'aide de cases distinctes non préalablement cochées ?

Réponse dans les 30 jours : Êtes-vous en mesure de traiter les demandes individuelles dans un délai de 30 jours ?

Droit à la désindexation : Disposez-vous d'un processus pour évaluer les demandes de désindexation des données personnelles ?

Conformité des contrats : Les demandes de consentement sont-elles présentées séparément des autres informations ?

Si vous n'avez pas coché tous les éléments applicables, des mesures immédiates sont à prévoir pour vous conformer à la Loi 25.

Commencez dès aujourd'hui



Nous espérons que ce guide vous a permis de mieux comprendre le cadre national régissant la protection de la vie privée ainsi que vos responsabilités spécifiques en vertu de la Loi 25, tant dans le secteur public que privé.

Nord Ouvert propose un service d'assistance ciblé pour vous accompagner dans votre mise en conformité. Pour en savoir plus sur notre offre de [service en matière de protection de la vie privée, cliquez ici](#) ou contactez-nous à l'adresse courriel info@opennorth.ca.

À propos de Nord Ouvert

Renforcer la confiance dans les données,
pour le bien commun

Nord Ouvert est une organisation à but non lucratif qui se consacre à l'avancement du bien commun. Aux côtés des gouvernements et des organisations à vocation civique de toutes tailles, nous fournissons une expertise en matière de données afin d'éclairer la prise de décision, de stimuler l'innovation, d'améliorer les services publics et les services offerts par la société civile, et de relever les défis les plus urgents de la société.

Notre travail consiste à renforcer la capacité des organisations, à prendre de meilleures décisions concernant la gestion de leurs données afin qu'elles soient utiles, exploitables, sécurisées et dignes de confiance tout au long de leur cycle de vie. Chez Nord Ouvert, nous combinons une expertise approfondie en matière de données avec une approche multidisciplinaire. Notre équipe est composée d'urbanistes, d'ingénieurs en logiciel, d'organiseurs communautaires, de scientifiques des données, de spécialistes en vérification cybernétique et des technologies de l'information, de sociologues, de géographes et de juristes spécialisés dans les technologies, ce qui nous permet d'apporter des perspectives diverses à chaque projet.

Nord Ouvert fait partie de Montréal en commun, un projet mené par la Ville de Montréal dans le cadre du Défi des villes intelligentes, réalisé avec le soutien financier du gouvernement du Canada.

opennorth.ca/fr

À propos du Défi des villes intelligentes et de Montréal en commun

Montréal en Commun est une communauté d'innovation pilotée par la Ville de Montréal dont les partenaires expérimentent des solutions en accès à l'alimentation, en mobilité et en réglementation municipale dans un désir de repenser la ville. Les projets sont mis en œuvre grâce au prix octroyé à la Ville de Montréal par le Gouvernement du Canada dans le cadre du Défi des villes intelligentes.

Auteurs: Cristiano Therrien et Samuel Kohn

Ce travail est protégé par le droit d'auteur de Nord Ouvert sous licence Creative Commons Attribution-NonCommercial 4.0 International ([CC BY-NC 4.0](https://creativecommons.org/licenses/by-nc/4.0/)), à l'exception des photographies, des images, des logos, de la marque et des autres marques de commerce de Nord Ouvert.



Loi 25 : Principes et pratiques en matière de protection
des renseignements personnels