POLITIQUE PROTECTION DES RENSEIGNEMENTS PERSONNELS

ADOPTÉE PAR :	Conseil d'administration	Résolution : ca2015.12.16-14
MODIFICATION :	Conseil d'administration	Résolution : ca2019.12.12-2
MISE EN VIGUEUR :	16 décembre 2015	

Sommaire

SECTION 1 – INTRODUCTION

But du présent document

La présente Politique de protection des renseignements personnels (« Politique ») expose la façon dont la Mutuelle traite les renseignements personnels qu'elle détient aux fins de ses activités, conformément à la *Loi sur la protection des renseignements personnels dans le secteur privé* (RLRQ c. P-39.1) (la « LPRP »).

Documents reliés

- Loi sur la protection des renseignements personnels dans le secteur privé (RLRQ c. P-39.1);
- Politique sur la conformité;
- Politique sur la gestion intégrée des risques;
- Politique sur les actifs informationnels;
- Plan directeur TI (guide de gestion);
- Code civil du Québec
- Code de déontologie de la Mutuelle

Définitions particulières

Renseignement personnel : Désigne tout renseignement qui concerne une personne physique et permet de l'identifier ou de la distinguer, notamment le nom, l'âge, le sexe et l'adresse de cette personne.

Politique

La gestion des renseignements personnels fait l'objet d'un encadrement juridique très élaboré. Une faute commise à ce titre présente des incidences importantes sur la réputation de la Mutuelle.

SECTION 2 – CONSTITUTION DES DOSSIERS ET TRAITEMENT DES INFORMATIONS

Constitution des dossiers

Les renseignements personnels détenus par la Mutuelle se retrouvent essentiellement dans les dossiers d'employés, ceux des administrateurs, ainsi que les candidatures reçues dans les deux cas. Des renseignements personnels peuvent se trouver au dossier de chaque membre ainsi que dans certains dossiers de réclamation.

L'objet de la constitution du dossier doit être inscrit au dossier, et ce, avant ou au moment de la collection des renseignements personnels[1]. Lorsque les renseignements sont demandés verbalement, l'employé faisant la collecte d'information doit être en mesure de bien expliquer la raison de cette collecte. En cas de formulaire, celui-ci doit clairement indiquer dans quel but l'information personnelle est collectée[2]. Si la Mutuelle venait qu'à changer le but de la collecte d'information initiale, celle-ci doit obtenir le consentement de la personne concernée préalablement.

La personne qui fait l'objet de la demande doit également être informée de l'utilisation qui sera faite des renseignements, de l'endroit où sera détenu son dossier et des droits d'accès à l'information ou de rectification[3].

Ainsi, les objets de la constitution des dossiers de la Mutuelle sont les suivants :

- Dossier d'employé : L'information recueillie auprès d'un employé est utilisée dans la gestion de son emploi à la Mutuelle pour traiter de différentes obligations telles que : le traitement de sa rémunération et les diverses informations devant être transmises aux différents paliers du gouvernement, son REER collectif, son adhésion à l'assurance collective, le traitement d'une

[1] Art. 4 LPRP
[2] Art. 8 LPRP, par 1e
[3] Art. 8 LPRP par. 2e et 3e

invalidité (indemnisation et suivi du dossier d'emploi), ou autre forme d'indemnisation impliquant l'employeur, ses contacts en cas d'urgence, des enquêtes de crédit et plumitif afin de répondre à un encadrement interne ou externe, le traitement d'un dossier de CNESST, l'information devant être transmise à l'AMF et au Registraire pour certains de ceux-ci ainsi que toute autre situation exigeant ces informations tels que requis par les différentes législations.

