



Rédiger une politique de confidentialité

Guide explicatif
pour les entreprises

Depuis le 22 septembre 2023, vous devez publier une politique de confidentialité si votre entreprise recueille des renseignements personnels par un moyen technologique (par exemple une adresse courriel, un site Web ou une application)¹. Cette politique doit être rédigée en termes clairs et simples.

Ce court guide vise à répondre aux questions suivantes :

- Qu'est-ce qu'une politique de confidentialité ?
- Que devrait contenir une telle politique ?
- Comment rédiger une politique en termes clairs et simples ?

1. Cette obligation est prévue à l'article 8.2 de la [Loi sur la protection des renseignements personnels dans le secteur privé](#).

1. Qu'est-ce qu'une politique de confidentialité ?

1.1 Un moyen d'informer les personnes dont vous recueillez les renseignements personnels

Une politique de confidentialité permet d'informer les personnes dont les renseignements personnels sont recueillis par un moyen technologique, comme les personnes qui visitent un site Web.

Quand une organisation recueille des renseignements personnels auprès de quelqu'un, elle doit lui fournir certaines informations². Si la collecte est faite par un moyen technologique, personne ne fournit ces informations au nom de l'organisation. La politique de confidentialité vise donc à fournir les mêmes informations à la personne concernée. Elle peut aussi inclure d'autres informations utiles pour prendre une décision éclairée.

Elle doit être publiée sur le site Web de l'entreprise, si elle en a un. Elle doit aussi être diffusée de façon à atteindre les personnes concernées, selon le contexte. Par exemple :

- Un lien à consulter avant de passer une commande en ligne;
- Un message affiché à la première utilisation d'une application mobile;
- Un livret inclus dans l'emballage d'un objet connecté, destiné à être lu avant la première utilisation.

2. Ces informations sont listées à l'article 8 de la [Loi sur la protection des renseignements personnels dans le secteur privé](#).

1.2 Qu'est-ce qui n'est pas une politique de confidentialité?

La politique de confidentialité fait partie d'un ensemble de documents liés à vos services et à vos pratiques de gestion des renseignements personnels. Il est important de ne pas confondre ces documents.

Politique de gouvernance ou de protection des renseignements personnels	Consentement	Conditions d'utilisation ou conditions de service
<p>Cette politique décrit la façon dont votre organisation gère les renseignements personnels dans le cadre de ses activités. Elle décrit notamment :</p> <ul style="list-style-type: none"> • Les rôles et responsabilités des membres du personnel dans la gouvernance des renseignements personnels, de leur collecte jusqu'à leur destruction; • Les règles de conservation et de destruction des renseignements personnels; • Le processus de plainte lié à la protection des renseignements personnels. <p>Cette politique s'adresse d'abord à votre organisation, puisqu'elle encadre vos activités, mais elle concerne aussi les personnes de qui vous recueillez les renseignements personnels. Vous pouvez la rendre publique et vous devez au minimum publier des informations détaillées sur vos pratiques.</p>	<p>C'est le processus qui permet à vos utilisateurs d'accepter vos pratiques en lien avec les renseignements personnels. Il peut prendre différentes formes, selon le contexte. Par exemple :</p> <ul style="list-style-type: none"> • Un formulaire papier ou en ligne pour vous autoriser à obtenir un dossier de crédit afin d'évaluer une demande de financement; • Une demande verbale en personne ou au téléphone pour envoyer un sondage à un client; • Une fenêtre pour paramétrer les témoins de connexion (<i>cookies</i>) sur un site Web. <p>Pour être valide, le consentement doit respecter les critères listés dans la loi³. Selon le cas, la demande de consentement peut contenir un hyperlien vers la politique de confidentialité.</p>	<p>Ce sont les règles qui encadrent l'utilisation de votre site Web, de votre application ou de vos services. Elles définissent ce que les utilisateurs et vous avez le droit de faire, et les responsabilités de chacun. Par exemple, elles peuvent inclure :</p> <ul style="list-style-type: none"> • Les utilisations permises et interdites de vos services; • Les cas où vous pouvez mettre fin à l'accès d'un utilisateur; • L'interdiction de reproduire le contenu de votre site ou d'autres règles liées à la propriété intellectuelle. <p>Les conditions d'utilisation ou de service ne sont pas liées aux renseignements personnels. Elles peuvent contenir un renvoi vers une politique de confidentialité, de gouvernance ou de protection des renseignements personnels, mais elles ne doivent pas être fusionnées.</p>

3. Ces critères sont listés à l'article 14 de la *Loi sur la protection des renseignements personnels dans le secteur privé* (RLRQ, c. P-39.1). Consultez les [Lignes directrices sur les critères de validité du consentement](#) pour en savoir plus.

