Politique encadrant la gouvernance des renseignements personnels et procédure de gestion des incidents de confidentialité

(Loi sur la protection des renseignements personnels dans le secteur privé, chapitre P-39.1 et Règlement sur les incidents de confidentialité)

PRÉAMBULE

L'entreprise doit prendre les mesures de sécurité propres à assurer la protection des renseignements personnels collectés, utilisés, communiqués, conservés ou détruits et qui sont raisonnables compte tenu, notamment, de leur sensibilité, de la finalité de leur utilisation, de leur quantité, de leur répartition et de leur support. L'entreprise est responsable de la protection des renseignements personnels qu'elle détient. Les renseignements personnels sont confidentiels, sauf dans la mesure prévue par la loi.

L'exploitant de l'entreprise doit veiller à ce que les dossiers qu'elle détient sur autrui soient à jour et exacts au moment où elle les utilise pour prendre une décision relative à la personne concernée.

L'utilisation des renseignements contenus dans un dossier n'est permise, une fois l'objet du dossier accompli, qu'avec le consentement de la personne concernée, sous réserve du délai prévu par la loi ou par un calendrier de conservation établi par règlement du gouvernement.

Nul ne peut communiquer à un tiers les renseignements personnels contenus dans un dossier qu'il détient sur autrui ni les utiliser à des fins non pertinentes à l'objet du dossier, à moins que la personne concernée n'y consente ou que la loi ne le prévoie.

Toute personne qui, dans le cadre de ses fonctions, a accès à un renseignement personnel détenu par l'entreprise doit prendre les moyens nécessaires pour en assurer la protection et la confidentialité. La présente procédure détermine notamment 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

1.1. La présente procédure précise les démarches à effectuer lorsque l'entreprise 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

2.1. 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 :

2.2. **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.

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.

2.3. **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 ;
- 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.

2.4. **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

3.1. L'entreprise 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.

3.2. Les personnes membres du personnel de l'entreprise ou qui travaillent en son nom doivent, notamment :

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

3.2.2. 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 leurs bureaux habituels;

et

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

4. COLLECTE, UTILISATION, CONSERVATION ET DESTRUCTION DES RENSEIGNEMENTS PERSONNELS

4.1. L'entreprise collecte les renseignements et constitue un dossier sur une personne lorsqu'elle a un intérêt sérieux et légitime pour ce faire en fonction de son mandat. La collecte est limitée aux renseignements nécessaires aux fins de son mandat. En cas de doute, un renseignement est réputé non nécessaire. Les renseignements sont collectés par des moyens légaux et légitimes, soit directement auprès de la personne concernée ou auprès de personnes autorisées par celle-ci. Avant de collecter les renseignements, l'entreprise obtient le consentement des personnes concernées.

4.2. L'entreprise ne peut pas recueillir de renseignements personnels auprès d'un tiers sans le consentement de la personne concernée ou d'une exception légale. Elle peut toutefois le faire, si elle a un intérêt sérieux et légitime, dans l'un des deux cas suivants :

4.2.1. Les renseignements sont recueillis dans l'intérêt de la personne concernée et ne peuvent être recueillis auprès de celle-ci en temps opportun;

4.2.2. La cueillette auprès d'un tiers est nécessaire pour s'assurer de l'exactitude des renseignements.

4.3. L'entreprise utilise les renseignements personnels durant la période de son mandat. L'accès aux renseignements personnels est limité aux seules personnes, parmi le responsable de l'entreprise, une personne qui travaille en son nom ou un membre du personnel, lorsque ces renseignements sont nécessaires à l'exercice de leurs fonctions. Une fois le mandat de l'entreprise accompli, l'entreprise doit obtenir le consentement de la personne concernés pour utiliser ses renseignements.

4.4. L'entreprise doit obtenir le consentement des personnes concernées pour communiquer leurs renseignements à un tiers, à moins d'une exception prévue dans la Loi sur la protection des renseignements personnels dans le secteur privé. L'entreprise, si elle communique des renseignements personnels sans le consentement de la personne concernée, respecte les obligations prévues par la Loi sur la protection des renseignements personnels dans le secteur privé pour ce faire. L'entreprise respecte les obligations particulières applicables à la communication de renseignements personnels à l'extérieur du Québec.

4.5. L'entreprise conserve les renseignements personnels, sous quelque forme que ce soit, en s'assurant que ces renseignements sont à jour et exacts au moment où elle les utilise. L'entreprise prend les mesures de sécurité propres à assurer la sécurité des renseignements personnels et à en préserver la confidentialité.

