Commission d'accès
à l'information
du Québec

Prévenir les incidents de confidentialité

Guide explicatif pour les entreprises

Janvier 2026

Mieux vaut prévenir que guérir!

Votre entreprise a l'obligation de mettre en place des mesures de sécurité adéquates pour protéger les renseignements personnels[1].

Vous contribuez ainsi à favoriser le respect de la vie privée de votre clientèle et de votre personnel, et à diminuer les risques d'atteinte à votre réputation.

Ce guide vise à répondre aux questions suivantes :

- **Qu'est-ce qu'un incident de confidentialité?**
- **Comment distinguer la protection des renseignements personnels et la sécurité informatique?**
- **Comment protéger les renseignements personnels?**

En complément de ce guide explicatif, la Commission rend disponible le document Prévenir les incidents de confidentialité – Liste de contrôle pour les entreprises. Il s'agit d'un outil pratique permettant d'aider les entreprises à se poser les bonnes questions dans le cadre de leur démarche de prévention.

[1] Cette obligation est prévue à l'article 10 de la *Loi sur la protection des renseignements personnels dans le secteur privé*.

Table des matières

Qu’est-ce qu’un incident de confidentialité ?

Un incident de confidentialité se produit lorsqu’il y a consultation, utilisation ou communication de renseignements personnels non autorisée par la loi ou lorsque de tels renseignements sont perdus ou volés.

Un incident de ce type peut prendre plusieurs formes :

- Consultation, extraction ou communication non autorisée de renseignements personnels
- Envoi d’une communication à la mauvaise personne
- Divulgation de renseignements personnels par des commérages à l’intérieur ou à l’extérieur des lieux de travail (p. ex. dans l’autobus)
- Perte de données provoquée par un virus, une faille informatique ou une erreur humaine
- Atteinte à la sécurité par une cyberattaque (p. ex. hameçonnage, rançongiciel)
- Intrusion d’un tiers dans le système informatique

Quelles entreprises sont visées?

Toute entreprise est à risque de subir un incident de confidentialité. Que vous soyez détenteur des renseignements ou sous-traitant, vous devez adopter des mesures concrètes de protection des renseignements personnels et en évaluer régulièrement l’efficacité pour les tenir à jour. Autrement, les probabilités que votre entreprise soit touchée par un incident sont plus élevées.

Quelles sont les conséquences ?

Un incident de confidentialité met à risque la vie privée des personnes concernées. Il peut s'agir de votre clientèle, de votre personnel ou de vos partenaires d'affaires.

Les conséquences potentielles peuvent être importantes, et la vie d'une personne peut basculer à la suite d'un incident. Elle peut notamment être victime d'un vol d'identité ou d'une fraude, subir de la discrimination, ressentir une forte détresse psychologique, ou même voir sa sécurité physique menacée, dans certains cas.

Vous avez donc le devoir envers les personnes dont vous détenez les renseignements personnels de minimiser le risque qu'elles soient touchées par un incident de confidentialité, diminuant du même coup les risques pour votre organisation. En effet, un tel incident peut affecter la confiance du public envers votre entreprise en nuisant à sa réputation. Il peut également compromettre la rentabilité, car sa prise en charge engendre des frais qui peuvent être élevés et affecte ainsi négativement votre chiffre d'affaires.

Quelles sont les causes ?

Il existe différents types de menaces à la confidentialité des renseignements personnels. Elles peuvent être :

- **humaines :** hameçonnage, piratage informatique, indiscrétions, perte ou vol de renseignements personnels par un employé, communication accidentelle, etc.
- **technologiques :** absence d'un pare-feu, désuétude des logiciels, données non chiffrées, services non sécurisés ou conservés alors qu'ils ne sont plus utiles, etc.
- **physiques :** accessibilité de la salle des serveurs ou des locaux où sont rangés des documents contenant des renseignements personnels, par exemple.