2. Que devrait contenir votre politique de confidentialité?

Un [règlement](#) décrit les informations à inclure dans les politiques de confidentialité des organismes publics. Ce règlement reprend principalement les informations que doit fournir un organisme public quand il recueille des renseignements personnels⁴.

Il n'existe pas de règlement équivalent pour le secteur privé. Le contenu suggéré ici est donc basé sur ce que doit fournir une entreprise quand elle recueille des renseignements personnels, en plus de certains ajouts inspirés du règlement prévu pour le secteur public.

Pour commencer, vous devez indiquer le nom de votre entreprise, la date d'entrée en vigueur de la politique et la date de la dernière mise à jour.

Voici les éléments à inclure ou à considérer.

2.1 La façon dont vous recueillez des renseignements personnels

Vous devez d'abord indiquer les moyens technologiques que vous utilisez pour recueillir des renseignements personnels. Par exemple :

- Les courriels reçus par votre service à la clientèle;
- Un formulaire de demande de rendez-vous en ligne;
- Une application offerte à votre clientèle;
- Certains témoins (*cookies*) de votre site Web;
- De la vidéosurveillance;
- Un objet connecté.

4. Ces informations sont listées à l'article 65 de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (RLRQ, c. A-2.1).

Vous devez aussi nommer les personnes ou les autres organisations qui recueillent des renseignements personnels pour vous, s'il y en a. Par exemple :

- Un fournisseur de services technologiques comme une plateforme de commande ou un gestionnaire d'infolettres;
- Un consultant qui fournit une partie des services que vous offrez à votre clientèle;
- Une agence chargée de répondre aux questions ou de traiter les plaintes de votre clientèle.

Si vous recueillez des renseignements personnels à l'aide d'une technologie permettant d'identifier la personne concernée, de la localiser ou d'en effectuer le profilage⁵ (comme un profil d'investisseur ou de consommateur), vous devez indiquer :

- Le recours à cette technologie;
- La manière d'activer ces fonctions. Elles doivent être désactivées par défaut.

Si vous offrez un produit ou un service technologique qui dispose de paramètres de confidentialité, ces paramètres doivent assurer le plus haut niveau de confidentialité par défaut. Vous pouvez le préciser dans la politique de confidentialité.

2.2 Les renseignements personnels que vous recueillez et ce pourquoi vous les recueillez

Vous devez aussi inclure les renseignements personnels que vous recueillez. Par exemple :

Catégories	Exemples
Renseignements d'identification	Nom, prénom, adresse postale, adresse courriel, numéro de téléphone
Renseignements techniques ou numériques	Adresse IP, date et heure de connexion, pages visitées, actions posées sur un site Web
Renseignements financiers	Salaire, informations de paiements, dossier de crédit
Renseignements de santé	Poids, sexe à la naissance, antécédents de santé, habitudes de vie, prise de médicament
Renseignements démographiques	Âge, origine ethnique, nationalité, lieu de résidence
Renseignements biométriques ⁶	Empreintes digitales, forme du visage, de la main ou de l'iris de l'œil, patron de frappe au clavier, empreinte de la voix

5. L'article 8.1 de la [Loi sur la protection des renseignements personnels dans le secteur privé](#) définit le profilage comme la collecte et l'utilisation de renseignements personnels afin d'évaluer certaines caractéristiques d'une personne physique, notamment à des fins d'analyse du rendement au travail, de la situation économique, de la santé, des préférences personnelles, des intérêts ou du comportement de cette personne.

6. Concernant la biométrie, consultez le guide d'accompagnement publié par la Commission, intitulé [Biométrie : principes à respecter et obligations légales des organisations](#).

