Commissariat
à la protection de
la vie privée du Canada

Office of the
Privacy Commissioner
Of Canada

LISTE DE CONTRÔLE CONCERNANT LES ATTEINTES À LA VIE PRIVÉE

Pour obtenir de plus amples renseignements, veuillez consulter le document
Principales étapes à suivre par les organismes en cas d'atteintes à la vie privée.

DESCRIPTION DE L'INCIDENT

- À quelle date a eu lieu l'incident?
- À quel moment l'incident a-t-il été découvert?
- Comment l'incident a-t-il été découvert?
- À quel endroit a eu lieu l'incident?
- Qu'est-ce qui a causé l'incident?

ÉTAPE 1 : LIMITATION DE L'ATTEINTE À LA VIE PRIVÉE ET ÉVALUATION PRÉLIMINAIRE

- Avez-vous limité la brèche dans les renseignements personnels (récupération de l'information, fermeture des ordinateurs, changement de serrures)?
- Avez-vous désigné une personne responsable pour diriger l'enquête initiale?
- Est-ce qu'il existe un besoin de mettre sur pied un groupe d'intervention pour l'incident? Le cas échéant, qui devrait être inclus? (p. ex. un agent de la protection de la vie privée, un agent de la sécurité, un agent des communications, un agent de la gestion du risque, un juriste)?
- À ce stade préliminaire, avez-vous décidé qui devrait être informé à l'interne et possiblement à l'externe?
- Est-ce que la brèche dans les renseignements personnels semble être causée par un vol ou toute autre activité criminelle? Si oui, est-ce que la police en a été informée?
- Vous êtes-vous assuré que les éléments de preuve, qui pourraient servir lors de l'enquête sur la brèche dans les renseignements personnels, n'ont pas été détruits?

ÉTAPE 2 : ÉVALUATION DES RISQUES ASSOCIÉS À L'ATTEINTE À LA VIE PRIVÉE

(i) Quels sont les renseignements personnels mis en cause?

- Quels sont les renseignements personnels mis en cause (nom, adresse, NAS, données financières, renseignements médicaux)?
- Quel en est le format (p. ex. support papier, base de données électronique)?
- Quelles mesures de sécurité matérielles ou techniques étaient en place au moment de l'incident (serrures, systèmes d'alarme, chiffrement, mots de passe, etc.)?

(ii) Quelles sont la cause et l'étendue de la brèche dans les renseignements personnels?

- Y a-t-il un risque que la brèche se répète ou que les renseignements soient davantage exposés?
- Est-ce que les renseignements personnels peuvent être utilisés de façon frauduleuse ou pour tout autre usage?
- 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?
- S'agit-il d'un problème systémique ou d'un incident isolé?

(iii) Combien de personnes sont concernées par cette brèche dans les renseignements personnels et qui sont ces personnes? (p. ex., des employés, entrepreneurs, membres du grand public, clients, fournisseurs de services, membres d'autres organismes)?

(iv) Existe-t-il des préjudices prévisibles liés à la brèche dans les renseignements personnels ?

- Quels préjudices aux personnes peuvent découler de la brèche dans les renseignements personnels? (p. ex. danger pour la sécurité, vol d'identité, perte financière ou de possibilité d'emploi, dommages physiques, humiliation, atteinte à la réputation, etc.)?
- Savez-vous qui a reçu les renseignements et quels sont les risques qu'on y accède, qu'on les utilise ou qu'on les communique de nouveau?
- Quel préjudice la brèche dans les renseignements personnels pourrait-elle causer à l'organisation concernée (p. ex., perte de confiance, perte d'actifs, enjeux financiers, poursuites, etc.)?
- Quel préjudice la notification de la brèche dans les renseignements personnels pourrait-elle causer au public (p. ex., risque pour la santé publique ou risque pour la sécurité publique)?

ÉTAPE 3 : NOTIFICATION

(i) Devrait-on notifier les personnes concernées?

- Quelles sont les attentes raisonnables des personnes concernées?
- Quels sont les risques de préjudice pour la personne concernée? Est-ce qu'il y a un risque raisonnable de vol d'identité ou de fraude?
- La personne concernée risque-t-elle de subir un dommage physique? Est-ce qu'il y a un risque d'humiliation ou d'atteinte à la réputation de la personne?
- Dans quelle mesure la personne concernée est-elle capable d'éviter ou d'atténuer les préjudices éventuels?
- Quelles sont les obligations juridiques et contractuelles de l'organisation?

Si vous décidez de ne pas notifier les personnes concernées, veuillez noter par écrit les raisons.

(ii) Si les personnes concernées doivent être notifiées, il faut déterminer qui le fera, comment et quand.

- De quelle façon ces personnes seront-elles notifiées (p. ex., par téléphone, courrier, courriel ou en personne, site Web, médias, etc.)?
- Qui va notifier les personnes concernées? Est-ce nécessaire d'inclure une tierce partie?
- Si les autorités policières sont impliquées, est-ce que la notification devrait être reportée à une date ultérieure afin d'être certain de ne pas nuire à l'enquête?

(iii) Que devrait comprendre la notification?

Suivant les circonstances, les notifications pourraient inclure certains des éléments suivants (veuillez toutefois limiter au strict minimum la quantité de renseignements personnels communiqués dans la notification) :

- un aperçu de l'incident et du moment où il s'est produit;
- une description des renseignements personnels en cause;

- une description sommaire des mesures que votre organisation a prises afin de contrôler ou de réduire les dommages;
- ce que fera votre organisation afin de venir en aide aux personnes concernées et les étapes que ces personnes peuvent suivre afin de réduire les risques de préjudice ou de mieux se protéger;
- les sources d'information conçues pour venir en aide aux personnes pour qu'elles se protègent contre le vol d'identité;
- les coordonnées d'un service ou d'une personne au sein de votre organisation qui peut répondre aux questions ou fournir de plus amples renseignements;
- indiquer si votre organisation a avisé ou non le bureau d'un commissaire à la protection de la vie privée;
- les coordonnées supplémentaires afin de faire part à votre organisation de toute préoccupation en matière de protection de la vie privée;
- les coordonnées du ou des commissaires à la protection de la vie privée compétents.

(iv) Est-ce que d'autres personnes devraient être informées de la brèche dans les renseignements personnels ?

- Devrait-on informer un commissaire à la protection de la vie privée? [http://www.privcom.gc.ca/fs-fi/02_05_d_15_f.asp]
- Devrait-on informer la police ou tout autre intervenant? Il pourrait s'agir d'assureurs; d'ordres professionnels ou d'autres organismes de réglementation; des compagnies émettrices de cartes de crédit, des institutions financières ou des agences d'évaluation de crédit, ou tout autre intervenant interne ou externe comme les entrepreneurs de tierce partie, les unités opérationnelles internes qui n'ont pas été préalablement informées de l'incident, les syndicats ou autres unités de négociation)

ÉTAPE 4 : PRÉVENTION DE FUTURES ATTEINTES À LA VIE PRIVÉE

- Quelles sont les étapes à court ou à long terme qui doivent être mises en place afin de corriger la situation (p. ex., la formation du personnel, la révision ou l'élaboration de politiques, une vérification)?