MÉMOIRE AU CONSEIL DES MINISTRES **GOUVERNEMENT DU QUÉBEC**

DE : Monsieur Éric Caire
Ministre responsable de l'Accès à l'information
et de la Protection des renseignements personnels

Le 12.05.2022

TITRE : Projet de règlement sur les incidents de confidentialité

PARTIE ACCESSIBLE AU PUBLIC

1- Contexte

Le 22 septembre 2021, la Loi modernisant des dispositions législatives en matière de protection des renseignements personnels (L.Q. 2021, c. 25) fut sanctionnée (ci-après « Loi »). Essentiellement, cette Loi modernise l'encadrement applicable à la protection des renseignements personnels dans diverses lois, dont la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (RLRQ, chapitre A-2.1) (ci-après « Loi sur l'accès ») et la Loi sur la protection des renseignements personnels dans le secteur privé (chapitre P-39.1) (ci-après « Loi sur le secteur privé »). La Loi incorpore dans la Loi sur l'accès de même que dans la Loi sur le secteur privé des exigences à respecter advenant la survenance d'un incident de confidentialité.

De plus, la Loi modifie la Loi électorale (chapitre E-3.3) afin d'y inclure l'article 127.22 qui indique que, sauf disposition inconciliable avec cette loi, la Loi sur le secteur privé s'appliquera aux renseignements personnels d'électeurs détenus par un parti politique, un député indépendant ou un candidat indépendant (ci-après « les entités politiques »), à l'exception de quelques exclusions. Ainsi, les dispositions incluses dans la Loi sur le secteur privé concernant de nouvelles obligations relatives aux incidents de confidentialité s'appliqueront à ces entités politiques.

2- Raison d'être de l'intervention

La Loi introduit les articles 63.8 dans la Loi sur l'accès et 3.5 dans la Loi sur le secteur privé, dont l'entrée en vigueur est prévue le 22 septembre 2022. La loi définit la notion d'« incident de confidentialité » et précise que, lors de la survenance d'un tel incident, l'organisation doit se demander si ce dernier présente un risque qu'un préjudice sérieux soit causé. Dans le cadre de l'évaluation de ce risque, l'organisation doit considérer notamment la sensibilité des renseignements personnels concernés, les conséquences appréhendées de leur utilisation et la probabilité qu'ils soient utilisés à des fins préjudiciables.

Les articles 63.8 de la Loi sur l'accès et 3.5 de la Loi sur le secteur privé, susmentionnés, visent respectivement à faire en sorte que, lorsqu'un incident de confidentialité présente un risque qu'un préjudice sérieux soit causé, l'organisme public ou la personne qui exploite une entreprise doit avec diligence, en aviser la Commission d'accès à l'information (ci-après « Commission ») ainsi que toute personne dont un renseignement

personnel est concerné par l'incident. Il est indiqué qu'un règlement du gouvernement peut déterminer le contenu et les modalités de ces avis.

La Loi introduit aussi les articles 63.11 dans la Loi sur l'accès et 3.8 dans la Loi sur le secteur privé, lesquels prévoient respectivement que l'organisme ou la personne qui exploite une entreprise doit tenir un registre des incidents de confidentialité, dont un règlement du gouvernement peut déterminer la teneur.

Puisque les articles 3.5 et 3.8 de la Loi sur le secteur privé s'appliqueront aux entités politiques lorsque l'article 127.22 de la Loi électorale entrera en vigueur le 22 septembre 2023, celles-ci devront également transmettre les avis susmentionnés et tenir un registre des incidents de confidentialité.

L'absence de règlement visant à encadrer le contenu et les modalités de ces avis de même que la teneur de ce registre laisserait les organismes publics, les entreprises et les entités politiques perplexes quant à ce qui doit s'y retrouver et pourrait créer de l'incertitude concernant le respect de leurs obligations légales.

De plus, si aucun règlement ne devait être édicté à ce sujet, il est possible de penser qu'une personne pourrait ne pas avoir accès aux mêmes informations, dépendamment du milieu où l'incident de confidentialité se produit. Cela pourrait également faire en sorte que des personnes concernées par un incident de confidentialité soient privées d'informations qui leur seraient utiles de connaître afin de se protéger contre les effets négatifs potentiels en découlant.

3- Objectifs poursuivis

L'adoption de ce projet de règlement vise à encadrer le contenu devant être énoncé autant dans l'avis destiné à la Commission que dans celui devant être transmis aux personnes concernées lorsqu'un incident de confidentialité présente un risque qu'un préjudice sérieux soit causé. Il a aussi pour objectif de faire état des informations devant être colligées dans le registre des incidents de confidentialité.

