



Guidelines

Lignes directrices

Principales étapes à suivre par les organisations en cas d'atteintes à la vie privée

But

Le présent document a pour but de fournir des directives aux organisations du secteur privé, petites et grandes, en cas d'atteinte à la vie privée. Les organisations devraient prendre des mesures préventives en se dotant de politiques et de garanties procédurales raisonnables, et en offrant la formation nécessaire. Les présentes lignes directrices visent à aider les organisations à prendre les mesures appropriées en cas d'atteinte à la vie privée et à offrir des directives sur la façon d'évaluer s'il convient de notifier les personnes concernées. Certaines étapes pourraient être omises ou combinées.

Qu'est-ce qu'une atteinte à la vie privée?

Une atteinte à la vie privée suppose l'accès non autorisé à des renseignements personnels ou la collecte, l'utilisation ou la communication non autorisée de tels renseignements. Ces activités sont « non autorisées » lorsqu'elles contreviennent aux lois applicables en matière de protection des renseignements personnels, telles que la LPRPDÉ, ou aux lois provinciales similaires en matière de protection des renseignements personnels. Certains des cas les plus courants d'atteinte à la vie privée surviennent lorsque des renseignements personnels de clients, de patients ou d'employés, sont volés, perdus ou communiqués par erreur (p. ex., lorsqu'un ordinateur renfermant des renseignements personnels est volé ou que des renseignements personnels sont accidentellement transmis par courriel aux mauvaises personnes). Une atteinte à la vie privée peut également découler d'une erreur de procédure ou d'une défaillance opérationnelle.

Quatre principales étapes à suivre en cas d'atteinte à la vie privée

Il y a quatre principales étapes à considérer en cas de brèche, présumée ou non, dans la protection des données : 1) limitation de la brèche dans la protection des données et évaluation préliminaire; 2) évaluation des risques associés à la brèche dans la protection des données; 3) notification; 4) prévention. Assurez-vous de prendre chaque cas au sérieux et d'amorcer immédiatement une enquête sur l'incident en question. Vous devez suivre les étapes 1, 2 et 3 simultanément ou rapidement l'une après l'autre. La 4^e étape comprend des

recommandations relatives aux solutions à long terme et aux stratégies de prévention. La décision sur la façon de réagir devrait être prise au cas par cas.

Comme supplément aux présentes lignes directrices, il existe une [liste de contrôle](#) que les organisations peuvent consulter pour s'assurer qu'elles ont pris en compte tous les éléments appropriés en cas d'atteinte à la vie privée.

Étape 1 : Limitation dans l'atteinte à la vie privée et évaluation préliminaire

Vous devez prendre sans tarder des mesures sensées pour limiter la brèche dans les renseignements personnels, telles que suit :

- Limiter immédiatement la brèche dans les renseignements personnels (p. ex., mettre fin à la pratique non autorisée, récupérer les dossiers, éteindre le système qui fait l'objet de la brèche, révoquer ou changer les codes d'accès informatiques ou corriger les lacunes des systèmes de sécurité matériels ou électroniques).
- Désigner une personne qualifiée pour la tenue de l'enquête initiale. Cette personne devrait avoir la latitude voulue au sein de l'organisation pour mener l'enquête initiale et formuler des recommandations. Une enquête plus minutieuse pourrait être réalisée subséquentement, au besoin.
- Déterminer s'il est nécessaire de mettre sur pied une équipe composée de représentants des secteurs concernés de l'entreprise.
- Déterminer qui doit être mis au courant de l'incident à l'interne et, éventuellement, à l'externe, à cette étape préliminaire. Remonter l'échelle à l'interne, au besoin, et aviser la personne responsable de la conformité aux mesures de protection des renseignements personnels au sein de votre organisation.
- Si la brèche dans les renseignements personnels procède d'un vol ou de toute autre activité criminelle, la police doit en être avisée.
- Ne pas nuire à la capacité d'enquêter sur l'incident. Prendre garde de ne pas détruire des éléments de preuve qui pourraient servir à déterminer la cause de l'incident ou vous permettre de prendre les mesures correctives qui s'imposent.