Vous devez mentionner les buts pour lesquels vous recueillez ces renseignements personnels. Par exemple :

- Ouvrir un dossier et traiter les demandes de service;
- Expédier les produits commandés;
- Gérer la facturation et traiter les paiements;
- Traiter et résoudre les plaintes et les insatisfactions;
- Offrir des recommandations personnalisées selon le profil d'achat⁷.

Vous devez indiquer les mesures offertes pour refuser la collecte de certains renseignements personnels et les conséquences possibles, s'il y en a. Par exemple :

- Obtenir des renseignements en personne, plutôt que par courriel;
- Faire une commande sans créer de compte et sans obtenir de points de fidélité;
- Refuser les témoins de connexion (*cookies*) et utiliser votre site Web sans bénéficier de certaines fonctionnalités.

2.3 Les personnes qui ont accès aux renseignements personnels

Les catégories de personnes qui ont accès aux renseignements personnels au sein de votre organisation doivent aussi être nommées dans votre politique de confidentialité. Par exemple :

- Le centre de service à la clientèle;
- Le département de la facturation;
- Les personnes responsables de fournir des produits et des services à la clientèle.

Si vous transmettez des renseignements personnels à d'autres personnes ou organisations pour atteindre l'objectif, ou si elles ont accès à des renseignements personnels, vous devez indiquer :

- Les renseignements personnels ou les catégories de renseignements personnels concernés;
- Les buts dans lesquels vous communiquez ces renseignements personnels;
- Les noms ou les catégories de personnes ou d'organisations qui reçoivent ces renseignements personnels ou y ont accès;
- Si des renseignements personnels peuvent être transmis à l'extérieur du Québec.

7. Dans ce cas, comme il s'agit de profilage, les conditions de l'article 8.1 de la [Loi sur la protection des renseignements personnels dans le secteur privé](#) doivent aussi être respectées.

2.4 Vos mesures de sécurité

Vous pouvez inclure une brève description des mesures prises pour assurer la confidentialité et la sécurité des renseignements personnels. Par exemple :

- Des mesures physiques, comme des locaux verrouillés;
- Des mesures technologiques, comme des pare-feu;
- Des mesures administratives, comme l'adoption d'une politique de sécurité de l'information.

2.5 Les droits des personnes concernées par les renseignements personnels

Vous devez indiquer les droits qu'ont les personnes dont vous détenez les renseignements personnels, soit ceux :

- D'accéder aux renseignements personnels que vous détenez à leur sujet;
- De faire rectifier ou de mettre à jour leurs renseignements personnels;
- De déposer une plainte selon le processus prévu dans votre politique et vos pratiques de gouvernance des renseignements personnels.

Vous pouvez aussi inclure :

- Les moyens technologiques offerts pour accéder aux renseignements personnels ou pour les rectifier, s'il y en a (par exemple un dossier accessible en ligne ou un formulaire de demande d'accès);
- Le nom de la personne responsable de la protection des renseignements personnels de votre entreprise et ses coordonnées;
- Les coordonnées de la personne, de l'organisme ou de l'unité administrative qu'il faut contacter pour toute question en lien avec la politique de confidentialité.

3. Conseils pour rédiger une politique claire et simple

La loi impose de rédiger une politique en termes clairs et simples. Pour y arriver, nous vous recommandons de suivre les règles de communication claire ci-dessous.

N'oubliez pas que la clarté s'évalue du point de vue de la personne qui lit, et non de celle qui écrit. Il faut donc être à l'écoute et s'ajuster quand c'est nécessaire.

Tout au long de votre travail, documentez vos réflexions, vos options et vos décisions. Ceci pourrait vous aider à démontrer le sérieux de votre démarche, au besoin.

3.1 Comprendre les besoins de votre public cible

Identifiez vos lecteurs

Déterminez leurs besoins et leurs particularités, notamment leurs compétences linguistiques et leur niveau de connaissance du sujet. Vous pouvez vous appuyer sur une combinaison de données internes et d'études ou de statistiques publiques.

Identifiez leur contexte de lecture

Déterminez la façon dont vos lecteurs accéderont à la politique, le moment et le parcours. Quel est leur objectif au moment de la lecture? Ceci influence leur niveau d'intérêt et le temps consacré à la lecture. Vous pouvez prendre des décisions en conséquence, comme les messages à prioriser et le format du texte.