Protection des renseignements personnels et sécurité informatique

La protection des renseignements personnels et la sécurité informatique sont complémentaires, mais ne sont pas synonymes. En effet, l'application de mesures de sécurité efficaces n'est qu'un des principes importants en matière de protection des renseignements personnels, qui dépend aussi de la saine gouvernance, de la transparence, de la limitation de la collecte, etc.

Bref, les mesures de sécurité informatique contribuent à la protection des renseignements personnels, mais ne préviennent pas automatiquement les intrusions dans la vie privée des personnes.

Voici des exemples où une bonne mesure de sécurité soulève malgré tout une problématique de non-conformité à la loi et aux principes de protection des renseignements personnels :

Collecte non conforme

Vous configurez un formulaire pour permettre une collecte sécuritaire des renseignements personnels, mais ils ne sont pas nécessaires au traitement du dossier du client ni pour lui offrir votre bien ou votre service.

Utilisation non conforme

Vous conservez des renseignements personnels dans un système ultrasécuritaire, mais vous les utilisez à d'autres fins que celles pour lesquelles ils ont été collectés ou auxquelles le client a consenti et qui ne sont pas autorisées par loi.

Communication non conforme

Vous sécurisez une correspondance électronique de façon à préserver le caractère confidentiel de son contenu, mais vous l'acheminez à une personne non autorisée à accéder aux renseignements personnels qui y figurent.