Étape 2 : Évaluation des risques associés à l'atteinte à la vie privée

Pour déterminer toute autre mesure devant être prise immédiatement, vous devez évaluer les risques associés à la brèche dans les renseignements personnels en tenant compte des facteurs suivants :

(i) Les renseignements personnels en cause

- Quels éléments de données sont en cause?
- Dans quelle mesure les renseignements sont-ils sensibles? En général, plus les renseignements sont sensibles, plus les risques de préjudice sont élevés pour les personnes. Certains renseignements personnels sont plus sensibles que d'autres (p. ex., les renseignements sur la santé, les pièces d'identité émises par le gouvernement, comme les numéros d'assurance sociale, de permis de conduire et de carte d'assurance-maladie, ainsi

que les numéros de comptes financiers, comme les numéros de cartes de crédit ou de débit, lesquels peuvent servir au vol d'identité). Une combinaison de renseignements personnels est généralement plus sensible qu'un renseignement personnel pris isolément. Toutefois, la nature sensible des renseignements n'est pas le seul critère à prendre en considération lorsqu'on évalue les risques; il faut également tenir compte des préjudices prévisibles pour les personnes concernées.

- Quel est le contexte lié aux renseignements personnels en cause? Par exemple, il se peut que la liste d'un livreur de journaux comportant des noms d'abonnés ne soit pas de nature sensible. Toutefois, l'information concernant des abonnés qui ont demandé une interruption de service pendant leurs vacances pourrait s'avérer sensible. De la même façon, les renseignements accessibles au public, tels que ceux contenus dans un annuaire téléphonique public, pourraient être moins sensibles.
- Les renseignements personnels sont-ils convenablement encodés, dépersonnalisés ou difficiles d'accès?
- Comment les renseignements personnels peuvent-ils être utilisés? L'information peut-elle servir à des fins frauduleuses ou autrement préjudiciables? Certains types de renseignements confidentiels sont plus vulnérables lorsqu'ils sont utilisés en combinaison avec le nom, l'adresse et la date de naissance d'une personne compte tenu des risques plus élevés de vol d'identité.

Une évaluation du type de renseignements personnels en cause vous aidera à déterminer les mesures à prendre, les personnes à aviser, y compris le(s) commissaire(s) à la protection de la vie privée approprié(s) et la manière dont les personnes concernées, le cas échéant, devraient être notifiées. Il n'est peut-être pas nécessaire de notifier les personnes concernées lorsque, par exemple, un ordinateur portatif renfermant des renseignements convenablement encodés a été volé puis retrouvé et que l'enquête a révélé que l'on n'a pas touché aux renseignements.

(ii) Cause et étendue de la brèche dans les renseignements personnels

- Dans la mesure du possible, déterminer la cause de la brèche dans les renseignements personnels.
- Y a-t-il un risque que des brèches se reproduisent ou que les renseignements soient davantage compromis?
- Quelle a été l'étendue de l'accès non autorisé aux renseignements personnels ou de la collecte, de l'utilisation ou de la communication non autorisée de tels renseignements, y compris le nombre et la nature des destinataires probables et la mesure dans laquelle l'accès non autorisé à ces renseignements personnels, leur utilisation ou leur communication risquent de se poursuivre, y compris par l'entremise de médias de masse ou en ligne?
- L'information a-t-elle été perdue ou volée? Si elle a été volée, peut-on déterminer si l'information était la cible du vol?
- Les renseignements personnels ont-ils été retrouvés?
- Quelles mesures ont déjà été prises pour atténuer les préjudices?
- S'agit-il d'un problème systémique ou d'un incident isolé?

(iii) Personnes concernées par la brèche dans les renseignements personnels

- Quelle est la quantité de renseignements personnels compromis par la brèche?

- Quelles personnes sont concernées par la brèche (employés, entrepreneurs, membres du public, clients, fournisseurs de services, autres organisations)?

