LA COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC PRÉSENTE UN GUIDE DE RÉDACTION D'UNE POLITIQUE DE CONFIDENTIALITÉ À PUBLIER SUR UN SITE WEB

Publié le 21 décembre, 2023

Catégories: Perspectives, Publications

Depuis l'entrée en vigueur d'importantes modifications[1] à la *Loi sur la protection des renseignements personnels dans le secteur privé* du Québec (la « ***Loi*** »), en septembre 2023, la Commission d'accès à l'information de la province (la « **Commission** ») a publié divers documents d'orientation.

Dans sa mise à jour du 18 décembre, la Commission a publié un court guide sur la rédaction d'une politique de confidentialité simple et claire (*Rédiger une politique de confidentialité – Guide explicatif pour les entreprises*, le « **Guide** »)[2]. Elle note que celui-ci est le premier d'une série d'outils qui seront diffusés au cours des prochains mois pour aider les organisations à comprendre et à respecter leurs obligations en vertu de la *Loi*. Le document vise à définir ce qu'est une politique de confidentialité et ce qu'elle doit contenir. Il donne aussi des conseils sur la manière de rédiger ce document en termes clairs et simples.

Le Guide est publié en français[3]. Nous en présentons ici un sommaire détaillé.

Dans quelles circonstances faut-il rédiger une politique de confidentialité?

Depuis le 22 septembre 2023, toute organisation qui recueille des renseignements personnels par un moyen technologique doit publier une politique de confidentialité sur son site Web. Cette politique doit aussi être rédigée en termes simples et clairs[4].

Quand une organisation recueille des renseignements personnels auprès de quelqu'un, elle doit lui fournir certaines informations. Si la collecte est faite par un moyen technologique, c'est la politique de confidentialité qui fournit ces informations. La politique peut aussi comprendre d'autres informations utiles à la prise d'une décision éclairée.

La Commission définit aussi ce qui n'est pas une politique de confidentialité. La politique de confidentialité fait partie d'un ensemble de documents. Il est important de ne pas la confondre avec les documents suivants :

- la **politique de gouvernance ou de protection des renseignements personnels**, qui décrit la façon

dont une organisation gère les renseignements personnels dans le cadre de ses activités. Ce document décrit notamment 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;[5]

- le **consentement** (qu'il soit demandé dans un formulaire papier, de vive voix ou dans une fenêtre servant à paramétrer les témoins de connexion (*cookies*) sur un site Web),même si la Commission note que la demande de consentement peut contenir un hyperlien vers la politique de confidentialité.
- les **conditions d'utilisation ou conditions de service**, qui encadrent l'utilisation d'un site Web, d'une application ou de services et définissent les droits et les responsabilités des utilisateurs et de l'organisation. Comme le note la Commission, les conditions d'utilisation ou conditions de service peuvent contenir un renvoi vers une politique de confidentialité, de gouvernance ou de protection des renseignements personnels, mais elles ne doivent pas être fusionnées[6].

Contenu d'une politique de confidentialité

Alors qu'un règlement prescrit les informations que doivent contenir les politiques de confidentialité des organismes publics assujettis à la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (la « ***Loi sur les organismes publics*** »)[7], il n'existe pas de règlement équivalent pour le secteur privé. Le contenu suggéré dans le Guide 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.

1. Les moyens utilisés pour recueillir des renseignements personnels

L'organisation doit indiquer les moyens technologiques utilisés pour recueillir des renseignements personnels. Par exemple, les courriels reçus par le service à la clientèle, un formulaire de demande de rendez-vous en ligne, une application offerte à la clientèle, certains témoins (*cookies*) du site Web, de la vidéosurveillance, un objet connecté.

Elle doit aussi nommer les personnes ou les autres organisations qui recueillent des renseignements personnels pour elle, s'il y en a. Par exemple, un fournisseur de services technologiques, un consultant qui fournit une partie des services offerts à la clientèle, une agence chargée de répondre aux questions ou de traiter les plaintes de la clientèle.

Si une organisation recueille des renseignements personnels à l'aide d'une technologie permettant d'identifier la personne concernée, de la localiser ou d'en effectuer le profilage, elle doit aussi indiquer le recours à cette technologie et la manière d'activer ces fonctions. Le Guide précise que ces fonctions doivent être désactivées

par défaut[8]. De plus, si l'organisation offre un produit ou un service technologique qui dispose de paramètres de confidentialité, ces paramètres doivent assurer le plus haut niveau de confidentialité par défaut[9].