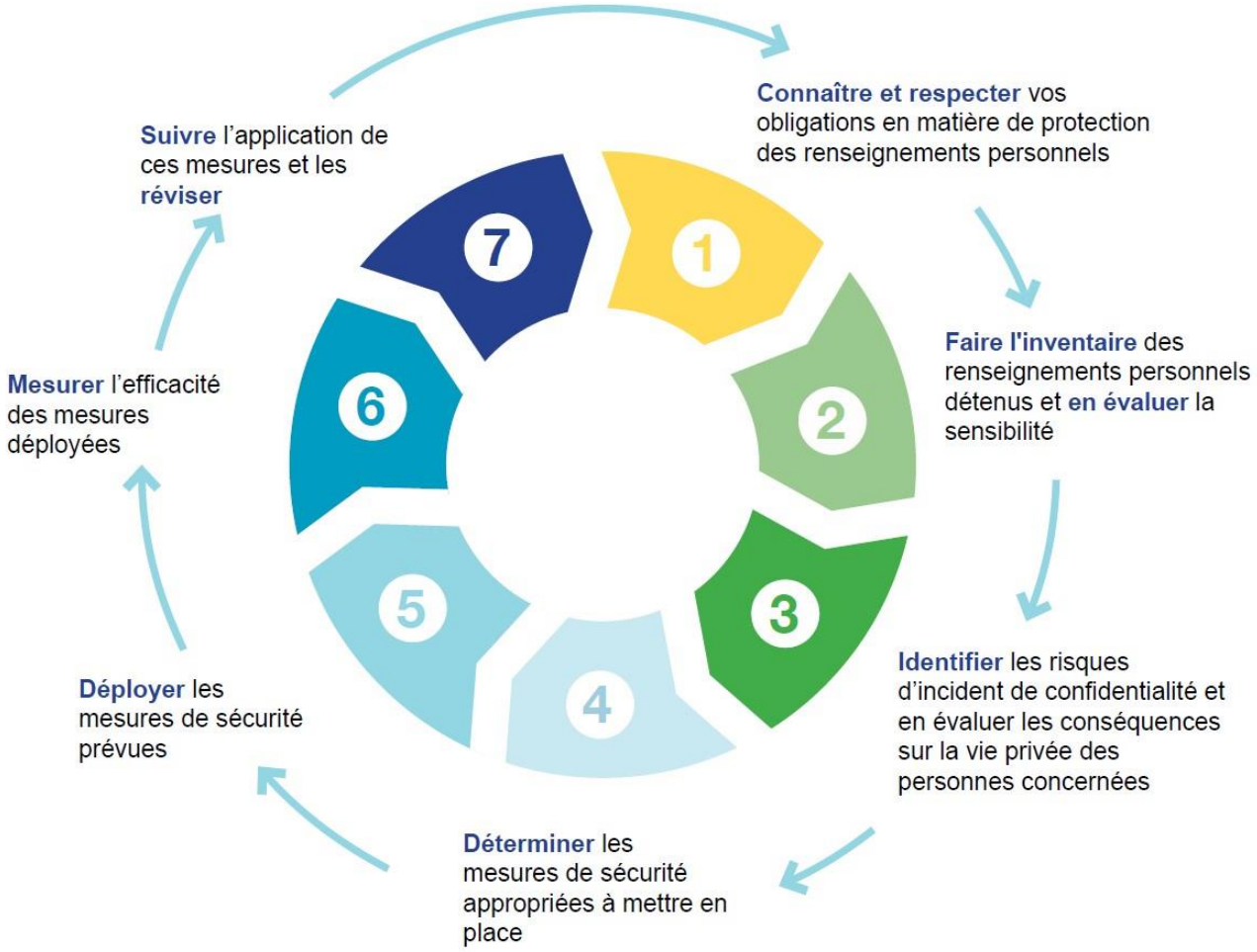
Conservation non conforme

Vous chiffrez les renseignements personnels que vous détenez et y restreignez l'accès, mais ils ne sont pas à jour ni exacts au moment où vous les utilisez pour prendre une décision relative à la personne concernée ou vous les conservez alors qu'ils auraient dû être détruits.

Comment protéger les renseignements personnels ?

En vertu de l'article 10 de la *Loi sur la protection des renseignements personnels dans le secteur privé*, « toute personne qui exploite une 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 ».

Pour vous aider dans la mise en œuvre de cette obligation, la Commission vous propose une démarche en **sept étapes** pour prévenir les incidents de confidentialité ou en limiter les conséquences.



Étape 1
Connaître et respecter vos obligations

Vous devez connaître et respecter vos obligations en matière de protection des renseignements personnels. Ainsi, votre entreprise sera moins susceptible d'être touchée par un incident de confidentialité.

Par exemple, si les membres du personnel ont des droits d'accès restreints, ils ne peuvent pas compromettre l'ensemble des renseignements détenus par votre entreprise. De même, des pirates ne peuvent pas voler les renseignements personnels que votre entreprise ne détient pas parce qu'ils n'ont pas été collectés ou qu'ils ont été détruits.

Pour en savoir davantage, consultez la section Protection des renseignements personnels – Entreprises et organisations privées du site Web de la Commission.

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

Il est primordial de faire l'inventaire des renseignements personnels détenus par votre entreprise[2]. Vous devez notamment documenter leur sensibilité, leur finalité (ce à quoi ils servent), leur quantité, leur répartition et leur support, de même que leur parcours au sein de votre entreprise, de leur collecte à leur destruction. Il vous faut également savoir qui y a accès et dans quel contexte ils sont utilisés.

Pour structurer votre inventaire, posez-vous les questions suivantes :

- Quels types de renseignements personnels votre entreprise collecte-t-elle sur sa clientèle ou son personnel?
- Quelle est l'ampleur des renseignements impliqués?
- Quelle est la nature de ces renseignements? Sont-ils sensibles en raison de cette nature (médicale, biométrique ou autrement intime) ou du contexte de leur utilisation?
- Pourquoi et comment ces renseignements sont-ils collectés, utilisés, communiqués ou conservés? Quelle en est la finalité?
- Quelles catégories de personnes sont susceptibles d'y accéder au sein ou en dehors de votre entreprise (tiers)?
- Combien de personnes auront accès aux renseignements et en quoi en ont-elles besoin dans l'exercice de leurs fonctions?
- Comment les personnes qui ont accès aux renseignements les utilisent-elles ou les communiquent-elles?
- Où sont conservés ces renseignements? Sur quels supports et dans quelles conditions le sont-ils?
- Comment détruisez-vous ces renseignements une fois la finalité justifiant leur collecte atteinte?

