

ANNEXE

Dispositions pertinentes de la Loi sur la protection *des renseignements personnels dans le secteur privé* telles qu'elles seront en vigueur au 23 septembre 2023

3.1. Toute personne qui exploite une entreprise est responsable de la protection des renseignements personnels qu'elle détient.

Au sein de l'entreprise, la personne ayant la plus haute autorité veille à assurer le respect et la mise en œuvre de la présente loi. Elle exerce la fonction de responsable de la protection des renseignements personnels; elle peut déléguer cette fonction par écrit, en tout ou en partie, à toute personne.

Le titre et les coordonnées du responsable de la protection des renseignements personnels sont publiés sur le site Internet de l'entreprise ou, si elle n'a pas de site, rendus accessibles par tout autre moyen approprié.

3.2. Toute personne qui exploite une entreprise doit établir et mettre en œuvre des politiques et des pratiques encadrant sa gouvernance à l'égard des renseignements personnels et propres à assurer la protection de ces renseignements. Celles-ci doivent notamment prévoir l'encadrement applicable à la conservation et à la destruction de ces renseignements, prévoir les rôles et les responsabilités des membres de son personnel tout au long du cycle de vie de ces renseignements et un processus de traitement des plaintes relatives à la protection de ceux-ci. Elles doivent également être proportionnées à la nature et à l'importance des activités de l'entreprise et être approuvées par le responsable de la protection des renseignements personnels.

Des informations détaillées au sujet de ces politiques et de ces pratiques, notamment en ce qui concerne le contenu exigé au premier alinéa, sont, en termes simples et clairs, publiées sur le site Internet de l'entreprise ou, si elle n'a pas de site, rendues accessibles par tout autre moyen approprié.

3.5. Une personne qui exploite une entreprise et qui a des motifs de croire que s'est produit un incident de confidentialité impliquant un renseignement personnel qu'elle détient doit prendre les mesures raisonnables pour diminuer les risques qu'un préjudice soit causé et éviter que de nouveaux incidents de même nature ne se produisent.

Si l'incident présente un risque qu'un préjudice sérieux soit causé, elle doit, avec diligence, aviser la Commission d'accès à l'information instituée par l'article 103 de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (chapitre A-2.1). Elle doit également aviser toute personne dont un renseignement personnel est concerné par l'incident, à défaut de quoi la Commission peut lui ordonner de le faire. Elle peut également aviser toute personne ou tout organisme susceptible de diminuer ce risque, en ne lui communiquant que les renseignements personnels nécessaires à cette fin sans le consentement de la personne concernée. Dans ce dernier cas, le responsable de la protection des renseignements personnels doit enregistrer la communication.

Malgré le deuxième alinéa, une personne dont un renseignement personnel est concerné par l'incident n'a pas à être avisée tant que cela serait susceptible d'entraver une enquête faite par une personne ou par un organisme qui, en vertu de la loi, est chargé de prévenir, détecter ou réprimer le crime ou les infractions aux lois.

Un règlement du gouvernement peut déterminer le contenu et les modalités des avis prévus au présent article.

3.6. Pour l'application de la présente loi, on entend par « incident de confidentialité » :

- 1° l'accès non autorisé par la loi à un renseignement personnel;
- 2° l'utilisation non autorisée par la loi d'un renseignement personnel;
- 3° la communication non autorisée par la loi d'un renseignement personnel;
- 4° la perte d'un renseignement personnel ou toute autre atteinte à la protection d'un tel renseignement.

3.7. Lorsqu'elle évalue le risque qu'un préjudice soit causé à une personne dont un renseignement personnel est concerné par un incident de confidentialité, la personne qui exploite une entreprise doit considérer notamment la sensibilité du renseignement concerné, les conséquences appréhendées de son utilisation et la probabilité qu'il soit utilisé à des fins préjudiciables. Elle doit également consulter son responsable de la protection des renseignements personnels.

3.8. La personne qui exploite une entreprise doit tenir un registre des incidents de confidentialité. Un règlement du gouvernement peut déterminer la teneur de ce registre.

Sur demande de la Commission, une copie de ce registre lui est transmise.

8. La personne qui recueille des renseignements personnels auprès de la personne concernée doit, lors de la collecte et par la suite sur demande, l'informer:

- 1° des fins auxquelles ces renseignements sont recueillis;
- 2° des moyens par lesquels les renseignements sont recueillis;
- 3° des droits d'accès et de rectification prévus par la loi;
- 4° de son droit de retirer son consentement à la communication ou à l'utilisation des renseignements recueillis.

Le cas échéant, la personne concernée est informée du nom du tiers pour qui la collecte est faite, du nom des tiers ou des catégories de tiers à qui il est nécessaire de communiquer les renseignements aux fins visées au paragraphe 1° du premier alinéa et de la possibilité que les renseignements soient communiqués à l'extérieur du Québec.

Sur demande, la personne concernée est également informée des renseignements personnels recueillis auprès d'elle, des catégories de personnes qui ont accès à ces renseignements au sein de l'entreprise, de la durée de conservation de ces renseignements, ainsi que des coordonnées du responsable de la protection des renseignements personnels.

