Commission d'accès
à l'information
du Québec

Prévenir les incidents de confidentialité

Liste de contrôle pour les entreprises

Janvier 2026

Mieux vaut prévenir que guérir!

Vous devez limiter les risques d'incident de confidentialité au sein de votre entreprise :

- en respectant vos obligations et les principes de protection des renseignements personnels;
- en mettant en place des mesures de sécurité adéquates;
- en vous assurant de leur application en tout temps afin de garantir leur efficacité.

La Commission propose cette fiche pratique pour vous accompagner à chacune des étapes de la démarche proposée dans son document Prévenir les incidents de confidentialité – Guide explicatif pour les entreprises.

Cet outil représente un modèle à adapter en fonction du contexte de votre entreprise. Il a pour objectif de guider la réflexion en matière de prévention des incidents de confidentialité. **Cocher les cases dans ce document n'assure pas la conformité de vos actions.**

Étape 1
Connaître et respecter vos obligations

Respecter vos obligations aide à prévenir les incidents de confidentialité ou à en minimiser les impacts.

Vous trouvez ci-dessous une liste des plus importantes obligations en matière de protection des renseignements personnels. D'autres obligations existent cependant. Pour en savoir davantage, consultez la section Protection des renseignements personnels – Entreprises et organisations privées du site Web de la Commission.

En matière de collecte

Faites de bonnes affaires en ne collectant que les renseignements personnels nécessaires!

- ☐ Vous avez déterminé les fins de la collecte et avez jugé que vous aviez un intérêt sérieux et légitime pour collecter des renseignements personnels sur votre personnel ou votre clientèle.
- ☐ Vous collectez uniquement les renseignements personnels nécessaires (p. ex. pour embaucher du personnel et gérer les dossiers d'employés ou pour offrir votre bien ou votre service).

Rappelez-vous : les renseignements personnels que votre entreprise n'a pas collectés ne peuvent pas être impliqués dans un incident de confidentialité!

- ☐ Votre collecte se fait par des moyens licites (c'est-à-dire légaux et légitimes).
- ☐ Au moment de collecter des renseignements concernant votre personnel ou votre clientèle, vous les avez au moins informés :
  - ☐ des fins de la collecte;
  - ☐ des moyens utilisés pour effectuer la collecte;
  - ☐ de leurs droits d'accès et de rectification;

- [ ] de leur droit de retirer leur consentement à la communication ou à l'utilisation des renseignements collectés.

Rappelez-vous : une personne informée de ses droits en vaut deux! Elle sera beaucoup plus attentive à la protection de ses renseignements personnels et alerte en cas d'incident si elle sait, par exemple, quelles catégories de personnes ou tiers sont susceptibles de les utiliser ou de les détenir. Vous devez fournir ces informations sur demande, mais vous pourriez les intégrer à votre politique de confidentialité.

- [ ] Vous avez obtenu un consentement valide des personnes concernées avant de collecter leurs renseignements personnels auprès d'un tiers, à moins d'une exception prévue par la Loi sur la protection des renseignements personnels dans le secteur privé (Loi sur le privé).

- [ ] Vous avez prévu une révision périodique des différentes collectes de renseignements personnels concernant votre personnel et votre clientèle.

Pour aller plus loin, consultez :

- *La collecte de renseignements personnels*
- *Pièces d'identité*

En matière d'utilisation

C'est élémentaire : il ne faut utiliser que les renseignements personnels nécessaires!

- [ ] Vous donnez accès aux renseignements personnels uniquement aux membres du personnel lorsque ces renseignements sont nécessaires à l'exercice de leurs fonctions.

Rappelez-vous : des membres du personnel détenant des droits d'accès restreints ne peuvent pas compromettre l'ensemble des renseignements détenus par votre entreprise!

- [ ] Une fois les fins accomplies, vous limitez l'utilisation de renseignements personnels aux fins auxquelles consentent les personnes concernées ou permises par la loi.

En matière de communication

Ne communiquez que ce qui est autorisé, de manière sécurisée!

- [ ] Vous avez obtenu le consentement des personnes concernées pour communiquer leurs renseignements à un tiers (p. ex. un assureur ou un prestataire de services), à moins d'une exception prévue par la Loi sur le privé.