[22] Pour en savoir plus sur la démarche d'inventaire des renseignements personnels, consultez le guide Réaliser une évaluation des facteurs relatifs à la vie privée.

- Si les renseignements sont anonymisés à des fins sérieuses et légitimes, le sont-ils selon les meilleures pratiques généralement reconnues et de manière conforme au *Règlement sur l'anonymisation des renseignements personnels*?

Voici un modèle de tableau conçu pour vous aider à effectuer cet exercice :

Questions	Ce que vous devez faire
Quoi?	Inscrire le type de renseignement personnel collecté (p. ex. : adresse, date de naissance, etc.), sa quantité et la sensibilité du renseignement
Pourquoi?	Inscrire les raisons pour lesquelles il est nécessaire que votre entreprise collecte ce renseignement personnel
Qui?	Inscrire les catégories de personnes autorisées à avoir accès à ce renseignement au sein ou à l'extérieur de l'entreprise, et en quoi il est nécessaire à l'exercice de leurs fonctions
Comment?	Indiquer le contexte ou la façon dont ce renseignement est utilisé ou communiqué au sein ou à l'extérieur de l'entreprise
Où?	Indiquer où ce renseignement est conservé au sein ou à l'extérieur de l'entreprise et sur quels types de support
Quand?	Indiquer quand ce renseignement doit être détruit et la méthode de destruction sécuritaire utilisée

Un inventaire des renseignements personnels que votre entreprise détient vous permet de mieux prévoir les mesures permettant de les protéger. Ces mesures doivent être raisonnables compte tenu de la sensibilité de ces renseignements, de la finalité de leur utilisation, de leur quantité, de leur répartition et de leur support.

Cet exercice d'inventaire sera aussi pertinent pour évaluer la conformité de vos pratiques en matière de protection des renseignements personnels, notamment si vous lancez un projet qui nécessite une évaluation des facteurs relatifs à la vie privée.

Évaluer le contexte de traitement des renseignements

L'ampleur des mesures de sécurité doit être proportionnée au contexte : elle doit être adaptée à la sensibilité des renseignements personnels, à la finalité de leur utilisation, à leur quantité, à leur répartition et à leur support de conservation. À cette étape, vous devriez vous questionner sur chacun de ces facteurs afin de faciliter la détermination ultérieure des mesures à adopter (voir l'étape 4).

La sensibilité

Un renseignement personnel est sensible lorsqu'il suscite un haut degré d'attente raisonnable en matière de vie privée, en raison de sa nature ou du contexte de son utilisation ou de sa communication. L'article 12 de la *Loi sur la protection des renseignements personnels dans le secteur privé* précise par exemple que les renseignements de nature médicale ou biométrique sont sensibles par nature, mais tout type de renseignement peut être considéré comme tel dans un contexte donné.

Par exemple, des renseignements peuvent être considérés comme sensibles s'ils servent à un projet touchant une population vulnérable (p. ex. des personnes mineures, des minorités ethnoculturelles, des minorités sexuelles).

La finalité

Pour quelles fins les renseignements personnels sont-ils utilisés ou communiqués? Ces fins sont-elles généralement risquées pour les individus? Produisent-elles des effets importants (p. ex. juridiques) sur eux? Si, malgré la finalité de la collecte des renseignements personnels, les risques sont trop importants, l'entreprise doit réévaluer le critère de nécessité de la collecte, car sa proportionnalité pourrait être compromise.

La quantité

Combien de renseignements personnels sont impliqués? Leur quantité influence-t-elle l'ampleur des risques prévisibles?

Plus une entreprise détient de renseignements personnels sensibles (p. ex. : numéro d'assurance sociale, numéro de carte de crédit, renseignements médicaux) et leur contexte de gestion les expose à des risques (p. ex. : utilisation par plusieurs personnes, répartition sur différents supports, communication à des tiers), plus les mesures de sécurité doivent être robustes.