(iv) Préjudices prévisibles découlant de la brèche dans les renseignements personnels

- Lorsque vous évaluez les risques de préjudice découlant de la brèche dans les renseignements personnels, avez-vous pris en considération les attentes raisonnables des personnes concernées. Par exemple, beaucoup de personnes estimerait que la perte d'une liste d'abonnés à une publication spécialisée traitant de questions délicates pourrait présenter davantage de risques que la perte d'une liste d'abonnés à un journal national.
- Qui est le destinataire de l'information? Y a-t-il un lien entre les destinataires non autorisés et les personnes visées par les renseignements? Par exemple, les renseignements ont-ils été communiqués à une personne inconnue ou soupçonnée d'être mêlée à des activités criminelles, ce qui laisserait présager une utilisation inappropriée des renseignements personnels? Ou le destinataire est-il une personne connue, digne de confiance et susceptible, selon toute vraisemblance, de rendre les renseignements sans les communiquer ou les utiliser?
- Quel préjudice la brèche dans les renseignements personnels pourrait-elle causer aux personnes concernées? Exemples :
 - risques pour la sécurité (p. ex., la sécurité physique);
 - vol d'identité;
 - pertes financières;
 - pertes commerciales ou perte de possibilités d'emploi;
 - humiliation, atteinte à la réputation ou détérioration des relations.
- Quel préjudice la brèche dans les renseignements personnels pourrait-elle causer à l'organisation concernée? Exemples :
 - perte de confiance en l'organisation;
 - perte de biens;
 - risques financiers;
 - actions en justice (c.-à-d., poursuites en recours collectif).
- Quel préjudice la notification de la brèche dans les renseignements personnels pourrait-elle causer au public? Exemples :
 - risques pour la santé publique;
 - risques pour la sécurité publique.

Étape 3 : Notification

La notification peut s'inscrire dans une stratégie d'atténuation des risques comportant potentiellement des avantages pour l'organisation autant que pour les personnes concernées par la brèche dans les données personnelles. Si l'atteinte à la vie privée pose un risque de préjudice pour les personnes concernées, celles-ci devraient en être notifiées. Notifier rapidement les personnes concernées leur permet de prendre des mesures pour se protéger. La difficulté consiste à déterminer les situations dans lesquelles l'incident doit être signalé. Chaque incident doit être examiné au cas par cas afin de déterminer si l'atteinte à la vie privée doit faire l'objet d'une notification. Par ailleurs, les organisations sont priées d'informer le(s) commissaire(s) à la protection de la vie privée approprié(s) des cas concrets d'atteinte à la vie privée.

Pour décider s'il convient de notifier les personnes concernées, il faut se demander si la notification est nécessaire pour éviter ou atténuer les préjudices découlant d'un accès non autorisé à des renseignements personnels ou d'une collecte, d'une utilisation ou d'une communication induite de tels renseignements. Les organisations devraient également tenir compte de la capacité des personnes à prendre des mesures précises pour réduire tout préjudice éventuel.

(i) Notifier les personnes concernées

Les organisations devraient tenir compte des facteurs suivants pour décider s'il convient de notifier les personnes concernées :

- Quelles sont les obligations légales et contractuelles?
- Quels sont les risques de préjudices pour les personnes concernées?
- Y a-t-il un risque raisonnable de vol d'identité ou de fraude (compte tenu, généralement, du type des renseignements perdus, tels que le nom et l'adresse d'une personne combinés à des numéros de pièces d'identité émises par le gouvernement ou la date de naissance)?
- La personne concernée risque-t-elle de subir un dommage physique (c.-à-d., la personne concernée risque-t-elle, entre autres, d'être suivie ou d'être victime de harcèlement à la suite de la perte des renseignements personnels)?
- La personne risque-t-elle de subir des humiliations ou des atteintes à sa réputation (p. ex., lorsque les renseignements perdus proviennent de dossiers médicaux et disciplinaires ou de dossiers sur la santé mentale)?
- Dans quelle mesure la personne concernée est-elle capable d'éviter ou d'atténuer les préjudices éventuels?