- Dossier d'administrateur : L'information recueillie auprès d'un administrateur est utilisée pour traiter de différents dossiers relatifs à son poste tels que : le traitement de sa rémunération et les diverses informations devant être transmises aux différents paliers du gouvernement, ses contacts en cas d'urgence, des enquêtes de crédit et plumitif afin de répondre à l'encadrement externe et interne[4], l'information devant être transmise à l'AMF et au Registraire ainsi que toute autre situation exigeant ces informations tels que requis par les différentes législations.
- Dossier des membres : L'information recueillie auprès d'un membre est utilisée dans la gestion de son dossier d'assurance et du respect des différentes législations à laquelle la Mutuelle est assujettie. Ces informations permettent aussi le traitement des avantages consentis par la Mutuelle.
- Dossiers d'indemnisation : Dans les dossiers d'indemnisation, si l'étude du dossier l'exige, la Mutuelle amassera de l'information sur le réclamant et sur les différentes parties concernées afin d'être en mesure de traiter la réclamation en question.
- Dossier d'un candidat à l'emploi ou d'un candidat administrateur: D'abord, les candidats fournissent leur CV pour se faire connaître de la Mutuelle. Ensuite, l'information additionnelle recueillie auprès d'un candidat, avec l'autorisation de ce dernier, est principalement utilisée pour enquêtes de crédit et plumitif ainsi que permettre à la Mutuelle de vérifier ses références.

L'objet d'un dossier constitué autre que ceux mentionnés précédemment devra être documenté.

Seuls les renseignements personnels pertinents à l'objet du dossier pour lequel ils sont nécessaires doivent être recueillis[5]. La Mutuelle recueille les renseignements personnels auprès de la personne concernée, et ce, avec son consentement, à moins que celle-ci ou la LPRP autorise la cueillette auprès d'autrui.

Tant qu'une personne est un employé ou un administrateur de la Mutuelle et pendant une période raisonnable à la suite de son départ, en respect avec les exigences légales, un dossier physique et/ou électronique est tenu par la Direction générale et contient, notamment, les renseignements nécessaires pour administrer le contrat de travail des employés et administrateurs.

Tant qu'un membre est actif et pendant une période raisonnable à la suite de son départ, compte tenu des dispositions législatives à cet égard[6], un dossier physique et/ou électronique est tenu par la Mutuelle. Aussi, pour les membres inactifs ayant eu une couverture d'assurance responsabilité, ces dossiers sont conservés indéfiniment étant donné que les risques de réclamations perdurent, car cette garantie est rattachée à l'acte (par exemple, les cas d'abus). Les dossiers de réclamations sont conservés tant que la

[4] Ligne directrice sur les critères de probité et de compétence, Politique d'encadrement des administrateurs et dirigeants et Code d'éthique et de déontologie
[5] Art. 5 LPRP
[6] Règlement sur la tenue et la conservation des livres et registres, notamment

réclamation est active et pendant une période raisonnable par la suite en respect avec les exigences légales[7].

Détention, utilisation et confidentialité des renseignements personnels

Les renseignements personnels sont détenus de façon à ce que leur caractère confidentiel soit assuré, et ce, peu importe le support utilisé. Les documents papier sont conservés dans des endroits barrés. Pour ce qui est des documents électroniques, ceux-ci sont conservés dans des répertoires avec accès restreints et font l'objet de différentes mesures de sécurité informatique additionnelles détaillées dans les politiques et guides correspondants.

La Mutuelle veille à ce que les renseignements détenus soient à jour et exacts au moment où elle les utilise pour prendre une décision relative au dossier en question.

En ce qui a trait aux renseignements concernant les employés, ceux-ci ont l'obligation de transmettre sans délai toute modification relative au contenu de leur dossier.

Accès aux renseignements personnels

L'accès aux renseignements personnels détenus par la Mutuelle s'effectue suivant la LPRP. Les personnes suivantes ont un droit d'accès aux renseignements personnels détenus par la Mutuelle, à moins d'une obligation de refus prévu à la LPRP :

- La personne concernée;
- Le représentant ou le mandataire de la personne concernée, sur production d'un consentement écrit par la personne visée par l'information. Une copie de cette autorisation sera transmise à la *Personne responsable des demandes d'accès aux renseignements personnels et de leur protection* avant que les renseignements ne soient communiqués;
- Les membres du personnel de la Mutuelle pour qui il est nécessaire de prendre connaissance du renseignement personnel dans l'exercice de leurs fonctions;
- Les réassureurs dans le traitement de dossiers d'assurance, lorsque cette information est nécessaire;
- Certains fournisseurs de service tel que : le service de paie, les experts en sinistres et autres fournisseurs au besoin, exclusivement dans le cadre de leur mandat, lorsque cette information est nécessaire.

