Commission d'accès à l'information du Québec

ENTREPRISES

Vers la conformité à la Loi sur le privé

La *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels* apporte des modifications **importantes** à la *Loi sur la protection des renseignements personnels dans le secteur privé* (Loi sur le privé). Il faut les mettre en œuvre dès septembre 2022!

Cet outil vise à vous familiariser avec certaines de vos **nouvelles responsabilités et obligations** (pages 1 et 2), qui entreront en vigueur progressivement en septembre 2022, 2023 et 2024.

Sans être exhaustives, des **pistes d'action** et des **bonnes pratiques** vous sont aussi proposées aux pages 3 et 4 afin de vous aider dans la planification de vos travaux de mise en conformité à la loi.

Ce document présente un contenu générique. Il ne tient pas compte des spécificités propres à chaque entreprise. Les lois et règlements ont priorité en tout temps.

N'hésitez pas à consulter un juriste spécialisé en protection de la vie privée et un spécialiste en sécurité de l'information pour vous accompagner.

Nouvelles responsabilités et obligations des entreprises

Entrée en vigueur le 22 septembre 2022

En plus de respecter vos obligations actuelles en matière de protection des renseignements personnels, à compter du 22 septembre 2022, vous devrez notamment:

1. **Désigner une personne** responsable de la protection des renseignements personnels et publier le titre et les coordonnées du responsable sur le site Internet de l'entreprise ou, si elle n'a pas de site, les rendre accessibles par tout autre moyen approprié.

Vous devrez également, entre autres :

2. En cas d'incident de confidentialité impliquant un renseignement personnel :
    a. prendre les **mesures raisonnables** pour **diminuer les risques** qu'un préjudice soit causé aux personnes concernées et éviter que de nouveaux incidents de même nature ne se produisent;
    b. **aviser la Commission** et la **personne concernée** si l'incident **présente un risque de préjudice sérieux**;
    c. **tenir un registre des incidents** dont une copie devra être transmise à la Commission à sa demande;

3. Respecter le **nouvel encadrement de la communication de renseignements personnels sans le consentement de la personne concernée** à des fins **d'étude, de recherche ou de productions de statistiques** et dans le cadre d'une **transaction commerciale**;
4. Procéder à une **évaluation des facteurs relatifs à la vie privée (ÉFVP)** avant de communiquer des renseignements personnels sans le consentement des personnes concernées à des fins d'étude, de recherche ou de production de statistiques;
5. **Divulguer préalablement** à la Commission la vérification ou la confirmation d'identité faite au moyen de caractéristiques ou de mesures biométriques.

Entrée en vigueur le 22 septembre 2023

En plus de respecter vos obligations en vigueur en matière de protection des renseignements personnels, à compter du 22 septembre 2023, à titre de personne exploitant une entreprise, vous devrez notamment :

1. Avoir établi des **politiques et des pratiques encadrant la gouvernance** des renseignements personnels et publier de l'information détaillée sur celles-ci en **termes simples et clairs** sur le site Internet de l'entreprise ou, si elle n'a pas de site, par tout autre moyen approprié;
2. Réaliser une **évaluation des facteurs relatifs à la vie privée** (ÉFVP) lorsque la Loi l'exige, par exemple avant de communiquer des renseignements personnels à l'extérieur du Québec;
3. Respecter les nouvelles règles entourant le **consentement** à la collecte, à la communication ou à l'utilisation des renseignements personnels;
4. **Détruire** les renseignements personnels lorsque la finalité de leur collecte est accomplie, ou les **anonymiser** pour les utiliser à des fins sérieuses et légitimes, sous réserve des conditions et d'un délai de conservation prévus par une loi;
5. Respecter vos nouvelles obligations **d'information et de transparence** envers les citoyens;
6. Respecter les nouvelles règles de communication de renseignements personnels sans le consentement de la personne concernée **(exercice d'un mandat ou exécution d'un contrat de service ou d'entreprise)**;
7. Respecter les nouvelles règles de **communication des renseignements personnels à l'extérieur du Québec**;
8. Respecter les nouvelles règles d'**utilisation des renseignements personnels**;
9. Prévoir, par défaut, les **paramètres assurant le plus haut niveau de confidentialité** du produit ou du service technologique offert au public;
10. Respecter les nouvelles règles entourant la collecte de renseignements personnels concernant un **mineur**;
11. Respecter le **droit à la cessation de la diffusion, à la réindexation ou à la désindexation** (ou droit à l'oubli);
12. Respecter les nouvelles règles de **communication des renseignements personnels facilitant le processus de deuil**.

Entrée en vigueur le 22 septembre 2024

À compter du 22 septembre 2024, à titre de personne exploitant une entreprise, vous devrez notamment :

- Répondre aux demandes de portabilité des renseignements personnels.