(ii) Quand / comment notifier et qui devrait le faire

À cette étape, vous devriez avoir dressé une liste la plus exhaustive possible des faits et avoir procédé à l'évaluation des risques pour déterminer s'il y a lieu de notifier les personnes concernées.

Quand notifier : Les personnes concernées par l'incident devraient être notifiées le plus tôt possible après l'évaluation de l'incident. Cependant, si des responsables de l'application de la loi sont saisis de l'affaire, il conviendrait de leur demander si la notification devrait être différée pour ne pas compromettre la tenue de l'enquête.

Comment notifier : Il est préférable de notifier directement les personnes concernées (par téléphone, courrier, courriel ou en personne). On ne devrait généralement recourir à la notification indirecte (au moyen de sites Web, d'avis publics, de médias) que si la notification directe est susceptible de causer davantage de préjudices, que les coûts afférents sont excessifs ou que les coordonnées actuelles des personnes concernées sont inconnues. Il pourrait être approprié, dans certains cas, d'utiliser plusieurs méthodes de notification. Demandez-vous également si la méthode choisie pour notifier pourrait accroître le risque de préjudice (p. ex., en renseignant le voleur d'un ordinateur portable sur la valeur de l'information contenue dans l'ordinateur).

Qui devrait procéder à la notification : Généralement, c'est à l'organisation qui entretient un rapport direct avec le client ou l'employé qu'il incombe de notifier les personnes concernées, y

compris lorsque la brèche s'est produite chez un tiers fournisseur de services embauché à contrat pour tenir à jour ou traiter les renseignements personnels. Cependant, la notification par une tierce partie pourrait convenir davantage dans certaines circonstances. Par exemple, advenant une brèche dans les renseignements personnels concernant des cartes de crédit chez un marchand détaillant, la compagnie émettrice de cartes de crédit pourrait notifier elle-même les personnes concernées puisque le marchand pourrait ne pas avoir les coordonnées de ces personnes.

(iii) Quel devrait être le libellé de la notification

Le libellé de la notification variera selon la nature de l'incident et la méthode choisie pour notifier. La notification devraient faire part des renseignements suivants, s'il y a lieu :

- Un aperçu de l'incident et le moment où il s'est produit;
- Une description des renseignements personnels en cause;
- Une description sommaire des mesures que l'organisation a prises pour contrôler ou réduire les préjudices;
- Ce que l'organisation compte faire pour aider les personnes et les mesures que ces dernières peuvent prendre pour éviter ou réduire les risques de préjudice ou pour se protéger davantage. Les actions possibles incluent des arrangements pour la surveillance du crédit et d'autres outils de prévention des fraudes, de l'information sur la façon de changer de numéro d'assurance sociale (NAS), d'assurance maladie ou de permis de conduire. Par exemple, pour obtenir un nouveau numéro d'assurance sociale, veuillez consulter le site suivant :
http://www1.servicecanada.gc.ca/fr/sm/nas/0200/0200_010.shtml.
- Les sources de renseignements visant à aider les personnes à se protéger contre le vol d'identité (p. ex., les conseils offerts sur le site Web du Commissariat à la protection de la vie privée à http://www.priv.gc.ca/resource/ii_4_01_f.cfm et sur le site Web d'Industrie Canada à http://strategis.ic.gc.ca/epic/site/oca-bc.nsf/fr/h_ca02226f.html.
- Les coordonnées d'un service ou d'un employé de votre organisation qui peut répondre aux questions ou fournir de plus amples renseignements.
- Le cas échéant, indiquez si l'organisation a communiqué avec un commissaire à la protection de la vie privée pour le mettre au courant de l'affaire.
- Des coordonnées additionnelles pour permettre à la personne de faire part de ses inquiétudes à l'organisation.
- Les coordonnées du/des commissaire(s) à la protection de la vie privée approprié(s).

Prenez garde de ne pas inclure de renseignements personnels superflus afin d'éviter toute autre communication non autorisée de renseignements personnels.