2. Les renseignements personnels recueillis et leur usage

L'organisation doit indiquer quels renseignements personnels elle recueille. Par exemple, des renseignements d'identification, de santé, démographiques, biométriques ou financiers ou encore des renseignements techniques ou numériques (comme l'adresse IP ou les actions posées sur un site Web).

Elle doit aussi mentionner les buts pour lesquels elle les recueille. Par exemple, ouvrir un dossier et traiter les demandes de service, expédier les produits commandés, gérer la facturation et traiter les paiements, offrir des recommandations personnalisées. L'organisation doit également indiquer les mesures offertes pour refuser la collecte de certains renseignements personnels et les conséquences possibles. 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 son site Web sans bénéficier de certaines fonctionnalités[10].

3. Les catégories de personnes qui ont accès aux renseignements personnels (au sein de l'organisation et à l'extérieur de celle-ci)

Les catégories de personnes qui ont accès aux renseignements personnels au sein de l'organisation (service à la clientèle, service de la facturation, etc.) doivent être nommées dans la politique de confidentialité[11].

Si, pour atteindre ses objectifs, l'organisation transmet des renseignements personnels à d'autres entités ou leur donne accès à des renseignements personnels, elle doit indiquer :

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

4. Les droits des personnes concernées

L'organisation doit indiquer les droits qu'ont les personnes dont elle détient les renseignements personnels, à savoir :

- accéder aux renseignements personnels détenus à leur sujet (ce qui peut comprendre les moyens technologiques offerts pour accéder aux renseignements personnels ou pour les rectifier, s'il y en a);
- faire rectifier ou mettre à jour leurs renseignements personnels;

- déposer une plainte selon le processus prévu dans la politique et les pratiques de gouvernance des renseignements personnels de l'organisation.

La Commission note que les organisations peuvent aussi fournir le nom et les coordonnées de la personne ou du service à contacter pour toute question sur la politique de confidentialité, de même que le nom et les coordonnées de la personne responsable de la protection des renseignements personnels au sein de l'entreprise[12].

5. Mesures de sécurité

Toujours selon le Guide, l'organisation peut fournir une brève description des mesures physiques, technologiques ou administratives qu'elle prend pour assurer la confidentialité et la sécurité des renseignements personnels.

Conseils pour rédiger une politique claire et simple

La Commission rappelle d'emblée que la clarté s'évalue du point de vue de la personne qui lit, et non de celle qui écrit, et qu'il faut donc être à l'écoute et s'ajuster quand c'est nécessaire. Elle recommande aussi aux organisations de consigner leurs réflexions, options et décisions tout au long du travail de rédaction, ce qui pourrait les aider à démontrer le sérieux de leur démarche, au besoin.

1. **Comprendre les besoins du public cible**, c'est-à-dire : identifier les lecteurs (ainsi que leurs besoins, leurs particularités, leurs compétences linguistiques et leur niveau de connaissance du sujet, en s'appuyant sur des données internes, des études ou des statistiques publiques); et identifier le contexte de lecture (déterminer la façon dont les lecteurs accéderont à la politique, le moment et le parcours, ainsi que leur objectif au moment de la lecture, facteurs qui auront une incidence sur le niveau d'intérêt et le temps consacré à la lecture).
2. **Choisir les messages**, c'est-à-dire : sélectionner l'information nécessaire pour comprendre les pratiques qu'exige la loi (et supprimer ce dont les lecteurs n'ont pas besoin); déterminer les messages clés en tenant compte des besoins et des spécificités des lecteurs et de leur contexte de lecture; et considérer l'ampleur et la sensibilité des renseignements recueillis, en évaluant si certains messages doivent être spécifiquement portés à l'attention des lecteurs (parce qu'ils pourraient les surprendre ou avoir un impact important sur leur vie privée).
3. **Créer une structure claire et apparente**, c'est-à-dire : utiliser des titres clairs et évocateurs qui reprennent vos messages clés, en évitant le jargon et les termes techniques; et créer une hiérarchie de titres et de sous-titres qui aident à trouver l'information et sont employés de façon cohérente dans l'ensemble de la politique.

