Secrétariat du Conseil du Trésor du Canada
Treasury Board of Canada Secretariat
Canada

Lignes directrices sur les atteintes à la vie privée

Publié : le 20 mai 2014

© Sa Majesté la Reine du chef du Canada,
représentée par le président du Conseil du Trésor, 2014

Publié par le Secrétariat du Conseil du Trésor du Canada
90 rue Elgin, Ottawa, Ontario, K1A 0R5, Canada

No de catalogue BT48-9/2014F-PDF
ISBN : 978-0-660-09808-1

Ce document est disponible sur Canada.ca, le site Web du gouvernement du Canada.

Ce document est disponible en médias substituts sur demande.

Nota : Pour ne pas alourdir le texte français, le masculin est utilisé
pour désigner tant les hommes que les femmes.

Also available in English under the title: Guidelines for Privacy Breaches

Lignes directrices sur les atteintes à la vie privée

Introduction

Les Canadiens et les Canadiennes attachent de l'importance à leur vie privée et à la protection de leurs renseignements personnels. Ils s'attendent à ce que les institutions fédérales respectent l'esprit et les exigences de la *Loi sur la protection des renseignements personnels* (la *Loi*). Le gouvernement du Canada s'est engagé à respecter la vie privée des personnes en ce qui a trait aux renseignements personnels relevant des institutions fédérales, et reconnaît qu'il s'agit d'un élément essentiel au maintien de la confiance du public à son égard.

Au sujet des présentes Lignes directrices

À titre de « ministre désigné » aux termes de la *Loi*, le président du Conseil du Trésor est chargé d'émettre des directives et des lignes directrices sur l'application de la *Loi*.

Les *Lignes directrices sur les atteintes à la vie privée* renferment des conseils pour les institutions concernant la gestion des atteintes à la vie privée. Les présentes Lignes directrices portent sur les exigences générales énoncées aux articles 4 à 8 de la *Loi* en ce qui concerne la collecte, la conservation, l'utilisation, la communication et le retrait des renseignements personnels.

La *Politique sur la protection de la vie privée* et la *Directive sur les pratiques relatives à la protection de la vie privée* qui appuient la *Loi* exigent que les institutions établissent des plans et des procédures relativement aux atteintes à la vie privée. Les présentes Lignes directrices doivent être utilisées de concert avec la Trousse d'outils pour la gestion des atteintes à la vie privée, qui procure des outils pour aider les institutions dans le processus de gestion des atteintes à la vie privée.

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

Une atteinte à la vie privée suppose la collecte, l'usage, la communication, la conservation ou le retrait inapproprié ou non autorisé de renseignements personnels. Les présentes Lignes directrices concernent principalement l'accès inapproprié ou non autorisé à des renseignements personnels ou la communication inappropriée ou non autorisée de tels renseignements, tels que définis par la *Loi.*

Une atteinte à la vie privée peut survenir au sein d'une institution ou à l'extérieur, et être le résultat d'erreurs de bonne foi ou d'actes malveillants commis par des employés, des tiers, des partenaires ou des intrus.

2. Causes potentielles des atteintes à la vie privée

Les exemples de situations suivantes pourraient avoir comme résultat que des renseignements personnels soient communiqués à des parties non autorisées ou que des parties non autorisées aient accès à des renseignements personnels :