La répartition

Comment sont répartis les renseignements personnels impliqués? Les lieux physiques où ils sont conservés sont-ils sécuritaires et protégés adéquatement? À qui sont-ils communiqués? Combien de personnes ont accès aux renseignements et sur combien de supports sont-ils hébergés?

Les serveurs infonuagiques utilisés offrent-ils des garanties de sécurité correspondant aux standards de l'industrie? Les règles applicables dans le pays où sont situés les serveurs infonuagiques sont-elles suffisantes pour protéger les renseignements comme s'ils étaient hébergés au Québec?

Le support

Quels types de supports de conservation permettent de consulter, de consigner ou de consulter, momentanément ou à long terme, les renseignements personnels? S'agit-il d'un support matériel ou numérique, ou les deux? Ce support est-il sécurisé? Est-il connecté à d'autres systèmes?

Bref, les mesures de sécurité doivent être proportionnelles à la sensibilité des renseignements personnels de même qu'à leur finalité, à leur quantité, à leur répartition et à leur support. Pour en savoir plus sur l'évaluation de ces éléments au moment de faire l'inventaire des renseignements personnels détenus, consultez le guide Réaliser une évaluation des facteurs relatifs à la vie privée.

Étape 3
Identifier les risques et en évaluer les conséquences

Après avoir fait l'inventaire des renseignements personnels que votre entreprise détient et documenté leur contexte, vous devez identifier les risques (événements) susceptibles de les menacer.

Vous pourrez ensuite analyser les causes potentielles des risques identifiés, mesurer les conséquences d'un incident de confidentialité pour les personnes concernées et estimer la probabilité qu'ils surviennent.

Voici des exemples :

- **Risques :**
  - Vol de renseignements personnels;
  - Perte ou divulgation non autorisée;
  - Réidentification de renseignements personnels dépersonnalisés ou anonymisés;
  - Conservation de renseignements lorsque leur utilité n'est plus démontrée.
- **Causes potentielles :**
  - Manque de connaissances ou de formation du personnel;
  - Gestion inadéquate des accès aux renseignements personnels;
  - Absence de politique de conservation et de destruction des données (ou méconnaissance de cette politique).
- **Conséquences potentielles en cas d'incident :**
  - Sollicitation non désirée;
  - Vols d'identité et fraude;
  - Détresse psychologique, discrimination, harcèlement, manipulation.

Une conséquence peut être manifeste et externe (p. ex. en cas d'atteinte à la réputation), ou vécue de l'intérieur par les personnes concernées (p. ex. un sentiment d'intrusion).

Pour en savoir plus sur l'évaluation des risques et des conséquences, consultez le guide Réaliser une évaluation des facteurs relatifs à la vie privée.

Étape 4
Déterminer les mesures appropriées

À la lumière de l'analyse des risques et de l'évaluation de leurs conséquences, vous pouvez déterminer quelles mesures de sécurité vous devez mettre en place afin d'atténuer les risques. Si votre entreprise dispose déjà de mesures d'atténuation des risques, vous devez en évaluer l'efficacité afin de les ajuster au besoin.

Voici des exemples de mesures de sécurité pouvant contribuer à la protection des renseignements personnels en entreprise**. Les éléments en gras sont des obligations prévues dans la loi**.

Mesures administratives ou organisationnelles

Mesures de gouvernance

- **S'assurer que les politiques et pratiques en matière de protection des renseignements personnels sont à jour** (p. ex. : politique de conservation et de destruction des données, processus de gestion contractuelle soucieux de la protection des renseignements personnels);
- Former un comité de sécurité de l'information et de protection des renseignements personnels regroupant les personnes jouant un rôle stratégique au sein de votre entreprise et relevant de la haute direction;
- Signifier clairement vos attentes au personnel;
- Rendre périodiquement des comptes à la haute direction.