En plus de fournir des indications précises sur le contenu devant se trouver dans ces documents, le projet de règlement tend vers une harmonisation de ceux-ci, en faisant en sorte que les personnes qui exploitent une entreprise et les entités politiques assujetties à la Loi sur le secteur privé soient, à ce chapitre, tenues de se conformer aux mêmes exigences que les organismes publics assujettis à la Loi sur l'accès. Le projet de règlement permettra donc aux personnes concernées d'avoir accès à des informations uniformes, peu importe le statut de l'organisation ayant fait l'objet de l'incident.

4- Proposition

Il est proposé d'adopter un seul projet de règlement donnant suite tant aux habilitations réglementaires introduites aux articles 63.8 et 63.11 de la Loi sur l'accès, qu'à celles qui seront introduites aux articles 3.5 et 3.8 de la Loi sur le secteur privé, en application de la Loi. Le projet de règlement fournit ainsi un socle réglementaire commun sur lequel les personnes qui exploitent une entreprise, les entités politiques et les organismes publics pourront s'appuyer quant au contenu devant se retrouver dans les avis transmis à la

Commission et aux personnes concernées, ainsi que dans le registre des incidents de confidentialité.

Le projet de règlement prévoit que ces avis doivent notamment contenir de façon commune :

- une description des renseignements personnels visés par l'incident, ou, si cette information n'est pas connue, la raison justifiant l'impossibilité de décrire ces renseignements;

- une brève description des circonstances de l'incident;

- la date ou la période où l'incident a eu lieu ou, si cette dernière n'est pas connue, une approximation de cette période;

- une référence aux mesures que l'organisation a prises ou entend prendre à la suite de la survenance de l'incident, afin de diminuer les risques qu'un préjudice soit causé;

- des coordonnées permettant de se renseigner davantage relativement à l'incident.

D'autres éléments plus spécifiques se trouvent également dans l'un ou l'autre de ces avis. Ainsi, par exemple, l'avis transmis à la Commission devra inclure la date ou la période au cours de laquelle l'organisation a pris connaissance de l'incident, de même que le nombre de personnes concernées par l'incident résidant au Québec et le nombre total de personnes concernées ou, s'ils ne sont pas connus, une approximation de ces nombres, tandis que l'avis destiné aux personnes concernées devra contenir les mesures que l'organisation leur suggère de prendre pour diminuer le risque qu'un préjudice soit causé ou afin d'atténuer un tel préjudice.

En lien avec l'avis transmis à la Commission, précisons qu'une disposition contenue dans le projet de règlement prévoit expressément que si une organisation prend connaissance, après lui avoir transmis cet avis, d'une information devant s'y retrouver en application du projet de règlement, elle doit alors s'assurer que l'information complémentaire soit transmise à la Commission dans les meilleurs délais.

Le projet de règlement prévoit qu'en règle générale, les personnes concernées par l'incident seront avisées (ex. : lettre transmise par la poste, courriel, etc.). Toutefois, si l'un ou l'autre des trois cas d'exception énoncés dans le projet de règlement s'applique, un avis public sera donné (ex. : communication publique dans les médias), à savoir :

- lorsque le fait de transmettre l'avis est susceptible de causer un préjudice accru à la personne concernée;

- lorsque le fait de transmettre l'avis est susceptible de représenter une difficulté excessive pour l'organisation;

- lorsque l'organisation n'a pas les coordonnées de la personne concernée.

Quant au registre, il contiendra essentiellement des informations similaires à l'avis devant être transmis à la Commission. Le projet de règlement, en plus d'en prévoir la teneur, indique que les renseignements y étant contenus doivent être tenus à jour et conservés pendant une période minimale de cinq ans après la date ou la période au cours de laquelle l'organisation a pris connaissance de l'incident.

5- Autres options

L'option consistant à ne pas édicter de règlement n'est pas recommandée, car le contenu des avis et la teneur du registre seraient alors laissés à la discrétion des organismes publics, des entreprises et des entités politiques, ce qui pourrait donner lieu à un manque d'uniformité. Une harmonisation est donc souhaitable.

Qui plus est, lorsque surviennent des incidents de confidentialité et, à plus forte raison, lorsque ceux-ci présentent un risque qu'un préjudice sérieux soit causé et nécessitent une action rapide, les organisations assujetties pourraient se sentir prises au dépourvu et déplorer un manque de repère si aucun règlement n'était adopté à ce sujet. Cela pourrait retarder la communication avec les personnes concernées ce qui, en contexte de survenance d'incident de confidentialité, n'est pas souhaitable. En effet, ces dernières doivent être informées le plus rapidement possible, afin de mettre en place des mesures visant à assurer la protection de leurs renseignements personnels, au besoin.