- le vol, la perte ou la disparition d'équipement ou d'appareils renfermant des renseignements personnels;
- la vente ou l'aliénation d'équipement ou d'appareils renfermant des renseignements personnels qui n'ont pas été entièrement purgés avant la vente ou l'aliénation;
- le transfert d'équipement ou d'appareils renfermant des renseignements personnels pour lesquels aucune mesure de sécurité appropriée n'a été prise;
- l'utilisation d'équipement ou d'appareils pour transporter ou stocker des renseignements personnels à l'extérieur du lieu de travail, aux fins du télétravail ou d'autres arrangements de travail à l'extérieur du bureau, sans que des mesures de sécurité appropriées soient prises;
- l'utilisation inappropriée d'appareils électroniques pour transmettre des renseignements personnels, y compris les appareils de télécommunication;
- les intrusions qui donnent un accès non autorisé à des renseignements personnels détenus dans un immeuble, un espace de stockage des fichiers, une application, un système, un réseau local ou tout autre équipement ou appareil;
- le manque de sensibilisation des employés, des entrepreneurs ou autres tiers chargés du traitement des renseignements personnels à la nécessité de protéger la vie privée des individus;
- des mesures inadéquates de sécurité et de contrôle d'accès aux versions papier ou électroniques de documents, à l'intérieur ainsi qu'à l'extérieur du lieu de travail;
- l'absence de dispositions ou des dispositions adéquates en matière de protection de la vie privée dans des marchés ou des ententes sur l'échange de renseignements contenant des renseignements personnels;
- des mesures inadéquates de contrôle de l'accès aux renseignements personnels et des droits de modification de ces renseignements, qui peuvent entraîner un accès illicite aux dossiers renfermant des renseignements personnels et en permettre la falsification;
- l'hameçonnage (*phishing*), qui est un recours à des tactiques visant à tromper les particuliers pour les amener à fournir leurs renseignements personnels, soit directement ou par le biais d'un site Web frauduleux. Par exemple, un imposteur appelle un employé de l'institution afin d'obtenir son code d'accès en prétendant qu'il est en train de faire l'entretien du système de l'institution;
- le détournement de domaine (*pharming*), qui consiste à utiliser une fausse copie d'un site officiel du gouvernement du Canada afin de rediriger l'utilisateur vers un site Web frauduleux qui peut servir à voler des renseignements personnels à l'insu de l'utilisateur. Cette méthode exploite les faiblesses du DNS (*Data Network System*). Par exemple, une personne peut accéder à ce qu'il croit être un site Web officiel du gouvernement et fournir les renseignements personnels requis par le site. La

personne ne se doute pas qu'il a été redirigé vers une copie frauduleuse du site Web officiel.

3. Prévention des atteintes à la vie privée

Pour prévenir une atteinte à la vie privée, les institutions devraient :