Communication des renseignements personnels

La Mutuelle peut communiquer des renseignements personnels concernant une personne physique à un tiers avec le consentement de cette personne. Les demandes de confirmation de salaire lors de vérifications de crédit, ainsi que les confirmations d'emploi après le départ d'un employé ou d'un administrateur, ou toute autre demande de cette nature, sont traitées uniquement avec le consentement écrit de cette personne.

La Mutuelle peut communiquer des renseignements personnels à un tiers sans le consentement de la personne physique lorsque cette communication est nécessaire à l'exercice d'un mandat ou à l'exécution

[7] Règlement sur la tenue et la conservation des livres et registres

d'un contrat de service ou d'entreprise confié par la Mutuelle (par exemple, le support à la paie). Elle peut également agir de la sorte en regard des personnes suivantes :

- Les procureurs de la Mutuelle;
- Le Procureur général du Québec, si le renseignement est requis aux fins d'une poursuite pour infraction à une loi applicable au Québec;
- Un organisme qui, en vertu de la LPRP, est chargé de prévenir, de détecter ou de réprimer le crime ou les infractions aux lois et qui peut le requérir dans l'exercice de ses fonctions;
- Revenu Québec, l'Agence du revenu du Canada et autres organismes gouvernementaux pour lesquels la Mutuelle a l'obligation de répondre;
- Toute personne à qui cette communication doit être faite en raison d'une situation d'urgence mettant en danger la vie, la santé ou la sécurité de la personne concernée.

La Mutuelle peut également communiquer un renseignement personnel à un tiers sans le consentement de la personne concernée pour tout autre motif prévu par la LPRP.

Motifs de refus

La Mutuelle peut refuser en tout ou en partie de communiquer à une personne des renseignements personnels qu'elle détient si :

- ces documents sont visés par le secret professionnel au sens de l'article 9 de la *Charte des droits et libertés de la personne* (RLRQ c. C-12); ou
- la communication des renseignements qu'elle détient peut avoir effet sur une procédure judiciaire, déposée ou imminente; ou
- pour tout autre motif prévu par la LPRP.

La Mutuelle doit refuser de donner communication d'un renseignement personnel concernant une personne lorsque la divulgation révélerait vraisemblablement un renseignement personnel sur un tiers et que cette divulgation serait susceptible de nuire sérieusement à ce tiers. La Mutuelle peut cependant communiquer un tel renseignement personnel si le tiers y consent.

SECTION 3 – MESURES DE PROTECTION

Protection des données personnelles

La Mutuelle doit s'assurer de protéger les renseignements personnels en tout temps, et ce, quelle que soit la forme sous laquelle ils sont conservés. Les mesures de sécurité doivent protéger les renseignements personnels contre la perte ou le vol ainsi que contre la consultation, la communication, la copie, l'utilisation ou la modification non autorisée.

D'abord, **avant** qu'une personne, un fournisseur ou un consultant n'ait accès à des renseignements personnels détenus par la Mutuelle, il est impératif que ceux-ci signent le code de déontologie de la Mutuelle ou une entente de confidentialité selon le cas.

Voici les mesures de sécurité de la Mutuelle :

- Les documents papier contenant des renseignements personnels sont toujours conservés sous clé et le bureau est muni d'un système d'alarme lorsque celui-ci est fermé. Il en est de même pour tout disque dur, clé USB ou autre contenant de telles informations.