(iv) Autres personnes à notifier

- **Commissaires à la protection de la vie privée** : Les organisations sont priées de signaler les cas concrets d'atteinte à la vie privée au bureau du commissaire à la protection de la vie privée approprié afin qu'il puisse répondre aux demandes de renseignements du public et à toute plainte éventuelle. Le/la commissaire pourrait également fournir aux organisations des conseils utiles pour faire face à ces situations. Par ailleurs, cette mesure pourrait contribuer à accroître la compréhension du public à l'égard des cas d'atteinte à la vie privée et à renforcer leur confiance en votre organisation. Les facteurs suivants devraient

être pris en compte pour décider s'il convient de signaler une brèche dans les renseignements personnels à d'autres commissaires :

- toute loi applicable pouvant exiger de notifier;
- les renseignements personnels en cause sont-ils visés par une loi en matière de protection des renseignements personnels;
- le type de renseignements personnels en cause, y compris ce qui suit :
 - les renseignements communiqués peuvent-ils être utilisés pour commettre un vol d'identité;
 - y a-t-il un risque raisonnable de préjudice découlant de la brèche dans la protection des données, y compris des pertes non financières;
- le nombre de personnes concernées par la brèche;
- les personnes concernées ont-elles été notifiées;
- peut-on s'attendre raisonnablement à ce que le bureau du commissaire à la protection de la vie privée reçoive des plaintes ou des demandes de renseignements concernant la brèche.

Que vous décidiez ou non qu'il est dans votre devoir de notifier les personnes concernées, il conviendrait de vous demander si les autorités ou les organisations suivantes devraient également être informées de la brèche, pourvu que de telles notifications soient conformes à la LPRPDÉ ou aux lois provinciales similaires en matière de protection des renseignements personnels :

- **Les policiers** : en cas de vols ou d'activités criminelles présumés.
- **Les compagnies d'assurances ou autres** : s'il est exigé de les notifier en vertu des obligations contractuelles.
- **Les ordres professionnels ou d'autres organismes de réglementation** : si les normes professionnelles ou d'application de la réglementation l'exigent.
- **Les compagnies émettrices de cartes de crédit, les établissements financiers ou les agences d'évaluation du crédit** : si leur aide est requise pour communiquer avec les personnes concernées ou pour atténuer les préjudices.
- **Autres parties internes ou externes qui n'ont pas déjà été notifiées** :
 - les entrepreneurs de tierce partie ou les autres parties qui pourraient être concernés;
 - les unités opérationnelles internes qui n'ont pas été préalablement avisées de l'incident, p. ex. les Relations gouvernementales, les Communications, les Relations avec les médias et les cadres supérieurs;
 - les syndicats ou d'autres unités de négociation.

Les organisations devraient évaluer les répercussions éventuelles que l'incident et la décision de notifier pourraient avoir sur des tierces parties, et prendre des mesures en conséquence. Par exemple, des tierces parties pourraient être touchées si des personnes annulent leur carte de crédit ou si des institutions financières émettent de nouvelles cartes.

Étape 4 : Prévention de futures atteintes à la vie privée

Une fois que les mesures immédiates sont prises pour réduire les risques associés à la brèche dans les renseignements personnels, les organisations doivent prendre le temps d'enquêter

sur les causes de l'incident et de réfléchir à la nécessité d'élaborer un plan de prévention. Plus ou moins d'efforts devraient être déployés en fonction de la gravité de l'incident et de son caractère systémique ou isolé. Le plan pourrait prévoir ce qui suit :

- une vérification de la sécurité physique et technique;
- un examen des politiques et des procédures et tout changement témoignant des leçons tirées de l'enquête et subséquemment (p. ex., les politiques sur la sécurité, les politiques sur la conservation des dossiers et la collecte de renseignements, etc.)
- un examen des pratiques de formation des employés;
- un examen des partenaires de la prestation de services (p. ex., négociants, détaillants, etc.)

Le plan pourrait prévoir une vérification à la fin du processus pour déterminer si votre plan de prévention a été mis en œuvre avec succès.