

LOI 25 – PREMIER PROJET DE RÈGLEMENT, À VOS MARQUES, PRÊTS, PARTEZ!

Publié le 18 juillet, 2022

Catégories: [Perspectives](#), [Publications](#)

L'application de la *Loi modernisant la protection des renseignements personnels* (ci-après la « **Loi 25** ») au Québec est enclenchée. Nous vous informons dans de récentes publications ([Projet de loi no 64 : aide-mémoire à l'intention des entreprises](#), [Adoption du projet de loi no 64 : modernisation du régime de protection de la vie privée](#)) des nouveautés à venir en matière de protection des renseignements personnels qui s'échelonneront en trois (3) étapes de septembre 2022 à 2024. Les premières démarches visant à décortiquer les nouvelles obligations des assujettis arrivent.

Le premier projet de règlement, *Règlement sur les incidents de confidentialité* (ci-après le « **Projet de Règlement** ») a été publié et entrera en vigueur, avec son obligation corollaire, le 22 septembre 2022.^[1] Nous vous invitons donc à prendre connaissance sans plus attendre des obligations incombant aux entreprises faisant affaire au Québec en matière de gestion des incidents de confidentialité.

La Loi 25 entend par « *incidents de confidentialité* » : tout accès, utilisation, ou communication non autorisé à des renseignements personnels ou encore leur perte ou tout manquement à leur protection. Les entreprises qui soupçonnent qu'un incident de confidentialité portant sur des renseignements personnels qu'elles détiennent s'est produit sont tenues de mettre en place des mesures raisonnables afin de diminuer les risques qu'un préjudice survienne et éviter la répétition d'incidents de même nature.

Incidents de confidentialité comportant un risque de préjudice sérieux : intervention et prévention

Les entreprises devront aviser la CAI, oralement ou par écrit, dès qu'elles soupçonnent qu'un incident de confidentialité susceptible de causer un risque de préjudice sérieux pourrait se produire.^[2] Si certaines informations ne sont pas connues par l'entreprise lorsqu'elle soumet son avis, elle devra les communiquer à la CAI de manière diligente dès qu'elle en prendra connaissance.^[3]

L'avis à la CAI doit contenir les informations suivantes :

- le nom de l'entreprise qui a subi l'incident et son numéro d'entreprise du Québec;
- le nom et les coordonnées de la personne ressource qui gère ce type d'incident;

- une description des renseignements personnels visés par l'incident ou les raisons pour lesquelles il est impossible de les décrire (si les informations sont inconnues);
- une courte description des circonstances entourant l'incident ainsi que sa cause (si elle est connue);
- la date ou la période où l'incident s'est produit ou une approximation (si la période est inconnue);
- la date ou la période lors de laquelle l'organisation a appris l'existence de l'incident;
- le nombre de personnes affectées ainsi que le nombre de personnes résidant au Québec ou une approximation de ce nombre (s'il est inconnu);
- les raisons qui poussent l'entreprise à croire que l'incident constitue un risque de préjudice sérieux, telles que la sensibilité des renseignements personnels ou la possibilité d'une utilisation malveillante, préjudiciable ou entraînant d'autres conséquences dommageables;
- les mesures prises ou que l'entreprise prévoit de prendre pour aviser les personnes concernées et la date de cet avis ou le délai d'exécution envisagé;
- les mesures prises ou que l'entreprise prévoit de prendre suite à l'incident afin de diminuer les risques que de tels préjudices se reproduisent ou d'en atténuer les effets, ainsi que le délai d'exécution envisagé; et
- la mention qu'une personne ou un organisme situé à l'extérieur du Québec et exerçant des fonctions similaires à la CAI a été avisé de l'incident.^[4]

Les entreprises devront informer les personnes dont les renseignements personnels ont été compromis des circonstances entourant l'incident et veiller à ce qu'elles soient adéquatement soutenues dans les démarches subséquentes, en leur transmettant un avis^[5] contenant :

- une description des renseignements personnels visés par l'incident ou les raisons pour lesquelles il est impossible de les décrire (si l'information est inconnue);
- une brève description des circonstances ayant donné lieu à l'incident;
- la date ou la période où l'incident s'est produit, ou une approximation (si la période est inconnue);
- les mesures prises ou que l'entreprise prévoit de prendre suite à l'incident afin de diminuer les risques de préjudice;
- les mesures que l'entreprise suggère aux personnes concernées afin de diminuer le risque de préjudice ou d'en atténuer les effets; et
- les coordonnées que les personnes concernées pourront utiliser pour se renseigner davantage sur l'incident.^[6]

Dans certaines circonstances, les entreprises devront cependant aviser les personnes concernées par un incident de confidentialité par le biais d'un avis public, notamment lorsque :