Soulignons cependant que certains éléments de contenu ont été demandés par la Commission notamment, mais que leur inclusion n'a pas été retenue. Ainsi, celle-ci aurait notamment souhaité qu'une évaluation du risque de préjudice causé par l'incident de confidentialité, comprenant une analyse de divers facteurs, apparaisse dans l'avis lui étant destiné. En tant que solution de compromis, le projet de règlement exige plutôt qu'« une description des éléments qui amènent l'organisation à conclure qu'il existe un risque qu'un préjudice sérieux soit causé aux personnes concernées, tels que la sensibilité des renseignements personnels concernés, les utilisations malveillantes possibles de ces renseignements, les conséquences appréhendées de leur utilisation et la probabilité qu'ils soient utilisés à des fins préjudiciables » figure dans l'avis à la Commission. De même, la Commission aurait aimé que l'avis lui étant transmis contienne un inventaire des mesures de sécurité pertinentes, déjà en place au moment de la survenance de l'incident, et qui visaient à empêcher que ce type d'incident ait lieu. En outre, ces suggestions n'ont pas été retenues, notamment par souci d'harmonisation avec le Règlement fédéral sur les atteintes aux mesures de sécurité (DORS/2018-64), mais aussi afin de ne pas indûment alourdir les démarches administratives devant être accomplies par les organisations ayant fait l'objet d'un incident de confidentialité, dans le but, corrélativement, d'éviter que cela n'allonge le délai avant que la Commission soit avisée.

6- Évaluation intégrée des incidences

Du point de vue des citoyens, un tel projet de règlement tend à harmoniser le contenu auquel ces derniers auront accès advenant qu'un avis leur soit transmis en raison de la survenance d'un incident de confidentialité présentant un risque qu'un préjudice sérieux

soit causé. Le citoyen devrait se sentir mieux informé quant aux circonstances entourant l'incident, mais aussi plus soutenu quant aux démarches qu'il lui est recommandé de faire, le cas échéant, afin de veiller à une protection accrue de ses renseignements personnels.

Pour ce qui est des organismes publics, des entreprises et des entités politiques assujettis, le projet de règlement tend à leur fournir des paramètres en ce qui a trait aux éléments de contenu devant être inclus dans les avis transmis à la Commission et aux personnes concernées, et dans le registre des incidents de confidentialité. Ils seront ainsi mieux outillés et encadrés quant à leurs obligations en semblable contexte. De plus, la tenue obligatoire d'un registre des incidents de confidentialité permettra de conserver une certaine mémoire organisationnelle et une documentation sur les incidents, ce qui pourrait encourager les réflexions relatives aux moyens à mettre en place afin de tenter de diminuer les risques que des incidents de même nature ne resurviennent.

Ajoutons que, selon la perspective gouvernementale, la Loi tend à démontrer de la transparence, afin d'informer les personnes concernées lorsqu'un incident touche leurs renseignements personnels et est susceptible de causer un préjudice sérieux.

Le fait que la Commission soit avisée advenant la survenance d'un incident de confidentialité présentant un risque qu'un préjudice sérieux soit causé et qu'elle puisse consulter le registre des incidents devrait faciliter son analyse de la situation, en lui donnant d'emblée accès à des informations circonstancielles jugées pertinentes. En accédant de façon systématique à ces informations, cela devrait réduire le nombre de demandes d'informations complémentaires qu'elle devra formuler et donc, limiter les cas où, par manque d'informations, l'émission de ses recommandations pourrait être retardée.

7- Consultation entre les ministères et avec d'autres parties prenantes

Des consultations ont été tenues afin d'obtenir des commentaires en lien avec ce projet de règlement.

Du côté du secteur privé, la Fédération des chambres de commerce du Québec, le Conseil du patronat du Québec, Manufacturiers et Exportateurs du Québec et le Conseil québécois du commerce de détail furent rencontrés.

Du côté du secteur public, des représentants de Retraite Québec, de la Régie de l'assurance maladie du Québec, du ministère du Travail, de l'Emploi et de la Solidarité sociale, de Revenu Québec, de l'Autorité des marchés financiers, de la Société de l'assurance automobile du Québec, de la Commission des normes, de l'équité, de la santé et de la sécurité du travail, du ministère de la Cybersécurité et du Numérique, de la Commission d'accès à l'information et du ministère de la Justice ont été consultés.