- [ ] Vous et votre personnel veillez à ce que les renseignements personnels que vous communiquez à l'extérieur du Québec, ou ceux que traitent pour vous une personne ou un organisme à l'extérieur du Québec, bénéficient d'un niveau de protection adéquat par rapport aux principes de protection

des renseignements personnels généralement reconnus. Vous démontrez cette protection par une évaluation des facteurs relatifs à la vie privée.

- ☐ Vous concluez également une entente avec la personne ou l'entreprise destinataire de ces renseignements.

☐ Vous concluez des ententes écrites pour encadrer la communication à un prestataire de renseignements personnels dans le cadre d'un mandat ou pour l'exécution d'un contrat de service ou d'entreprise.

En matière de conservation et de destruction

Ne conservez que des renseignements exacts et à jour, et pas pour toujours!

☐ Les renseignements personnels que vous détenez sur votre personnel et votre clientèle sont exacts et à jour au moment où vous les utilisez.

☐ Dès que la finalité pour laquelle les renseignements personnels ont été collectés ou utilisés est accomplie, vous en disposez :

- ☐ en les détruisant de manière sécuritaire, sous réserve du délai prévu par la loi (p. ex. pour des obligations fiscales);
- ☐ en les anonymisant pour les utiliser à des fins sérieuses et légitimes.

Rappelez-vous : des renseignements personnels que votre entreprise a détruits ne peuvent pas être compromis!

Pour aller plus loin, consultez :

- Conservation et destruction des renseignements personnels.

Étape 2
Faire l'inventaire des renseignements personnels détenus et en évaluer la sensibilité

Comprendre les renseignements que vous détenez vous permettra de mieux les protéger!

☐ Vous avez réalisé un inventaire des renseignements personnels que votre entreprise détient. Cet inventaire précise :

- ☐ les types de renseignements personnels que votre entreprise collecte sur sa clientèle ou son personnel (p. ex. : no de carte de crédit, adresse, no de téléphone);
- ☐ l'ampleur des renseignements;

- [ ] les fins (objectif recherché, résultat attendu) pour lesquelles il est nécessaire que votre entreprise collecte ces renseignements personnels;
- [ ] une évaluation du degré de sensibilité de ces renseignements;
- [ ] la façon dont votre entreprise collecte ces renseignements;
- [ ] les catégories de personnes autorisées à y avoir accès au sein de l'entreprise ou à l'extérieur (tiers);
- [ ] le contexte dans lequel ces renseignements sont utilisés ou communiqués au sein ou à l'extérieur de l'entreprise, ou la façon dont ils le sont;
- [ ] le lieu et la juridiction où sont conservés ces renseignements, les supports sur lesquels ils le sont et les conditions dans lesquelles ils sont conservés;
- [ ] la façon dont votre entreprise dispose de ces renseignements une fois la finalité justifiant leur collecte accomplie.

Pour bien structurer votre inventaire, consultez le guide Réaliser une évaluation des facteurs relatifs à la vie privée.

Étape 3
Identifier les risques et en évaluer les conséquences

Ne pas évaluer ses risques est un risque encore plus grand!

- [ ] Vous avez identifié les situations ou les événements (risques) pouvant raisonnablement survenir et menacer les renseignements personnels que votre entreprise détient (p. ex. : vol ou divulgation non autorisée).
- [ ] Vous avez analysé les causes susceptibles de générer ces risques (p. ex. : mécanismes de vérification insuffisants ou inexistants, manque de connaissances ou de formation, erreurs de manipulation des renseignements).
- [ ] Vous avez évalué l'impact potentiel de chacun des risques (p. ex. : très faible ou inexistant, faible, grand, très grand).
- [ ] Vous avez estimé les probabilités que ces risques se réalisent.
- [ ] Vous avez considéré les stratégies et les mesures de sécurité existantes.
- [ ] Vous avez déterminé le seuil de tolérance pour chaque risque.

Étape 4
Déterminer les mesures appropriées

Adopter des mesures de sécurité appropriées : un premier pas vers des renseignements bien protégés!