4. **Rester fidèle au ton de l'organisation, et adopter un ton invitant à la lecture**, c'est-à-dire : garder le ton habituel des communications de l'organisation; et employer un ton favorisant la création d'un lien de confiance (éviter le ton autoritaire, froid ou menaçant).
5. **Adopter un style clair et précis**, c'est-à-dire : placer les idées principales en début de paragraphe; rédiger des phrases courtes avec une structure simple; supprimer les mots inutiles; utiliser des mots courants (éviter le langage formel et le jargon); ajouter une explication ou un exemple si un terme technique est nécessaire.
6. **Optimiser la mise en page**, c'est-à-dire : utiliser un format de texte lisible, en choisissant une police facile à lire et une taille assez grande; créer une mise en page aérée, en rédigeant des sections et des paragraphes courts; utiliser des éléments visuels, au besoin.
7. **Tester la politique**, c'est-à-dire : faire relire la politique par des collègues et la tester auprès du public cible; faire des ajustements en fonction du résultat des tests.
8. **Réévaluer la politique régulièrement** et l'actualiser à mesure que les activités et les pratiques évoluent.

Le groupe Protection de la vie privée et des données de McMillan se fera un plaisir de vous conseiller sur la rédaction de politiques de confidentialité ou sur vos autres obligations en vertu du régime québécois de protection de la vie privée.

[1] Pour en savoir plus sur la portée des modifications en question, consultez nos bulletins antérieurs Adoption du projet de loi no 64 : modernisation du régime de protection de la vie privée et Projet de loi no 64 : aide-mémoire à l'intention des entreprises.
[2] Original en français sur le site Web de la Commission.
[3] La Commission a récemment indiqué, dans son document résumant les commentaires reçus dans le cadre de sa consultation sur le consentement, qu'elle ne pouvait pas traduire le document en anglais sans contrevenir à la Politique linguistique de l'État et aux dispositions de la *Charte de la langue française*.
[4] Voir l'article 8.2 de la *Loi*.
[5] Voir l'article 3.2 de la *Loi* au sujet de l'obligation faite aux organisations d'établir et de mettre en œuvre des politiques et des pratiques de gouvernance, et de publier sur leur site Web des informations détaillées en termes simples et clairs à leur sujet.
[6] La Commission adopte une position comparable dans ses *Lignes directrices 2023-1 – Consentement : critères de validité*, établissant que la demande de consentement doit être présentée séparément des conditions d'utilisation, des politiques de confidentialité et des signatures.
[7] *Règlement sur les politiques de confidentialité des organismes publics recueillant des renseignements personnels par un moyen technologique*, en ligne. Nous notons que, malgré les nombreuses similarités entre les obligations imposées par la *Loi* et celles imposées par la *Loi sur les organismes publics*, des nuances

distinguent les obligations de transparence des entités des secteurs public et privé. Le Secrétariat à la réforme des institutions démocratiques, à l'accès à l'information et à la laïcité a publié un guide similaire qui s'adresse aux entités du secteur public assujetties à la *Loi sur les organismes publics*.

[8] Voir l'article 8.1 de la *Loi*.

[9] Voir l'article 9.1 de la *Loi*.

[10] Nous notons que cette exigence est absente de la formulation de la *Loi*, alors que le paragraphe 65(5) de la *Loi sur les organismes publics* oblige l'organisme public à informer la personne concernée des conséquences d'un refus de répondre à la demande ou, le cas échéant, d'un retrait de son consentement à la communication ou à l'utilisation des renseignements recueillis.

[11] Nous notons qu'en vertu de l'article 8 de la *Loi*, cette information doit être fournie à la personne concernée « sur demande », tandis qu'en vertu de l'article 3.2, l'organisation doit publier sur son site Web des informations détaillées, en termes simples et clairs, au sujet de ses politiques de gouvernance, notamment en ce qui concerne les rôles et responsabilités des membres de son personnel.

[12] Nous notons que l'article 8 de la *Loi* oblige l'organisation à informer la personne concernée des « coordonnées » du responsable de la protection des renseignements personnels, tandis que l'article 3.1 l'oblige à publier « le titre et les coordonnées » de ce responsable, mais n'exige pas la publication de son nom.

par Ayse Gauthier

Mise en garde