- Les ordinateurs portables ou ordinateurs personnels utilisés dans le cadre du travail ne doivent contenir aucun renseignement personnel visé par la présente politique. Tous les dossiers informatiques de la Mutuelle se trouvent sur le serveur, l'ordinateur utilisé ne servant que d'interface. Occasionnellement, des renseignements personnels peuvent être enregistrés sur un portable lorsqu'une situation l'exige (travail à distance sans accès aux serveurs). Dans ce cas, les informations doivent être détruites du portable dès le retour au travail.
- Les serveurs de la Mutuelle contiennent énormément de renseignements personnels. Ces serveurs sont protégés des accès par différentes protections. D'abord, les employés de la Mutuelle doivent avoir un code d'usager valide ainsi qu'un mot de passe à changement périodique. Les employés n'ont accès qu'aux répertoires et aux différentes applications ou différents modules qui les concernent dans leur travail. Il en est de même pour les administrateurs, consultants ou fournisseurs externes qui auraient besoin d'accès au serveur. Finalement, le support informatique (en impartition) a de hauts standards de sécurité et restreint les accès qu'aux techniciens concernés par la Mutuelle. Tout le personnel du fournisseur informatique fait l'objet de vérifications de la part de son employeur et signe un engagement de confidentialité.
- Les serveurs de la Mutuelle sont protégés des accès externes. Ces protections sont élaborées dans la Politique sur les actifs informationnels ainsi que dans le Plan directeur TI.

Conservation d'un registre d'atteintes aux mesures de sécurité

La Mutuelle conserve un registre de toutes les « atteintes aux mesures de sécurité », et ce, dans les 24 mois suivant la date de l'atteinte.

Par « atteintes aux mesures de sécurité », on entend toute communication non autorisée ou perte de renseignements personnels, ou accès non autorisé à ceux-ci, par suite d'une atteinte aux mesures de sécurité d'une organisation ou du fait que ces mesures n'ont pas été mises en place. À titre d'exemple, les situations suivantes seraient considérées comme une atteinte aux mesures de sécurité :

- La perte ou le vol d'une clé USB, d'un disque dur ou d'un ordinateur ou tout autre appareil électronique contenant des renseignements personnels relatifs aux dossiers de la Mutuelle;
- La découverte d'une tentative de piratage d'un serveur contenant des renseignements personnels;
- La découverte d'un virus ayant affecté un ordinateur ou un réseau contenant des renseignements personnels;
- La découverte d'un employé ayant accédé à des renseignements personnels ne respectant pas ses droits d'accès.

Ainsi, dans le registre, la Mutuelle doit documenter chaque problème de sécurité touchant aux informations personnelles, qu'il soit informatique, matériel ou humain et ce, qu'il y ait eu des dommages ou non.

Obligation d'informer les autorités en cas d'atteinte aux mesures de sécurité

La Mutuelle notifie le plus rapidement possible la Commission d'accès à l'information, dès qu'une atteinte aux mesures de sécurité pourrait entraîner un « préjudice grave ».

Un « préjudice grave » comprend la lésion corporelle, l'humiliation, le dommage à la réputation ou aux relations, la perte financière, le vol d'identité, l'effet négatif sur le dossier de crédit, le dommage aux biens ou leur perte, et la perte de possibilités d'emploi ou d'occasion d'affaires ou d'activités professionnelles.

Ainsi, pour chaque incident, la Mutuelle doit procéder à l'évaluation du risque de préjudice en considérant notamment le degré de sensibilité des renseignements personnels en cause et la probabilité que les renseignements soient mal utilisés.

Le signalement d'une atteinte à la vie privée doit se faire à l'aide du formulaire suivant :

http://www.cai.gouv.qc.ca/documents/CAI_FO_decl_incident_securite.docx

Obligation d'informer les personnes concernées en cas d'atteinte aux mesures de sécurité

Lorsque la Mutuelle découvre qu'un incident a pu entraîner la divulgation de données personnelles, elle en informe toutes les personnes dont les données ont été compromises, et ce, même si la Mutuelle n'a pas la certitude que leurs données ont été divulguées. Cette communication doit se faire rapidement après la découverte de l'atteinte aux renseignements personnels.

Possibilité de porter plainte à l'égard du non-respect de la protection des renseignements personnels

Il est possible de porter plainte à l'égard du non-respect de la protection des renseignements personnels. Pour plus de détail, vous référez à la Politique sur le traitement des plaintes et le règlement des différends.

