LAVIN GOSSELIN
AVOCATS · MÉDIATEURS

Politique et procédure de gestion des incidents de confidentialité

(article 3.2 de la Loi sur la protection des renseignements personnels dans le secteur privé, chapitre P-39.1 et Règlement sur les incidents de confidentialité ;
Loi sur le Barreau, chapitre B-1 et ses règlements)

PRÉAMBULE

Le cabinet est responsable de la protection des renseignements personnels qu'il détient. Les renseignements personnels sont confidentiels, sauf dans la mesure prévue par la législation. Toute personne qui, dans le cadre de ses fonctions, a accès à un renseignement personnel détenu par le cabinet doit prendre les moyens nécessaires pour en assurer la protection et la confidentialité. La présente procédure détermine les mesures à prendre pour diminuer les risques qu'un préjudice soit causé, dans de tel cas, et éviter que de nouveaux incidents de même nature se produisent.

1. OBJECTIF ET CADRE NORMATIF

La présente procédure précise les démarches à effectuer lorsque le cabinet a des motifs raisonnables de croire que s'est produit un incident de confidentialité, impliquant un renseignement personnel qu'elle détient, ou si un tel incident est avéré, et ce, conformément à la Loi sur la protection des renseignements personnels dans le secteur privé, chapitre P-39.1 et le Règlement sur les incidents de confidentialité).

2. DÉFINITIONS

Les définitions à considérer pour l'application de la présente procédure, pouvant être complétées par tout autre règlement, politique, directive ou procédure y faisant référence, sont les suivantes :

Incident de confidentialité : accès, utilisation, communication d'un renseignement personnel non autorisé par la loi, de même que sa perte ou toute autre forme d'atteinte à sa protection.

En voici quelques exemples :

- Un membre du personnel consulte des renseignements personnels non nécessaires à l'exercice de ses fonctions ;
- Un pirate informatique s'infiltre dans un système ;
- Une personne utilise des renseignements personnels d'une base de données à

laquelle il a accès dans le cadre de ses fonctions dans le but d'usurper l'identité d'une personne ;

- Une communication est effectuée par erreur à la mauvaise personne ;
- Une personne perd ou se fait voler des documents contenant des renseignements personnels ;
- Une personne s'immisce dans une banque de données contenant des renseignements personnels afin de les altérer.

Renseignement personnel : tout renseignement qui concerne une personne physique et qui permet de l'identifier. Le nom d'une personne, pris isolément, n'est pas un renseignement personnel. Cependant, lorsque ce nom est associé ou jumelé à un autre renseignement visant cette même personne, il devient alors un renseignement personnel.

Voici des exemples de renseignement personnel :

- Le nom d'une personne et sa date de naissance ;
- Numéro d'assurance sociale ;
- Numéro de carte de crédit ;
- Numéro d'assurance maladie ;
- Numéro de permis de conduire ;
- Renseignement de nature médicale ou financière ;
- Le nom d'une personne et son numéro de téléphone personnel ;
- Le nom d'une personne et son adresse de domicile.

Renseignement personnel sensible : un renseignement personnel est considéré comme sensible lorsque, 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 respect de la vie privée.

Il peut s'agir, par exemple, de renseignements médicaux, biométriques, génétiques ou financiers, ou de renseignements sur l'origine ethnique, la conviction politique, la vie ou l'orientation sexuelle, les convictions religieuses.

3. PROTECTION DES RENSEIGNEMENTS PERSONNELS

Le cabinet met en place des mesures de sécurité appropriées et raisonnables afin de protéger les renseignements personnels contre la perte ou le vol, et contre l'accès, la divulgation, la copie, l'utilisation ou la modification non autorisés par la loi. Seuls les membres du personnel qui doivent absolument avoir accès aux renseignements personnels dans le cadre de leurs fonctions sont autorisés à y accéder.

Les personnes membres du personnel du cabinet ou qui travaillent en son nom doivent, notamment :

- Faire des efforts raisonnables pour minimiser le risque de divulgation non intentionnelle de renseignements personnels;

- Prendre des précautions particulières pour s'assurer que les renseignements personnels ne sont pas surveillés, entendus, consultés ou perdus lorsqu'elles travaillent dans des locaux autres que les bureaux du cabinet;

et

- Prendre des mesures raisonnables pour protéger les renseignements personnels lorsqu'elles se déplacent d'un endroit à l'autre.

4. SIGNALEMENT D'UN INCIDENT DE CONFIDENTIALITÉ

Toute personne à laquelle le cabinet communique des renseignements personnels (collègues, fournisseurs, partenaires, experts incluant les sous-traitants) doit effectuer un signalement lorsqu'elle a un motif raisonnable de croire que s'est produit un incident de confidentialité impliquant un renseignement personnel détenu par le cabinet. Pour ce faire, ce signalement doit être effectué sans délai à la personne responsable de la protection des renseignements personnels

Le membre du cabinet ou un membre du personnel qui a un motif raisonnable de croire que s'est produit un incident de confidentialité impliquant un renseignement personnel détenu par le cabinet doit aussi aviser son supérieur hiérarchique ou la personne responsable de la protection des renseignements personnels sans délai.