- se conformer aux exigences de la *Politique sur la sécurité du gouvernement* (PSG) et aux autres directives émises par le Secrétariat du Conseil du Trésor du Canada (SCT). La Gendarmerie royale du Canada (GRC) et le Centre de la sécurité des télécommunications Canada (CSTC) émettent aussi respectivement des directives sur la sécurité physique et la sécurité des technologies de l'information. Les institutions fédérales peuvent également établir leurs propres politiques, procédures et lignes directrices en matière de sécurité en s'inspirant de ces normes;
- effectuer des évaluations des facteurs relatifs à la vie privée (ÉFVP) et des évaluations de la menace et des risques (EMR), conformément à la *Directive sur l'évaluation des facteurs relatifs à la vie privée*;
- tenir compte de la protection des renseignements personnels avant de conclure des marchés ou ententes sur l'échange de renseignements. Les institutions fédérales devraient prévoir dans ces marchés des dispositions pertinentes sur la protection de la vie privée, notamment l'obligation d'informer immédiatement l'institution fédérale de toute atteinte à la vie privée. Pour plus de renseignements, consultez le document du SCT intitulé *Document d'orientation : Prise en compte de la protection des renseignements personnels avant de conclure un marché*;
- assurer la formation régulière et continue du personnel, des gestionnaires et des cadres, afin de les sensibiliser aux exigences du Code de pratiques équitables en matière de renseignements (articles 4 à 8 de la *Loi sur la protection des renseignements personnels*), des politiques connexes du SCT et des pratiques et procédures de sécurité des ministères et des organismes;
- s'assurer que les employés qui travaillent en dehors des bureaux connaissent leurs responsabilités en matière de sécurité et de protection de la vie privée et que des mesures adéquates soient prises pour assurer la protection des renseignements personnels qu'ils traitent à l'extérieur des bureaux. Les institutions fédérales devraient envisager la possibilité de conserver les renseignements personnels à l'interne lorsque le télétravail ou des arrangements semblables risquent de compromettre la protection de la vie privée (p. ex., renseignements personnels très nombreux ou particulièrement délicats);
- établir des contrôles administratifs clairs afin de restreindre les droits d'accès et de modification pour les dossiers contenant des renseignements personnels aux seules personnes qui ont un besoin légitime de connaître cette information, et pour permettre aux institutions de mettre en place des pistes d'audit suffisantes pour faire en sorte que ces contrôles administratifs fonctionnent comme il se doit;
- utiliser le chiffrement pour protéger les renseignements personnels sauvegardés sur un ordinateur ou sur un support portable, ou communiqués par courriel, sur un réseau public, un réseau sans-fil, ou par l'entremise d'Internet. La *PSG* renferment d'autres orientations sur le chiffrement;
- établir des procédures claires relativement à l'utilisation des appareils sans-fil (p. ex., communications poste à poste [NIP à NIP]);
- en règle générale, ne pas transmettre de renseignements personnels par télécopieur sauf si cela est absolument nécessaire. Le cas échéant, il faut consulter les mesures de sécurité recommandées par le Commissariat à la protection de la vie privée à ceux qui communiquent des renseignements personnels par télécopieur;
- purger tout équipement ou autre appareil électronique de tout renseignement personnel avant de le vendre, de l'éliminer ou de le transférer, conformément aux lignes directrices de la GRC et du CSTC;
- avant de vendre ou de transférer des conteneurs de sécurité, comme des classeurs, des coffres-forts ou des étagères mobiles, à un autre centre de responsabilité ou à un tiers à l'extérieur du gouvernement, il faut les vider et s'assurer qu'il n'y reste aucun document classifié ou protégé;
- prendre les précautions suivantes contre l'« hameçonnage » et le « détournement de domaine » :
    - veiller à ce que la demande de renseignements personnels soit valide et que le demandeur soit bien la personne qu'il prétend être;
    - refuser de fournir de renseignements personnels en réponse à une demande non sollicitée faite par téléphone, télécopieur, lettre, pièce jointe à un courriel ou publicité par l'entremise d'Internet;
    - chercher les indices qui pourraient indiquer un site Web frauduleux (p. ex., erreurs d'orthographe, publicités inhabituelles, sections défectueuses du site);
    - vérifier la présence d'une icône de cadenas visible au bas de la page du navigateur pour s'assurer de transmettre des renseignements personnels par le biais d'une connexion sécurisée;
    - en cas de doute, vérifier le numéro de téléphone et appeler l'organisme afin d'en déterminer la validité.
- aviser immédiatement l'agent de sécurité du ministère, lorsque des données personnelles risquent d'être compromises et qu'une atteinte à la vie privée pourrait en résulter.

4. Processus de gestion des atteintes à la vie privée

Les institutions doivent consulter la Trousse d'outils pour la gestion des atteintes à la vie privée concernant les pratiques, plans et procédures efficaces en cas d'atteintes à la vie privée.

Parmi les exemples de pratiques exemplaires en gestion des atteintes à la vie privée, mentionnons :

- l'évaluation préliminaire et la limitation des conséquences;
- l'évaluation complète;
- l'envoi d'avis (aux personnes touchées et à la direction interne s'il y a lieu);
- l'atténuation et la prévention;
- un avis au Commissariat à la protection de la vie privée du Canada et au Secrétariat du Conseil du Trésor du Canada;
- le partage des leçons retenues.

Rôle des bureaux de première responsabilité (BPR)

Il incombe aux bureaux de première responsabilité (BPR) de prendre des mesures immédiates pour réprimer l'atteinte et protéger les dossiers, systèmes ou sites Web touchés comme suit :

- retirer, déplacer ou isoler les renseignements ou dossiers vulnérables, pour prévenir tout accès injustifié ultérieur;
- mettre temporairement hors service le site Web, l'application ou l'appareil, afin d'effectuer une évaluation complète de l'atteinte et de corriger les faiblesses;
- s'efforcer de récupérer les documents ou copies de documents communiqués à tort ou saisis par une personne non autorisée;
- remettre les documents à leur emplacement d'origine ou les retourner au destinataire visé, à moins qu'il ne soit nécessaire de les conserver à des fins probatoires (l'institution devrait consulter un avocat pour déterminer si cela est nécessaire).