SECTION 4 – ATTRIBUTION DES RESPONSABILITÉS

Imputabilité, rôles et responsabilités

Personne responsable de l'accès aux renseignements personnels et de leur protection

Le directeur général de la Mutuelle est la Personne responsable de l'accès aux renseignements personnels et de leur protection.

Conseil d'administration

Le conseil d'administration a les responsabilités suivantes :

a)
b) Promouvoir une culture de protection des renseignements personnels;
c) Adopter la Politique de protection des renseignements personnels sur la recommandation du comité d'éthique et s'assurer de sa révision périodique.

Direction générale

Le directeur général a les responsabilités suivantes :

a) Assurer la mise à jour de la présente Politique;
b) Mettre en place des mesures de protection des renseignements personnels;
c) Assurer l'application constante et rigoureuse de la présente Politique;

d) Assurer la protection des renseignements personnels et la prévention d'utilisation inappropriée des renseignements personnels détenus par la Mutuelle sur ses membres, employés, administrateurs et autres;
e) Assurer la publication des renseignements de cette politique sur le site Web de la Mutuelle ainsi que les éléments requis par les lois applicables;
f) Assurer la formation du personnel et la transmission de l'information relative à la présente politique et aux pratiques de la Mutuelle.

Employés et administrateurs

Les employés et les administrateurs de la Mutuelle doivent connaître la présente politique et s'assurer de son respect en tout temps. Le respect de cette politique implique aussi:

- La lecture de courriel sur les cellulaires ou autres appareils électroniques, ou encore l'utilisation de renseignements personnels par le biais de ces appareils. L'usager doit s'assurer que ces appareils soient munis de mots de passe;
- L'information transportée hors du bureau, quelque qu'en soit la raison, doit toujours être faite de façon sécurisée.

De plus, ils doivent aviser le directeur général de toute atteinte aux mesures de sécurité dès la découverte d'une telle situation. Ceci inclut aussi le vol ou la perte d'appareils électroniques personnels qui auraient été utilisés pour la lecture de courriel de la Mutuelle par exemple. Dans une telle situation, l'usager se doit de faire changer son mot passe immédiatement.

Le défaut d'un utilisateur de se conformer à cette Politique pourra entraîner des sanctions disciplinaires.

Fournisseurs de services informatiques

Tout fournisseur de services informatiques doit fournir un rapport de sécurité détaillé.

SECTION 5 – PROCÉDURES

Procédure pour une demande d'accès

La demande d'accès doit être faite par écrit par une personne justifiant son identité. La demande doit être suffisamment précise pour identifier le requérant, ainsi que les renseignements auxquels il veut avoir accès.

La demande doit être adressée à la *Personne responsable de l'accès aux renseignements personnels et de leur protection*. L'accès aux renseignements personnels contenus dans un dossier est gratuit sous réserve des frais raisonnables de transcription, de reproduction ou de transmission que la Mutuelle peut exiger. La Mutuelle informera le requérant de ces frais avant la communication et le requérant devra les acquitter à l'avance.

Procédure pour une demande de rectification

Toute personne peut faire corriger à son dossier les renseignements personnels inexacts, incomplets ou équivoques et faire supprimer les renseignements périmés ou non justifiés par l'objet du dossier. La demande doit être faite par écrit à la Personne responsable.

Seuls les renseignements factuels et objectifs contenus au dossier peuvent faire l'objet d'une demande de rectification ou de suppression. La personne concernée peut cependant formuler des observations et

exiger qu'elles soient versées au dossier à l'égard des opinions, jugements ou commentaires contenus à son dossier.

La rectification doit être notifiée sans délai à toute personne qui a reçu les renseignements inexacts, périmés ou non justifiés dès que l'erreur est connue.

Afin de permettre aux membres de communiquer avec la Mutuelle s'ils souhaitent apporter des changements à leurs renseignements personnels (modification, rectification ou suppression), les coordonnées complètes de la Mutuelle ont été ajoutées sur le site Web dans la section Modification, rectification ou suppression des renseignements personnels de la Politique de protection des renseignements personnels.