8- Mise en œuvre, suivi et évaluation

Considérant que les articles 63.8 et 63.11 de la Loi sur l'accès et les articles 3.5 et 3.8 de la Loi sur le secteur privé entreront en vigueur le 22 septembre 2022 en application de la Loi, l'objectif est de faire en sorte que le projet de règlement entre en vigueur au même moment. Toutefois, à l'égard des entités politiques, il entrera en vigueur le 22 septembre

2023, soit en même temps que l'article 127.22 de la Loi électorale, conformément à ce que prévoit la Loi.

Précisons que le projet de règlement ne fait que préciser le contenu des avis et la teneur du registre que la Loi introduit tant dans la Loi sur l'accès que dans la Loi sur le secteur privé. Ces démarches, essentiellement administratives, ne nécessitent pas l'ajout de ressources. Par ailleurs, notons que le Secrétariat à la réforme des institutions démocratiques, à l'accès à l'information et à la laïcité veillera à accompagner les organismes publics assujettis, notamment en leur proposant des documents d'accompagnement.

Concernant la reddition de comptes, il est à noter que la Commission doit produire annuellement un rapport sur ses activités portant sur l'exercice financier précédent. Ce rapport porte notamment sur l'observation de la Loi sur l'accès et de la Loi sur le secteur privé, et sur les moyens dont dispose la Commission pour son application. À cette occasion, la Commission pourra, le cas échéant, faire un suivi par rapport à l'application du projet de règlement. Elle pourrait faire de même dans son rapport quinquennal qui porte notamment sur l'application de la Loi sur l'accès et de la Loi sur le secteur privé. Ces deux rapports sont déposés à l'Assemblée nationale et sont étudiés par une commission de celle-ci.

9- Implications financières

Le projet de règlement ne fait que préciser le contenu des avis et la teneur du registre des incidents de confidentialité qui sont exigés par la Loi sur l'accès et la Loi sur le secteur privé. Le projet de règlement ne nécessite donc pas que des crédits budgétaires supplémentaires soient octroyés pour son application.

Concernant le secteur privé, les coûts proviennent essentiellement des nouvelles dispositions qui seront ajoutées à la Loi sur le secteur privé concernant les incidents de confidentialité, en application de la Loi, et non pas du projet de règlement en tant que tel. Les estimations qui avaient été effectuées dans le contexte de la Loi ont été actualisées dans l'analyse d'impact réglementaire, notamment en fonction des mesures prévues au projet de règlement.

Les coûts récurrents estimés dans l'analyse d'impact réglementaire en considérant les exigences de la Loi sur le secteur privé et le projet de règlement sont de 8 262 430 $ par année. Il n'y aura pas de coût d'implantation.

10- Analyse comparative

Le Règlement fédéral sur les atteintes aux mesures de sécurité, duquel le projet de règlement s'inspire fortement, propose un découpage de sections et des dispositions similaires au contenu du projet de règlement. Il y est notamment question de la déclaration au commissaire et de l'avis à l'intéressé, lesquelles notions sont respectivement assimilables à l'avis à la Commission et l'avis à toute personne dont un renseignement personnel est concerné par l'incident. Le règlement fédéral traite également du fait que l'avis transmis à l'intéressé doit normalement être donné directement, mais qu'en certains cas circonscrits, une transmission par voie indirecte peut être effectuée. Ces cas, qui font

office d'exceptions, sont d'ailleurs les mêmes dans le projet de règlement proposé. Enfin, le règlement fédéral de même que le projet de règlement font tous deux état de la tenue d'un registre.

L'Alberta s'est également doté d'un règlement dont le contenu des avis destinés à l'« Information and Privacy Commissioner » et aux personnes concernées est semblable au projet de règlement.

En Europe, le contenu minimal des avis destinés à l'autorité de contrôle compétente et aux personnes concernées, prévu par le Règlement général sur la protection des données (ci-après « RGPD »), est semblable à ce que propose le projet de règlement. Par ailleurs, les entreprises doivent également documenter toute violation de données à caractère personnel, en indiquant les faits concernant la violation des données à caractère personnel, ses effets et les mesures prises pour y remédier. Ceci correspond à l'obligation de tenir un registre et le contenu prévu au RGPD est semblable à celui du projet de règlement.

Enfin, les États américains disposent également de lois qui obligent les entreprises à déclarer les incidents de confidentialité aux personnes concernées. Le contenu des avis prévu au projet de règlement n'entre pas en conflit avec les législations des États américains.

Le ministre responsable de
l'Accès à l'information et de
la Protection des
renseignements personnels,

Monsieur Éric Caire