POLITIQUE DE GESTION

Commissaire à la lutte contre la corruption Québec	**PROTECTION DES RENSEIGNEMENTS PERSONNELS**	**Codification** VOLUME 2 Fiche 2.2
	Directive en cas de perte ou de vol de renseignements personnels	**Dernière mise à jour :** 29/09/2013

ÉNONCÉ DE PRINCIPE

La présente directive vise à définir le cadre opérationnel à suivre au sein du Commissaire à la lutte contre la corruption lorsqu'une perte ou un vol de renseignements personnels est constaté.

Elle vise du même coup à limiter les préjudices et dommages pouvant résulter d'une perte ou d'un vol de renseignements personnels.

CHAMP D'APPLICATION

La directive s'applique à tous les membres du personnel du Commissaire à la lutte contre la corruption.

La directive s'applique également aux individus liés au Commissaire à la lutte contre la corruption par contrat de services professionnels.

DÉFINITIONS

Renseignements personnels
En vertu de la Loi sur l'accès aux documents des organismes publics et la protection des renseignements personnels, sont personnels, dans un document, les renseignements qui concernent une personne physique et qui permettent de l'identifier.

À titre indicatif, ont été reconnus comme renseignements personnels au sujet d'un individu, les renseignements d'identité, la photographie ou vidéo d'une personne, les renseignements sur sa situation financière et familiale, ses caractéristiques physiques, les éléments de son dossier d'employé, de son dossier scolaire, de son dossier médical, ses opinions personnelles, un témoignage comme témoin, le contenu d'une plainte ou d'une dénonciation permettant d'identifier son auteur.

Cette loi confère cependant un caractère public à différents renseignements personnels détenus par les organismes publics, comme le nom, le titre, la fonction, l'adresse et le numéro de téléphone du lieu de travail et la classification d'un membre d'un organisme public, de son conseil d'administration ou de son personnel de direction et, dans le cas d'un ministère, d'un sous-ministre, de ses

adjoints et de son personnel d'encadrement et elle prévoit qu'un renseignement personnel qui a un caractère public en vertu de la loi n'est pas personnel.

Les renseignements suivants ont également un caractère public :

- le nom, le titre, la fonction, l'adresse et le numéro de téléphone du lieu de travail et la classification, y compris l'échelle de traitement rattachée à cette classification, d'un membre du personnel d'un organisme public. Cependant, la divulgation de ces renseignements personnels ne doit pas avoir pour effet de révéler le traitement d'un membre du personnel d'un organisme public ;

- un renseignement concernant une personne en sa qualité de partie à un contrat de services conclu avec un organisme public, ainsi que les conditions de ce contrat;

- le nom et l'adresse d'une personne qui bénéficie d'un avantage économique conféré par un organisme public en vertu d'un pouvoir discrétionnaire et tout renseignement sur la nature de cet avantage;

- le nom et l'adresse de l'établissement du titulaire d'un permis délivré par un organisme public et dont la détention est requise en vertu de la loi pour exercer une activité ou une profession ou pour exploiter un commerce;

Toutefois, ces renseignements n'ont pas un caractère public si leur divulgation est de nature à nuire ou à entraver le travail d'un organisme qui, en vertu de la Loi, est chargé de prévenir, détecter ou réprimer le crime.

MODALITÉS D'APPLICATION

- Dès que la perte ou le vol de renseignements personnels est constaté, tout employé doit en aviser **immédiatement** son supérieur immédiat.

- Le supérieur hiérarchique doit sans délai informer le commissaire et le responsable de l'accès aux documents et de la protection des renseignements personnels.

- Le commissaire évalue les mesures nécessaires à mettre en place, selon la situation.

- Un rapport contenant notamment les informations listées ci-dessous sera produit :

  - identifier les renseignements personnels touchés ainsi que leur support;
  - identifier les personnes, leur nombre ainsi que le groupe de personnes touchées;
  - établir le contexte des événements (date, heure, lieu, etc.) en identifiant, si possible, les circonstances entourant la perte (cause, personnes susceptibles d'être impliquées dans l'incident, etc.);
  - répertorier les mesures de sécurité physiques et informatiques en place lors de l'incident;
  - informer, au besoin, le service de police sur les circonstances laissant croire à la possibilité d'un crime;
  - aviser, au besoin, la Commission d'accès à l'information.

- Le commissaire doit prendre sans tarder des mesures adéquates pour limiter les conséquences pour les personnes concernées d'une possible utilisation malveillante de leurs renseignements personnels, de l'usurpation ou du vol de leur identité, soit :

  - mettre fin à la pratique non-conforme, le cas échéant;
  - récupérer les dossiers physiques ou numériques, selon le cas;
  - révoquer ou modifier les mots de passe ou les codes d'accès informatiques;
  - contrôler les lacunes dans les systèmes de sécurité.