5. PERSONNES RESPONSABLE DES RENSEIGNEMENTS PERSONNELS (*PRP*) : RÔLES ET RESPONSABLITÉS

La personne responsable de la protection des renseignements personnels (ci-après « *PRP* ») pour le cabinet est Me Erica Gosselin. Il peut être rejoint aux coordonnées suivantes :

- Courriel : egosselin@lagavocats.com
- Téléphone : 450-266-1666

Son rôle est notamment de :

- Contribuer à la mise en place du processus de gestion des incidents de sécurité de l'information ;

- Tenir à jour le registre des incidents de sécurité de l'information ayant pu mettre en péril la sécurité de l'information, de documenter ces incidents et d'en tenir informé la directrice ou le directeur de la sécurité de l'information ainsi que la secrétaire générale ou le secrétaire général ;
- Contribuer aux analyses de risques de sécurité de l'information afin d'identifier les menaces et les situations de vulnérabilité et de mettre en place les solutions appropriées.

En cas d'incident de confidentialité, la personne responsable de la protection des renseignements personnels prend en charge le traitement de l'incident et s'associe avec toute autre personne utile selon la nature de l'incident.

À ce titre, la *PRP* :

- Évalue le risque qu'un préjudice soit causé et en détermine le degré de sévérité. Lors de cette évaluation, sont considérées notamment la sensibilité du renseignement concerné, les conséquences appréhendées de son utilisation et la probabilité qu'il soit utilisé à des fins préjudiciables.

- Avise, avec diligence, la personne dont un renseignement personnel est concerné par l'incident, lorsqu'il présente un risque qu'un préjudice sérieux soit causé, sauf lorsque 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. Cet avis doit contenir les renseignements suivants :

  a. Une description des renseignements personnels visés par l'incident ou, si cette information n'est pas connue, la raison justifiant l'impossibilité de fournir une telle description ;
  b. Une brève description des circonstances de l'incident ;
  c. La date ou la période où l'incident a eu lieu ou, si cette dernière n'est pas connue, une approximation de cette période ;
  d. Une brève description des 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 ;
  e. Les mesures que l'organisation suggère à la personne concernée de prendre afin de diminuer le risque qu'un préjudice lui soit causé ou afin d'atténuer un tel préjudice ;
  f. Les coordonnées permettant à la personne concernée de se renseigner davantage relativement à l'incident.

- Avise, le cas échéant, toute personne ou tout organisme susceptible de diminuer le risque, en ne lui communiquant que les renseignements personnels nécessaires à cette fin, sans le consentement de la personne concernée.

- Avise, avec diligence et par écrit, la Commission d'accès à l'information de l'incident de confidentialité lorsqu'il présente un risque qu'un préjudice sérieux soit causé. L'avis doit contenir les renseignements suivants :

  a. Le nom du cabinet et le numéro d'entreprise du Québec qui lui est attribué en vertu de la Loi sur la publicité légale des entreprises ;

  b. Le nom et les coordonnées de la personne à contacter au sein du cabinet relativement à l'incident ;

  c. Une description des renseignements personnels visés par l'incident ou, si cette information n'est pas connue, la raison justifiant l'impossibilité de fournir une telle description ;

  d. Une brève description des circonstances de l'incident et, si elle est connue, sa cause ;

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

  f. La date ou la période au cours de laquelle le cabinet a pris connaissance de l'incident ;

  g. Le nombre de personnes concernées par l'incident et, parmi celles-ci, le nombre de personnes qui résident au Québec ou, s'ils ne sont pas connus, une approximation de ces nombres ;

  h. Une description des éléments qui amènent le cabinet à conclure qu'il existe un risque qu'un préjudice sérieux soit causé aux personnes concernées, telles 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 ;

  i. Les mesures que le cabinet a prises ou entend prendre afin d'aviser les personnes dont un renseignement personnel est concerné par l'incident, de même que la date où les personnes ont été avisées ou le délai d'exécution envisagé ;

  j. Les mesures que le cabinet a prises ou entend prendre à la suite de la survenance de l'incident, notamment celles visant à diminuer les risques qu'un préjudice soit causé ou à atténuer un tel préjudice et celles visant à éviter que de nouveaux incidents de même nature ne se produisent, de même que le délai où les mesures ont été prises ou le délai d'exécution envisagé ;

k. Le cas échéant, une mention précisant qu'une personne ou un organisme situé à l'extérieur du Québec et exerçant des responsabilités semblables à celles de la Commission d'accès à l'information à l'égard de la surveillance de la protection des renseignements personnels a été avisé de l'incident.

- Avise, avec diligence, les assureurs du cabinet, le cas échéant.
- Inscris l'incident de confidentialité dans le registre prévu à cet effet.
- Sur demande de la Commission d'accès à l'information, transmets une copie de ce registre.

6. REGISTRE DES INCIDENTS DE CONFIDENTIALITÉ

Le cabinet doit tenir un registre des incidents de confidentialité.

6.1 Durée de conservation des renseignements contenus au registre

Les renseignements contenus au registre doivent être tenus à jour et conservés pendant la plus longue des deux périodes ci-après : pendant une période minimale de cinq ans après la date à laquelle le cabinet a pris connaissance de l'incident ou la période requise par le Barreau du Québec pour la conservation des dossiers.

7. ENTRÉE EN VIGUEUR

La présente procédure entre en vigueur le 22 septembre 2023

Signé à Cowansville, ce 22 septembre 2023.

Me Erica Gosselin, avocate et propriétaire
Lavin Gosselin avocats inc.