- ☐ Vous avez mis en œuvre votre obligation légale de nommer une personne responsable de la protection des renseignements personnels au sein de votre entreprise.
- ☐ Votre entreprise a adopté, tel que prescrit par la loi, des politiques et des pratiques encadrant sa gouvernance à l'égard des renseignements personnels qu'elle détient. Par exemple :
  - ☐ Votre entreprise offre régulièrement à son personnel des séances de formation et de sensibilisation sur la protection des renseignements personnels et sur les politiques et pratiques en vigueur.
  - ☐ Votre entreprise a adopté une politique, des directives ou des procédures sur l'utilisation d'appareils mobiles personnels au travail ou l'utilisation d'appareils mobiles professionnels à l'extérieur du lieu de travail.
  - ☐ Dans le cas de contrats conclus avec des tiers comme des prestataires ou des fournisseurs de service, votre entreprise a adopté des politiques, des procédures ou des directives établissant les exigences en matière de protection des renseignements personnels.
  - ☐ Vous avez vérifié les mesures de sécurité mises en place par les tiers avec qui vous partagez des renseignements.
- ☐ Votre entreprise a adopté des mesures de sécurité techniques visant la protection des renseignements personnels qu'elle détient. Par exemple :
  - ☐ Des procédures visant à guider le personnel relativement aux mesures à appliquer pour sécuriser ses réseaux (y compris sans fil), prévenir les attaques contre les logiciels malveillants, gérer les accès des utilisateurs, etc.
  - ☐ Des façons de faire qui favorisent la prévention des incidents de confidentialité : mots de passe forts, chiffrement des communications, coupe-feu, dépersonnalisation des données, mise à jour des logiciels, etc.
- ☐ Votre entreprise a adopté des mesures de sécurité physique à appliquer pour assurer la protection des renseignements personnels qu'elle détient (p. ex. : locaux et classeurs fermés à clef, accès limités, etc.).
- ☐ Votre entreprise a adopté d'autres politiques, procédures ou directives qui peuvent avoir un impact positif sur la prévention des incidents de confidentialité.

Étape 5
Déployer les mesures de sécurité

Prévoyez le déploiement de vos mesures et assurez-en une mise en œuvre complète et intégrée!

- ☐ Par ses actions, la haute direction démontre que la protection des renseignements personnels est une priorité organisationnelle et qu'elle respecte son obligation légale de veiller à leur protection. En cela, elle exerce un leadership fort et mobilisant :
  - ☐ en approuvant les mesures de sécurité mises en place et en assurant leur contrôle;
  - ☐ en faisant leur promotion active auprès du personnel;
  - ☐ en fournissant les ressources nécessaires pour assurer l'implantation et le maintien d'une culture forte de protection des renseignements personnels.
- ☐ Vous avez élaboré un plan d'action en concertation avec les personnes qui auront la responsabilité de le mettre en œuvre.
- ☐ Vous avez élaboré une stratégie de communication afin de faire connaître les mesures à votre personnel.
- ☐ Les mesures mises en place sont claires, complètes, concrètes et cohérentes.

Étape 6
Mesurer l'efficacité des mesures

Prenez la mesure de vos mesures!

- ☐ Vous avez mesuré la performance des stratégies et des moyens de sécurité que vous avez mis en place par le biais d'outils de mesure (p. ex. : exercice d'hameçonnage auprès du personnel avant et après une campagne de sensibilisation) ou d'autres sources de rétroaction (p. ex. : analyse des plaintes reçues au regard des pratiques en matière de protection des renseignements personnels).
- ☐ Vous avez réévalué le niveau de chacun des risques à la lumière des mesures déployées.

Étape 7
Surveiller l’application des mesures et les réviser

Protéger les renseignements personnels n’est pas l’affaire d’une seule journée!

- ☐ Vous avez mis en place des mécanismes pour surveiller de manière active l’efficacité des mesures de sécurité déployées.
- ☐ Vous réévaluez régulièrement l’efficacité de ces mesures et les mettez à jour.
- ☐ Votre entreprise a adopté une politique, des directives ou des procédures sur la gestion des incidents de confidentialité (p. ex. : procédures pour détecter, consigner ou rapporter les incidents et y répondre, y compris les mesures de mitigation des risques associés à de tels incidents, et stratégies de prévention pour éviter qu’ils se reproduisent). D’ailleurs, toute entreprise doit tenir un registre dans lequel elle collige tous les incidents de confidentialité impliquant des renseignements personnels.

Cet outil d’information vous a-t-il été utile? Complétez notre court sondage de satisfaction!

CAI Commission d'accès à l'information du Québec

cai.gouv.qc.ca