- Le commissaire doit également évaluer les risques de la perte ou du vol de renseignements personnels. Pour ce faire, il doit :

  - compléter une **évaluation préliminaire des risques**, en considérant la sensibilité des renseignements personnels en cause, leur nature,

leur quantité, la possibilité de les combiner avec d'autres renseignements, les personnes concernées, etc.;

- déterminer le contexte de l'incident, incluant :
  - la cause (ex : le caractère délibéré ou non de la perte ou du vol de renseignements personnels, l'erreur humaine, une faille informatique, etc.);
  - les auteurs connus ou probables des renseignements personnels perdus ou subtilisés (ex. organisation criminelle, public en général, etc.);
  - l'étendue de la situation (nombre de personnes touchées et secteurs touchés);
  - le caractère systémique ou non de la disparition des renseignements personnels (particulièrement lorsque la perte n'est pas générée directement par une intervention humaine);
  - une évaluation de la probabilité qu'un événement similaire se reproduise.
- évaluer la possibilité que les renseignements personnels concernés fassent l'objet d'une utilisation préjudiciable pour les personnes concernées en tenant compte, notamment, des mesures de sécurité prises pour les protéger, de leur difficulté d'accès et de leur intelligibilité (mot de passe, encodage, etc.);
- évaluer le caractère réversible ou non de la situation, dont la possibilité de récupérer les renseignements personnels;
- évaluer si les mesures immédiates prises étaient adéquates pour limiter l'atteinte et les compléter si nécessaire;
- déterminer les préjudices potentiels, notamment en évaluant les possibilités d'utilisation future des renseignements personnels par des personnes malveillantes, notamment le vol d'identité;
- déterminer les priorités et identifier les actions à prendre à partir des résultats de l'évaluation de ces risques.

- Le commissaire doit aviser les organisations et personnes concernées par la perte ou le vol de renseignements personnels. Pour ce faire, il doit déterminer qui doit être mis au courant de la perte ou du vol de renseignements personnels en fonction de l'évaluation des risques :

    - service de police : dans les cas où la disparition peut résulter de la commission d'un crime, le service de police concerné doit être avisé des éléments entourant cette disparition tout d'abord et, ensuite, de toutes les démarches subséquentes. Il est nécessaire de porter une attention particulière afin de ne pas nuire à l'enquête et de préserver les éléments de preuve pouvant être pertinents;

    - Commissaire d'accès à l'information : si les personnes concernées par les renseignements personnels proviennent du Québec, la Commission pourrait amorcer une inspection ou une enquête et jouer un rôle de conseiller dans la recherche de solutions;

    - autres : il peut également être nécessaire d'aviser d'autres intervenants, tels que les agences de crédit, un mandataire, un cocontractant, une instance gouvernementale, un syndicat, un ordre professionnel, etc.

    Toutefois, dans la diffusion des informations concernant la perte de renseignements personnels, une attention particulière doit être portée afin de ne pas aggraver le préjudice que pourraient subir les personnes concernées (ex : limiter au minimum les renseignements personnels dans les avis).

    Le commissaire doit également désigner les personnes d'aviser les intervenants externes identifiés précédemment ainsi que le moment et le moyen (lettre, courriel, téléphone) et le cas échéant, identifier et consigner les motifs à l'origine de la décision de ne pas aviser les personnes concernées et les autres intervenants.

- Le commissaire doit faire **rapport** sur la perte ou le vol de renseignements personnels en :

    - approfondissant l'analyse des circonstances de la perte ou du vol des renseignements personnels et effectuant une description

chronologique des événements et des actions prises face à cet incident, incluant les dates et les intervenants concernés;

- répertoriant et examinant les normes, politiques ou directives internes en place au moment de l'incident, autant au niveau de la sécurité informatique, lorsque l'information est en cause, que de la protection des renseignements personnels en général;

- vérifiant si ces normes ou directives internes ont été suivies par les personnes impliquées; identifiant les raisons pour lesquelles elles n'ont pas été suivies, le cas échéant.

RÔLES ET RESPONSABILITÉS

Le responsable de l'accès :
Il tient à jour cette politique et conseille toute personne sur son application.

Le gestionnaire d'une unité administrative :
Il doit s'assurer que les mesures de sécurité adéquates sont en place pour limiter les risques de perte ou de vol de renseignements personnels et aviser, le cas échéant, immédiatement le commissaire et le responsable de l'accès à l'information.

Chaque membre du personnel :
Chacun est responsable d'assurer la protection des renseignements personnels et confidentiels qu'il utilise dans le cadre de ses fonctions et doit immédiatement aviser son supérieur immédiat en cas de perte ou de vol.

Cette politique a été approuvée le : 2014/03/04

Le commissaire à la lutte contre la corruption,

Robert Lafrenière