Mesures tactiques

- **Former et sensibiliser le personnel** (p. ex. : mots de passe forts, risques liés aux maliciels ou à l'ingénierie sociale ou principes du bureau propre);
- Concevoir un plan d'action annuel concernant l'ajout de mesures de sécurité;
- Exercer une surveillance active de l'efficacité des mesures déployées.

Mesures opérationnelles

- **Octroyer des droits d'accès aux renseignements personnels seulement au personnel dont les fonctions rendent cet accès nécessaire**;
- Selon la taille de votre entreprise, former des répondants qui offrent des conseils sur les mesures de sécurité déterminées à leurs collègues;
- Élaborer des modèles types (p. ex. : formulaire de collecte de renseignements personnels, engagement à la confidentialité, entente de non-divulgation, contrats) et les réviser périodiquement;
- Utiliser un protocole d'identification robuste.

Mesures physiques

- Contrôler les accès (p. ex. : bureaux, salles des serveurs, salles de câblage, système d'alarme);
- Restreindre l'accès aux locaux ou aux classeurs où sont conservés des documents papier contenant des renseignements personnels.

Mesures techniques

- Favoriser les identifiants et mots de passe forts;
- Assurer le chiffrement des communications et des informations stockées;
- Chiffrer les appareils mobiles;

- Mettre en place un coupe-feu;
- Assurer la défense du périmètre réseau;
- Dépersonnaliser les renseignements avant leur utilisation lorsque l'identité des personnes n'est pas nécessaire au traitement envisagé;
- Assurer la gestion efficace des accès aux renseignements personnels par les employés, journaliser ces accès et exploiter les journaux pour détecter les situations irrégulières;
- Appliquer systématiquement les mises à jour logicielles;
- Bloquer les ports USB;
- Adopter un système de gestion documentaire;
- Mettre en place des moyens permettant la destruction sécuritaire des renseignements personnels.

Étape 5
Déployer les mesures de sécurité

Après avoir déterminé les moyens à mettre en place pour réduire les risques identifiés, vous devez planifier leur mise en œuvre complète et intégrée. Pour vous aider, établissez un plan d'action et une stratégie de communication.

Les 10 C : une façon de ne rien oublier!

Concertation et communication : deux prérequis à une bonne gestion du changement

Vous prévoyez déployer ou bonifier des mesures de sécurité? La concertation avec les personnes qui auront la responsabilité de les mettre en œuvre permettra de vous assurer que les mesures proposées sont cohérentes pour elles.

Les membres du personnel pourraient vous fournir des informations sur leur contexte de travail pouvant vous amener à ajuster certaines stratégies ou mesures. Une bonne communication permettra également que ces personnes comprennent vos objectifs et y adhèrent, et appliquent les mesures conformément à vos attentes.

Complètes, claires, concrètes et cohérentes

Assurez-vous de mettre en œuvre des mesures complètes et intégrées, rédigées en termes clairs, qui sont concrètes et cohérentes afin qu'elles soient bien comprises et appliquées par l'ensemble du personnel.

Constance, contrôle et conséquences

Protéger les renseignements personnels n'est pas l'affaire d'une seule journée. L'efficience de vos mesures sera proportionnelle à leur constance et au contrôle que vous assurerez quant à leur application.

À titre d'exemple, vous pourriez mettre en place des mécanismes de contrôle des accès aux renseignements personnels et les journaliser, vous permettant ainsi de savoir qui a accédé à quel

renseignement. Vous devriez également informer le personnel concerné des mesures de surveillance et de contrôle dont il fait l'objet.

Enfin, le personnel devrait aussi être informé des conséquences (p. ex. : mesures disciplinaires) auxquelles il s'expose s'il fait preuve d'indiscrétion, ne respecte pas les politiques et directives ou transgresse les mesures de sécurité.