Les BPR consignent aussi l'atteinte à la vie privée comme suit :

- décrire les circonstances dans lesquelles l'atteinte à la vie privée a été commise. L'outil Évaluation préliminaire et confinement par le BPR et le formulaire Évaluation préliminaire peuvent être mis à contribution dans le cadre de l'enquête sur l'atteinte à la vie privée. L'outil et le formulaire se trouvent dans la Trousse d'outils pour la gestion des atteintes à la vie privée;
- faire l'inventaire des renseignements personnels qui ont été ou pourraient avoir été compromis;
- identifier les parties dont les renseignements personnels ont été communiqués ou consultés à tort, volés ou perdus;
- identifier le secteur institutionnel ou le tiers responsable des renseignements personnels en question;
- inclure tout autre renseignement pertinent (p. ex., incidents semblables ou liés);
- déterminer les personnes touchées par l'atteinte ou, si cela s'avère impossible, cerner les groupes susceptibles de l'avoir été. L'institution devrait aussi décrire le processus qui a été suivi pour déterminer les personnes touchées;
- aviser le coordonnateur de l'accès à l'information et de la protection des renseignements personnels (AIPRP) ou le délégué pour la vie privée ainsi que l'agent de sécurité du ministère (ASM).La plupart des atteintes à la vie privée impliquent une infraction à la sécurité. Il importe de mettre le coordonnateur de l'AIPRP ou le délégué et l'ASM à contribution, pour que la protection de la vie privée et la sécurité des biens soient prises en considération dans le processus de résolution.

Rôle des agents de sécurité ministériels

En application de la *PSG* du Conseil du Trésor, les ministères doivent établir des politiques et des procédures afin de composer avec les incidents de sécurité (la plupart des atteintes à la vie privée impliquent une infraction à la sécurité). Dans la plupart des ministères, les ASM sont chargés de mener des enquêtes sur les incidents de sécurité.

Selon le processus établi, le coordonnateur de l'AIPRP, le délégué ou le fonctionnaire responsable de la sécurité doit aviser l'administrateur général et la Direction des communications le cas échéant.

- Si l'infraction suscite ou pourrait susciter l'intérêt du public, il faudrait en aviser les responsables des communications pour qu'ils puissent préparer des documents d'information en réponse aux questions du public, des médias ou de la Chambre des communes. Toute information personnelle devrait toutefois être retirée et ne pas être divulguée au personnel des communications.

Si une infraction à la sécurité a entraîné une atteinte à la vie privée, l'ASM devrait mener une enquête pour cerner les faiblesses des procédures et processus de sécurité et devrait formuler des recommandations lorsqu'il est approprié ou nécessaire de le faire. Si la *PSG* l'exige, il peut être nécessaire de signaler l'incident aux autorités policières. Si l'infraction a une incidence sur la sécurité nationale, il faudrait également en faire part au Service canadien du renseignement de sécurité (SCRS).

Les bureaux responsables de la protection de la vie privée et de la sécurité devraient établir un processus interne de gestion et de suivi des atteintes à la vie privée, qui peut inclure ce qui suit :

- la révision des procédures et politiques internes;
- une formation additionnelle aux employés;
- des restrictions d'accès à certains renseignements personnels pour les employés, basées sur les rôles et les responsabilités et sur le principe du « besoin d'en connaître »;
- le chiffrement des renseignements personnels;
- des dispositions contractuelles plus claires en cas d'atteinte à la vie privée.

Rôle des coordonnateurs de l'AIPRP

Comme l'exige la *Directive sur les pratiques relatives à la protection de la vie privée*, les institutions et leurs délégués sont tenus d'établir des plans et des procédures en cas d'atteintes à la vie privée. Cette exigence incombe habituellement au coordonnateur de l'AIPRP.