3.2 Choisir les messages

Sélectionnez l'information pertinente

Allez droit au but. Donnez l'information nécessaire pour comprendre vos pratiques et respecter la loi. Supprimez ce dont vos lecteurs n'ont pas besoin.

Identifiez les messages clés

Tenez compte des besoins et des spécificités de vos lecteurs ainsi que de leur contexte de lecture. Déterminez les éléments les plus importants pour répondre à leurs questions.

Considérez l'ampleur et la sensibilité des renseignements recueillis

Par souci de transparence, identifiez ce qui peut surprendre vos lecteurs ou avoir un impact important sur leur vie privée. Évaluez si certains messages doivent être spécifiquement portés à l'attention des lecteurs.

3.3 Créer une structure claire et apparente

Utilisez des titres clairs et évocateurs qui reprennent vos messages clés

Survoler les titres devrait donner un bon aperçu du contenu de la politique. Vous pouvez tester plusieurs types de titres, comme des phrases ou des questions. Évitez le jargon et les termes techniques.

Créez une hiérarchie de titres qui aide à trouver l'information

Créez des niveaux de titres et de sous-titres clairs et faciles à identifier. Utilisez-les à travers la politique de façon cohérente.

3.4 Choisir votre ton

Restez fidèle au ton de votre organisation

La politique de confidentialité fait partie de vos communications! Tentez de garder le ton habituel de votre organisation.

Adoptez un ton qui invite à la lecture

Rédiger au «vous» et au «nous» peut aider à instaurer une relation de confiance et de proximité, en plus de faciliter la lecture. Faites preuve de considération envers vos lecteurs. Évitez le ton autoritaire, froid ou menaçant.

3.5 Adopter un style clair et précis

Placez les idées principales en début de paragraphe

Donnez l'information complémentaire après les idées principales.

Rédigez des phrases courtes avec une structure simple

Limitez-vous à une idée par phrase. Autant que possible, rassemblez le sujet, le verbe et le complément. Supprimez les mots inutiles.

Utilisez des mots courants

Évitez le langage formel et le jargon. Choisissez des mots habituels que vos lecteurs connaissent. Si un terme technique est nécessaire, ajoutez une explication ou un exemple.

3.6 Optimiser la mise en page

Utilisez un format de texte lisible

Choisissez une police facile à lire et une taille assez grande.

Créez une mise en page aérée

Rédigez des sections et des paragraphes courts. Pour faciliter la lecture, ajoutez des sous-titres aux plus longues sections et raccourcissez les lignes.

Utilisez des éléments visuels, au besoin

Des techniques toutes simples comme des listes à puces ou des tableaux aident à briser la longueur du texte. Vous pouvez aussi créer des éléments visuels ou des schémas explicatifs.

3.7 Tester votre politique

Faites relire la politique par vos collègues

Demandez à quelques personnes de votre organisation de lire la politique. Arrivent-elles à se repérer dans le texte et à comprendre les principaux messages? Quel est leur ressenti en lisant la politique?

Testez votre politique auprès de votre public cible

Vous pouvez le faire de plusieurs façons, par exemple par un sondage, des entrevues individuelles ou des entrevues de groupes. Avec une bonne méthodologie, quelques personnes suffisent généralement à déceler les problèmes.

Adaptez la politique en fonction du résultat des tests

Faites des ajustements et testez à nouveau, au besoin.

3.8 Réévaluer votre politique régulièrement

Maintenez la politique à jour

Réévaluez régulièrement votre politique pour la mettre à jour. Par exemple, vous devrez l'adapter si vos activités évoluent et que vous recueillez de nouveaux renseignements personnels. Tenez aussi compte des questions ou des commentaires que vous pourriez recevoir. Quand vous modifiez votre politique, testez-la à nouveau auprès de votre public cible pour évaluer sa clarté et la compréhension qu'elle permet envers vos pratiques.

Montréal

2045, rue Stanley, bur. 900
Montréal (Québec) H3A 2V4
Téléphone : 514 873-4196

Québec

525, boul. René-Lévesque E,
bur. 2.36
Québec (Québec) G1R 5S9
Téléphone : 418 528-7741



Commission d'accès
à l'information
du Québec

1 888 528-7741 | cai.gouv.qc.ca

Décembre 2023