- i. la transmission d'un avis individuel causerait un préjudice accru à ces personnes;
- ii. l'avis individuel constitue une difficulté excessive pour l'entreprise; ou
- iii. les coordonnées des personnes sont inconnues.[\[7\]](#)

Les entreprises peuvent néanmoins choisir d'émettre un avis public en dehors de ces cas afin d'atténuer le risque de préjudice pendant que l'entreprise coordonne la transmission d'avis individuels aux personnes concernées, qui peut s'avérer un long processus.[\[8\]](#)

La tenue du registre des incidents de confidentialité

La Loi 25 prévoit en outre la tenue obligatoire d'un registre des incidents de confidentialité. Le Projet de Règlement précise le contenu de ce registre, qui doit notamment comprendre :[\[9\]](#)

- une description des renseignements personnels visés par l'incident ou les raisons pour lesquelles il est impossible de faire une telle description (si l'information est inconnue);
- une brève description des circonstances de l'incident;
- la date ou la période à laquelle l'incident s'est produit ou une approximation (si la période est inconnue);
- la date ou la période au cours de laquelle l'entreprise a pris connaissance de l'incident;
- le nombre de personnes affectées ou une estimation (si ce nombre est inconnu);
- les paramètres, tels que la sensibilité des renseignements personnels, la possibilité que leur utilisation soit malveillante, préjudiciable ou qu'elle entraîne d'autres conséquences dommageables, permettant à l'entreprise de déterminer s'il existe ou non un risque de préjudice sérieux pour les personnes concernées;
- les dates de transmission des avis à la CAI et aux personnes visées si l'incident présente un risque de préjudice sérieux et, le cas échéant, la mention que des avis publics ont été donnés et pour quelles raisons; et
- une courte description des mesures prises par l'entreprise suite à l'incident afin de diminuer les risques qu'un autre préjudice similaire ne survienne.[\[10\]](#)

Les entreprises devront conserver ces informations dans leur registre pour une période minimale de cinq (5) ans suivant la prise de connaissance de l'incident.[\[11\]](#)

Les impacts du Projet de Règlement sur votre entreprise

Selon le Projet de Règlement actuel, vous devrez donc, dès le 22 septembre 2022 :

1. Aviser la CAI de tout incident de confidentialité qui pourrait causer un préjudice sérieux en mentionnant dans votre avis tous les éléments énoncés ci-dessus;

2. Aviser les personnes concernées de l'incident de confidentialité en leur transmettant un avis contenant toutes les informations précisées ci-dessus ou par le biais d'un avis public, le cas échéant; et
3. Tenir un registre des incidents de confidentialité avec tous les éléments détaillés ci-dessus durant au moins cinq (5) ans suite à la survenance de chaque incident, le cas échéant.

Veillez noter que le Projet de Règlement constitue une version préliminaire de l'éventuel Règlement à être adopté 45 jours suivant sa publication, soit le 13 août 2022. Ainsi, il n'est présentement pas possible de confirmer le contenu final du Règlement. Nous vous tiendrons informés de tout développement à cet égard. N'hésitez pas à contacter un membre de notre équipe de protection de la vie privée et des données pour toute question relative à la Loi 25.

[1][ps2id id='1' target=''] *Règlement sur les incidents de confidentialité* (projet), (2022) n° 26 G.O. II, 3935, art. 9.

[2][ps2id id='2' target=''] *Ibid.*, art. 3.

[3][ps2id id='3' target=''] *Ibid.*, art. 4.

[4][ps2id id='4' target=''] *Règlement sur les incidents de confidentialité* (projet), (2022) n° 26 G.O. II, 3935, art. 3.

[5][ps2id id='5' target=''] *Ibid.*, art. 5.

[6][ps2id id='6' target=''] *Ibid.*

[7][ps2id id='7' target=''] *Ibid.*, art. 6.

[8][ps2id id='8' target=''] *Ibid.*

[9][ps2id id='9' target=''] *Ibid.*, art. 7.

[10][ps2id id='10' target=''] *Règlement sur les incidents de confidentialité* (projet), (2022) n° 26 G.O. II, 3935, art. 7.

[11][ps2id id='11' target=''] *Ibid.*, art. 8.

par [Candice Hévin](#), [Marie-Eve Jean](#), [Alexandrina Boboc](#) (étudiante en droit)

Mise en garde

Le contenu du présent document ne fournit qu'un aperçu du sujet et ne saurait en aucun cas être interprété comme des conseils juridiques. Le lecteur ne doit pas se fonder uniquement sur ce document pour prendre une décision, mais devrait plutôt obtenir des conseils juridiques précis.

© McMillan S.E.N.C.R.L., s.r.l. 2022