Pistes d’action et bonnes pratiques

D’ici le 22 septembre 2022

1. Si vous êtes la plus haute autorité de l’entreprise et que vous ne souhaitez pas exercer la fonction de **responsable de la protection des renseignements personnels**, désignez une personne pouvant assumer efficacement ce rôle. Par exemple, celle-ci devrait avoir les compétences requises et un pouvoir décisionnel important;
2. Appuyez la personne responsable de la protection des renseignements personnels avec les **ressources nécessaires** (humaines, techniques et financières) pour assurer la réussite de votre mise en conformité;
3. Faites l’**inventaire des renseignements personnels** détenus par votre entreprise (ou pour son compte par un tiers) et évaluez leur sensibilité;
4. Mettez en place des **mesures** pour **prévenir ou limiter les conséquences d’un incident de confidentialité impliquant un renseignement personnel**;
5. Instaurez des pratiques qui vous permettront de **réagir adéquatement et rapidement en cas d’incident de confidentialité** impliquant un renseignement personnel (ex. : plan de réponse aux incidents et directive au personnel);
6. Si vous prévoyez **utiliser une technique biométrique (ex. : empreinte digitale, reconnaissance faciale ou vocale), informez-vous au préalable de vos obligations** en la matière**.**

D’ici le 22 septembre 2023

Pour établir et mettre en œuvre vos **politiques de gouvernance en matière de protection des renseignements personnels**, vous aurez besoin notamment de :

1. Faire l’**inventaire des renseignements personnels** détenus par votre entreprise (ou pour son compte par un tiers) et évaluer leur sensibilité;
2. L’inventaire des renseignements personnels étant évolutif, il importe de **le tenir à jour** pour rendre compte des changements susceptibles d’être survenus au sein de votre entreprise (ex. : nouvelle collecte de renseignements personnels pour un projet) et de **vous assurer de planifier adéquatement vos actions et de respecter toutes vos obligations**;
3. Préciser les **rôles et responsabilités des membres du personnel** impliqués dans la protection des renseignements personnels tout au long de leur cycle de vie.

La réalisation de ces tâches est essentielle pour la mise en œuvre de vos obligations et pour prioriser certaines de vos actions par la suite.

Pour réaliser une évaluation des facteurs relatifs à la vie privée vous aurez besoin d’avoir réalisé les tâches précédentes, mais vous devrez, entre autres :

1. Évaluer la conformité du projet au regard des lois sur la protection des renseignements personnels;
2. Identifier les risques du projet sur la vie privée des personnes concernées;
3. Mettre en place des stratégies et des mesures pour éviter ces risques ou les réduire efficacement;
4. Surveiller l’application de ces mesures et les réviser.

Pour respecter les nouveaux droits des citoyens et vos nouvelles obligations de transparence à leur égard, vous devrez mettre en place les mécanismes (ex. : directive, processus, formulaire ou solution technologique adaptés) qui vous permettront notamment :

1. D'obtenir un consentement valide pour chacune des fins visées au moment de la collecte, et ce, en **termes simples et clairs**;
2. De présenter distinctement la demande de consentement des autres informations fournies si elle est écrite;
3. De fournir les informations prévues par la loi à la personne dont les renseignements sont collectés;
4. D'informer une personne lorsqu'elle fait l'objet d'une décision fondée exclusivement sur un traitement automatisé;
5. D'informer une personne avant de recourir à une technologie permettant de l'identifier, de la localiser ou d'effectuer son profilage et des moyens offerts pour activer ces fonctions;
6. De publier de l'information détaillée sur vos politiques et vos pratiques sur le site Internet de l'entreprise ou, si elle n'a pas de site, de rendre cette information accessible par tout autre moyen approprié;
7. De publier une politique de confidentialité rédigée en **termes simples et clairs** sur le site Internet de votre entreprise et la diffuser par tout moyen propre à atteindre les personnes concernées si vous collectez des renseignements personnels à l'aide d'un moyen technologique tel qu'un site Web;
8. De traiter les demandes et les plaintes des citoyens concernant votre gestion des renseignements personnels.

D'ici le 22 septembre 2024

1. Informez l'équipe responsable de l'entretien, de la mise à jour ou du développement de vos systèmes informatiques que vous avez de nouveaux besoins d'affaires en lien avec le droit à la portabilité des renseignements personnels, à savoir :

    - que vos systèmes permettent de communiquer, sur demande d'une personne concernée, un renseignement personnel informatisé recueilli auprès d'elle, et ce, dans un format technologique structuré et couramment utilisé;

    - que cette communication puisse également se faire à une personne ou à un organisme autorisé par la Loi à recueillir le renseignement, à la demande de la personne concernée.

À noter :

Assurez-vous de **former votre personnel** pour qu'il développe les bons réflexes en matière de protection des renseignements personnels.