4.6. L'entreprise détruit les renseignements personnels de manière sécuritaire dès que la finalité pour laquelle ils ont été collectés est accomplie, sous réserve du délai prévu par la loi ou par un calendrier de conservation établi par règlement du gouvernement (ex. pour des obligations fiscales). La méthode de destruction est adaptée au support et au niveau de confidentialité des documents et assure la destruction définitive des renseignements personnels qu'ils contiennent.

4.7. L'entreprise mets en place des mesures de sécurité propres à assurer la protection des renseignements personnels collectés, utilisés, communiqués, conservés ou détruits. Ces mesures sont raisonnables compte tenu, notamment, de la sensibilité, de la finalité, de la quantité, de la répartition et du support des renseignements personnels.

4.8. L'entreprise permet l'exercice des droits d'accès et de rectification et répondre avec diligence, dans les 30 jours, aux demandes d'accès aux renseignements personnels et de rectification soumises par les personnes concernées. L'absence de réponse dans ce délai équivaut à un refus. Un client peut contester un refus ou une réponse jugée insatisfaisante en exerçant son droit de recours devant la Commission d'accès à l'information.

4.9. Sur demande, l'entreprise doit fournir à la personne concernée les informations suivantes :

4.9.1. Renseignements personnels qui sont recueillis auprès d'elle;

4.9.2. Catégories de personnes qui ont accès à ces renseignements au sein de l'entreprise;

4.9.3. Durée de conservation des renseignements personnels;

4.9.4. Coordonnées du responsable de la protection des renseignements personnels.

5. SIGNALEMENT D'UN INCIDENT DE CONFIDENTIALITÉ

5.1. Toute personne à laquelle l'entreprise 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 l'entreprise. Pour ce faire, ce signalement doit être effectué sans délai à la personne responsable de la protection des renseignements personnels.

5.2. Le responsable de l'entreprise, une personne qui travaille en son nom 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 l'entreprise doit aussi aviser son supérieur hiérarchique ou la personne responsable de la protection des renseignements personnels sans délai.

6. PERSONNE RESPONSABLE DES RENSEIGNEMENTS PERSONNELS (*PRP*) : RÔLES ET RESPONSABLITÉS

6.1. La personne responsable de la protection des renseignements personnels (ci-après « *PRP* ») pour l'entreprise est **Madame Trycia Turcotte**. Elle peut être rejointe aux coordonnées suivantes :

Téléphone : 581-372-0832
Courriel : trycia.professeure.chant@gmail.com

6.2. Son rôle est notamment de :

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

6.2.2. 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 ;

6.2.3. 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.

6.3. 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.

6.4. À ce titre, la *PRP* :

6.4.1. 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.

6.4.2. 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 :

6.4.2.1. 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 ;

6.4.2.2. Une brève description des circonstances de l'incident ;

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

6.4.2.4. 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 ;

6.4.2.5. 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 ;

6.4.2.6. Les coordonnées permettant à la personne concernée de se renseigner davantage relativement à l'incident.

6.4.3. 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.

6.4.4. 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 :

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

6.4.4.2. Le nom et les coordonnées de la personne à contacter au sein de l'entreprise relativement à l'incident ;

6.4.4.3. 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 ;

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

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

6.4.4.6. La date ou la période au cours de laquelle l'entreprise a pris connaissance de l'incident ;

6.4.4.7. 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 ;

6.4.4.8. Une description des éléments qui amènent l'entreprise 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 ;

6.4.4.9. Les mesures que l'entreprise 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 ;

6.4.4.10. Les mesures que l'entreprise 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 ;

6.4.4.11. 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.

6.4.5. Avise, avec diligence, les assureurs de l'entreprise, le cas échéant.

6.4.6. Inscris l'incident de confidentialité dans le registre prévu à cet effet.

6.4.7. Sur demande de la Commission d'accès à l'information, transmets une copie de ce registre.

7. REGISTRE DES INCIDENTS DE CONFIDENTIALITÉ

7.1. L’entreprise doit tenir un registre des incidents de confidentialité.

7.2. Les renseignements contenus au registre doivent être tenus à jour et conservés pendant une période minimale de cinq ans après la date à laquelle l’entreprise a pris connaissance de l’incident, et pendant toute durée de conservation du dossier requise par la loi.

8. ENTRÉE EN VIGUEUR

8.1. La présente procédure entre en vigueur le 22 septembre 2023.