L'information doit être transmise à la personne concernée en termes simples et clairs, quel que soit le moyen utilisé pour recueillir les renseignements.

12. Un renseignement personnel ne peut être utilisé au sein de l'entreprise qu'aux fins pour lesquelles il a été recueilli, à moins du consentement de la personne concernée. Ce consentement doit être manifesté de façon expresse dès qu'il s'agit d'un renseignement personnel sensible.

Un renseignement personnel peut toutefois être utilisé à une autre fin sans le consentement de la personne concernée dans les seuls cas suivants:

1° lorsque son utilisation est à des fins compatibles avec celles pour lesquelles il a été recueilli;

2° lorsque son utilisation est manifestement au bénéfice de la personne concernée;

3° lorsque son utilisation est nécessaire à des fins de prévention et de détection de la fraude ou d'évaluation et d'amélioration des mesures de protection et de sécurité;

4° lorsque son utilisation est nécessaire à des fins de fourniture ou de livraison d'un produit ou de prestation d'un service demandé par la personne concernée;

5° lorsque son utilisation est nécessaire à des fins d'étude, de recherche ou de production de statistiques et qu'il est dépersonnalisé.

Pour qu'une fin soit compatible au sens du paragraphe 1° du deuxième alinéa, il doit y avoir un lien pertinent et direct avec les fins auxquelles le renseignement a été recueilli. Toutefois, ne peut être considérée comme une fin compatible la prospection commerciale ou philanthropique. Pour l'application de la présente loi, un renseignement personnel est :

1° dépersonnalisé lorsque ce renseignement ne permet plus d'identifier directement la personne concernée;

2° sensible lorsque, de par sa nature notamment médicale, biométrique ou autrement intime, ou en raison du contexte de son utilisation ou de sa communication, il suscite un haut degré d'attente raisonnable en matière de vie privée.

Toute personne qui exploite une entreprise et qui utilise des renseignements dépersonnalisés doit prendre les mesures raisonnables afin de limiter les risques que quiconque procède à l'identification d'une personne physique à partir de renseignements dépersonnalisés.

13. Nul ne peut communiquer à un tiers les renseignements personnels qu'il détient sur autrui, à moins que la personne concernée n'y consente ou que la présente loi ne le prévoie.

Le consentement doit être manifesté de façon expresse dès qu'il s'agit d'un renseignement personnel sensible.

14. Un consentement prévu à la présente loi doit être manifeste, libre, éclairé et être donné à des fins spécifiques. Il est demandé à chacune de ces fins, en termes simples et clairs. Lorsque la demande de consentement est faite par écrit, elle doit être présentée distinctement de toute autre information communiquée à la personne concernée. Lorsque celle-ci le requiert, il lui est prêté assistance afin de l'aider à comprendre la portée du consentement demandé.

Le consentement du mineur de moins de 14 ans est donné par le titulaire de l'autorité parentale ou par le tuteur. Le consentement du mineur de 14 ans et plus est donné par le mineur, par le titulaire de l'autorité parentale ou par le tuteur.

Le consentement ne vaut que pour la durée nécessaire à la réalisation des fins auxquelles il a été demandé.

Un consentement qui n'est pas donné conformément à la présente loi est sans effet.

20. Dans l'exploitation d'une entreprise, un renseignement personnel n'est accessible, sans le consentement de la personne concernée, à tout préposé ou agent de l'exploitant qui a qualité pour le connaître qu'à la condition que ce renseignement soit nécessaire à l'exercice de ses fonctions.

23. Lorsque les fins auxquelles un renseignement personnel a été recueilli ou utilisé sont accomplies, la personne qui exploite une entreprise doit le détruire ou l'anonymiser pour l'utiliser à des fins sérieuses et légitimes, sous réserve d'un délai de conservation prévu par une loi.

Pour l'application de la présente loi, un renseignement concernant une personne physique est anonymisé lorsqu'il est, en tout temps, raisonnable de prévoir dans les circonstances qu'il ne permet plus, de façon irréversible, d'identifier directement ou indirectement cette personne.

Les renseignements anonymisés en vertu de la présente loi doivent l'être selon les meilleures pratiques généralement reconnues et selon les critères et modalités déterminés par règlement.

32. Le responsable de la protection des renseignements personnels doit répondre par écrit à la demande d'accès ou de rectification, avec diligence et au plus tard dans les 30 jours de la date de réception de la demande.

À défaut de répondre dans les 30 jours de la réception de la demande, la personne est réputée avoir refusé d'y acquiescer.

33. L'accès aux renseignements personnels est gratuit.

Toutefois, des frais raisonnables peuvent être exigés du requérant pour la transcription, la reproduction ou la transmission de ces renseignements.

La personne qui exploite une entreprise et qui entend exiger des frais en vertu du présent article doit informer le requérant du montant approximatif exigible, avant de procéder à la transcription, la reproduction ou la transmission de ces renseignements.

34. Le responsable de la protection des renseignements personnels doit motiver tout refus d'acquiescer à une demande et indiquer la disposition de la loi sur laquelle ce refus s'appuie, les recours qui s'offrent au requérant en vertu de la présente loi et le délai dans lequel ils peuvent être exercés. Il doit également prêter assistance au requérant qui le demande pour l'aider à comprendre le refus.