Étape 6
Mesurer l'efficacité des mesures

À cette étape, vous devriez mesurer la performance des stratégies et des moyens mis en place. Par exemple, si vous avez mené une campagne de sensibilisation sur les risques de l'hameçonnage auprès du personnel, mesurez son effet afin de déterminer si des améliorations sont requises.

Divers outils peuvent vous aider à évaluer l'efficacité de vos mesures :

- Sondages de satisfaction;
- Analyse des journaux;
- Rapports comportementaux;
- Tests d'intrusion et de vulnérabilité.

L'évaluation et la rétroaction vous fourniront des informations additionnelles qui vous aideront à évaluer le niveau de risque à la suite de l'application des mesures. Vous pourrez alors juger si ce nouveau seuil est acceptable et bonifier les mesures déployées

Étape 7
Surveiller l'application des mesures et les réviser

Pour assurer l'efficacité de vos mesures de sécurité, vous devez en surveiller l'application et les réviser en fonction des risques émergents. Vos mesures doivent également s'adapter aux changements de votre entreprise : nouvelle ligne d'affaires, nouveau système transactionnel, nouvel outil de partage des informations, etc.

Des outils de contrôle des mesures, comme un tableau de bord de sécurité, vous permettront de jeter un regard d'ensemble sur l'application cohérente et intégrée des stratégies et des mesures mises en place.

Voici un exemple de questions que vous pourriez vous poser :

- Vos processus d'attribution et de gestion des accès informatiques sont-ils revus fréquemment? Par exemple, les cartes d'accès et les codes d'accès des personnes qui quittent le bâtiment sont-ils désactivés en temps utile?
- Auditez-vous régulièrement les pratiques de votre personnel en matière de protection des renseignements personnels (p. ex. par le biais de simulations de maliciels ou grâce à des clients mystère)?

Mieux vaut prévenir que guérir!

Sauriez-vous comment réagir si un incident de confidentialité survenait au sein de votre entreprise? Un plan d'intervention vous permettra d'agir plus rapidement et efficacement et contribuera à réduire les conséquences de l'incident, à faciliter le nettoyage adéquat des systèmes touchés et à relancer vos activités en peu de temps.

Que faire en cas d'incident de confidentialité?

Il est fort probable (voire certain) que votre entreprise sera touchée, un jour ou l'autre, par un incident de confidentialité, qu'il soit mineur ou de grande ampleur. Vous devrez alors réagir rapidement pour limiter les risques, évaluer les préjudices possibles et, dans certains cas, aviser la Commission et les personnes concernées.

Si vous avez des motifs de croire qu'un incident de confidentialité s'est produit au sein de votre entreprise, vous devez prendre des mesures raisonnables pour diminuer les risques qu'un préjudice soit causé et éviter que de nouveaux incidents de même nature ne se produisent.

De plus, pour tout incident de confidentialité, vous devez évaluer la gravité du risque de préjudice pour les personnes concernées. Si l'analyse fait ressortir un risque de préjudice sérieux, vous devez aviser la Commission et les personnes concernées.

Vous devez également tenir un registre et y colliger tous les incidents de confidentialité, que le risque de préjudice soit sérieux ou non.

Pour en savoir plus, consultez la page Incidents de confidentialité et mesures de sécurité.

Rappels

Pour qu'elles soient efficaces, vos mesures de sécurité doivent tenir compte de plusieurs éléments, comme la sensibilité des renseignements, la finalité de leur utilisation, leur quantité, leur utilisation, leur répartition et leur support.

Ces mesures doivent être mises en œuvre, diffusées à l'ensemble du personnel, documentées, surveillées et révisées régulièrement.

Des mesures de sécurité visant la protection des renseignements personnels ont-elles été mises en place au sein de votre entreprise? Êtes-vous certain de l'efficacité de ces mesures?

Pour vous aider à appliquer la démarche de gestion de risques proposée dans ce guide, consultez l'outil pratique Prévenir les incidents de confidentialité – Liste de contrôle pour les entreprises.

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