Les coordonnateurs de l'AIPRP et leurs bureaux sont responsables d'enquêter et de gérer le cycle de vie d'une atteinte à la vie privée et d'aviser le SCT et le CPVP, s'il y a lieu. Ils sont l'unique bureau de liaison de l'institution pour aviser le CPVP et le SCT.

1. Les institutions devraient conserver un registre de toutes les atteintes à la vie privée.

- Le registre devrait couvrir la nature et la portée de l'atteinte, le type de renseignements personnels compromis, les parties en cause, les risques prévus, les dispositions prises ou prévues pour aviser les personnes touchées, les mesures correctives prises et déterminer si l'enquête a permis de conclure à une atteinte substantielle à la vie privée.
- Les registres documentant les atteintes à la vie privée ne devraient pas contenir de renseignements personnels.

- Les institutions devraient documenter toute décision de ne pas aviser le CPVP et le SCT dans un dossier ministériel standard, avec justification à l'appui.
- Les institutions devraient examiner les conseils et recommandations formulés par le CPVP afin d'atténuer les risques de répétition du problème.
- Les institutions peuvent utiliser l'outil Établissement de rapports qui se trouve dans la Trousse d'outils pour la gestion des atteintes à la vie privée pour tenir ces registres à jour.

2. Les institutions devraient envisager la possibilité d'aviser les personnes dont les renseignements personnels ont été communiqués à tort, volés ou perdus.

- Dans la mesure du possible, il est fortement recommandé à l'institution d'aviser toute personne dont les renseignements personnels ont été ou pourraient avoir été volés, perdus ou communiqués sans autorisation, surtout si l'atteinte :
    - touche des données personnelles de nature délicate comme des renseignements financiers ou médicaux, p.ex., le numéro d'assurance sociale;
    - risque d'entraîner un vol d'identité ou une fraude similaire;
    - risque autrement de causer un préjudice ou un embarras à la carrière, la réputation, la situation financière, la sécurité, la santé ou le mieux-être d'une personne.
- L'institution devrait aviser les personnes touchées de l'infraction dans les meilleurs délais, pour leur permettre de prendre des mesures de protection ou d'atténuer les préjudices causés par le vol d'identité ou les autres torts possibles.
- Consulter l'ASM et les autorités policières pour déterminer si l'envoi de l'avis devrait être retardé afin de s'assurer de ne compromettre aucune enquête. Il faudrait prendre soin de ne pas alarmer inutilement les personnes, particulièrement si l'institution soupçonne mais ne peut pas confirmer que certaines personnes ont été touchées par l'atteinte.
- Il est toujours préférable d'aviser les personnes touchées directement par lettre (courrier de première classe, de préférence), par téléphone ou en personne, sauf si la personne est introuvable ou si le nombre de personnes est si élevé que la tâche deviendrait trop lourde. Des exemples de lettres se trouvent dans la Trousse d'outils pour la gestion des atteintes à la vie privée.

En pareil cas, l'institution peut afficher un avis bien en vue dans son site Web ou sur les écrans d'accès aux données ministérielles ou faire passer des annonces dans les principaux médias locaux ou nationaux (télévision, radio, journaux et revues). L'institution ne doit utiliser le courrier électronique que si la personne a consenti à recevoir des avis électroniques.

3. L'avis envoyé aux personnes touchées devrait inclure:

- une description générale de l'incident, y compris la date et l'heure;
- la source de l'atteinte (une institution, un entrepreneur ou une partie à une entente sur l'échange de renseignements);
- une liste des renseignements personnels qui ont été ou pourraient avoir été compromis;
- une description des mesures prises ou à prendre pour récupérer les renseignements personnels, réprimer l'atteinte et empêcher qu'elle ne se reproduise;
- des conseils sur les moyens de réduire les risques de vol d'identité ou sur les mesures à prendre lorsque les renseignements personnels ont été compromis (p. ex., numéro d'assurance sociale);
- le nom et les coordonnées d'un représentant de l'institution à qui les personnes touchées peuvent s'adresser pour discuter de la question plus en détail ou pour obtenir de l'aide;
- un renvoi indiquant que le CPVP a été informé de la nature de l'atteinte et que la personne a le droit de porter plainte au CPVP, s'il y a lieu;
- l'institution devrait également informer les personnes touchées des progrès de l'enquête et du règlement des questions en suspens.

4. Les institutions et leurs délégués doivent établir un processus de déclaration obligatoire des atteintes substantielles à la vie privée au Commissariat à la protection de la vie privée (CPVP) et au Secrétariat du Conseil du Trésor du Canada (SCT). Ces procédures doivent correspondre à la Politique sur la sécurité du gouvernement (PSG).

- Des atteintes sont réputées « substantielles » si :
    - elles concernent des renseignements personnels sensibles;
    - il serait raisonnable de penser qu'elles pourraient causer un dommage ou un préjudice grave à une personne ou qu'elles touchent un grand nombre de personnes.
- Parmi les exemples de renseignements personnels sensibles, mentionnons, sans s'y limiter :
    - renseignements médicaux, psychiatriques ou psychologiques;
    - information compilée et identifiable dans le cadre d'une enquête sur une violation potentielle de la loi;
    - antécédents criminels;
    - renseignements sur l'admissibilité à des avantages sociaux ou sur la détermination des taux de ces avantages;
    - renseignements décrivant la situation financière d'une personne (ses revenus, son passif, ses avoirs nets, ses soldes bancaires, ses déclarations de revenus, ses activités ou antécédents financiers ou sa solvabilité);
    - renseignements sur la race ou l'origine ethnique d'une personne, ses croyances religieuses ou convictions politiques, ses associations ou son mode de vie.
- Parmi les exemples de dommage ou de préjudice grave à une personne, mentionnons :
    - le vol d'identité ou toute fraude du même genre;
    - une perte matérielle importante pour la personne;
    - un préjudice ou un embarras de longue durée qui aura des répercussions négatives directes sur la personne ou sur sa carrière, sa réputation, sa situation financière, sa sécurité, sa santé ou son mieux-être.

On peut trouver des formulaires de déclaration d'atteinte substantielle à la vie privée sur le site Web du CPVP. Le même formulaire

dûment rempli peut être envoyé à la fois au CPVP et au SCT. Le formulaire se trouve sur le site Web du CPVP et s'intitule : Formulaire de rapport d'incident en cas d'atteinte à la vie privée. En complétant le formulaire de déclaration d'atteinte à la vie privée, les institution ne doivent pas inclure de renseignements personnels.

5. Suivi

L'institution devrait :

- veiller à ce qu'un plan d'atténuation des risques cernés au cours de l'enquête soit élaboré et qu'il soit mis en uvre;
- informer le CPVP et les parties touchées, s'il y a lieu, du plan d'atténuation des risques à mettre en uvre.

6. Politiques et documents d'orientation pertinents

Secrétariat du Conseil du Trésor du Canada

- Directive sur l'évaluation des facteurs relatifs à la vie privée
- Document d'orientation : Prise en compte de la protection des renseignements personnels avant de conclure un marché
- Norme de sécurité relative à l'organisation et l'administration
- Norme opérationnelle de sécurité : Gestion de la sécurité des technologies de l'information (GSTI)
- Norme opérationnelle sur la sécurité matérielle
- Politique sur la protection de la vie privée
- Politique sur la sécurité du gouvernement
- Trousse d'outils pour la gestion des atteintes à la vie privée

Gendarmerie royale du Canada

- Sécurité matérielle
- Publications, instruments de politique et lignes directrices

Centre de la sécurité des télécommunications Canada

- Lignes directrices du CST : Effacement et déclassification des supports d'information électroniques

Commissariat à la protection de la vie privée du Canada

- Commissariat à la vie privée – Fiches d'information
- Rapport d'incident en cas d'atteinte à la vie privée au Commissariat

Les questions concernant le contenu des présentes lignes directrices doivent être adressées aux experts de la sécurité et de la protection de la vie privée de l'institution, qui peuvent à leur tour consulter le Secrétariat du Conseil du Trésor du Canada à l'adresse ippd-dpiprp@tbs-sct.gc.ca pour obtenir de plus amples précisions.