Réponse à une demande d'accès ou de rectification au dossier

La *Personne responsable de l'accès aux renseignements personnels et de leur protection* pourra contacter le requérant afin de vérifier son identité et la détention des autorisations nécessaires.

Un accusé de réception sera transmis au requérant dans lequel sera indiquée la date de réception de la demande, ainsi que le délai dont la Mutuelle bénéficie pour y répondre.

Lorsque la demande n'est pas suffisamment précise ou lorsque le requérant le requiert, la Personne responsable de l'accès doit prêter assistance au requérant pour identifier le document susceptible de contenir les renseignements recherchés.

Une réponse écrite doit être transmise dans les trente (30) jours de la réception de la demande d'accès ou de rectification de dossier. À défaut de réponse, la Mutuelle est réputée avoir refusé d'y acquiescer.

Le refus de faire suite à la demande du requérant doit être notifié par écrit et les motifs sur lesquels ils sont fondés doivent y être indiqués. Ce refus doit de plus informer le requérant de ses recours en révision.

Demande d'examen de mésentente

Le requérant peut, dans les trente (30) jours de la date de la décision ou de l'expiration du délai dont bénéficiait la Mutuelle pour répondre à la demande, s'adresser à la Commission d'accès à l'information afin de soumettre une demande d'examen de mésentente relative à l'application d'une disposition législative portant sur l'accès ou la rectification d'un renseignement personnel.

Destruction des documents renfermant des renseignements personnels

Lorsque la conservation d'un renseignement personnel n'est plus nécessaire en fonction de l'objet pour lequel il a été recueilli, la Mutuelle assure sa destruction d'une manière qui protège le caractère confidentiel du renseignement et son importance.

Procédure en cas d'atteinte aux mesures de sécurité, de la perte ou d'un vol de renseignements personnels

En cas d'atteinte aux mesures de sécurité, de la perte ou d'un vol de renseignements personnels, la Mutuelle applique le protocole suivant :

ÉTAPE 1 : ÉVALUATION PRÉLIMINAIRE DE LA SITUATION

1. Définir sommairement le contexte de la perte ou du vol de renseignements personnels :
    a. Identifier les renseignements personnels touchés ainsi que leur support;
    b. Identifier les personnes, leur nombre ainsi que le groupe de personnes (clients, employés, etc.) touchées;
    c. Établir le contexte des événements (date, heure, lieu, etc.);
    d. Identifier, si possible, les circonstances entourant la perte (cause, personnes susceptibles d'être impliquées dans l'incident, etc.);
    e. Répertorier les mesures de sécurité physiques et informatiques en place lors de l'incident.
2. Désigner une personne ou une équipe responsable de la gestion de la situation.
3. Informer les intervenants concernés à l'interne :
    a. Dirigeants de l'organisme ou de l'entreprise;
    b. Responsable de l'unité administrative concernée;
    c. Responsable de la protection des renseignements personnels;
    d. Conseiller juridique;
    e. Direction des communications (gestion des médias et des appels de la clientèle).
4. Informer les autorités externes concernées qui doivent être avisées de l'incident immédiatement:
    a. Service de police (si les circonstances laissent croire à la possibilité d'un crime);
    b. Commission d'accès à l'information.

ÉTAPE 2 : LIMITER L'ATTEINTE À LA VIE PRIVÉE

La Mutuelle doit prendre sans tarder des mesures adéquates pour limiter les conséquences pour les personnes concernées d'une possibilité d'utilisation malveillante de leurs renseignements personnels, de l'usurpation ou du vol de leur identité :

1. Prendre des mesures afin de limiter immédiatement les conséquences d'une perte ou d'un vol de renseignements personnels en s'assurant de mettre fin à la pratique non conforme le cas échéant;
2. Récupérer les dossiers physiques ou numériques, selon le cas;
3. Révoquer ou modifier les mots de passe ou les codes d'accès informatiques;
4. Contrôler les lacunes dans les systèmes de sécurité.

ÉTAPE 3 : ÉVALUER LES RISQUES

1. Compléter une évaluation préliminaire des risques, en considérant la sensibilité des renseignements personnels en cause, tenant compte de leur nature, leur quantité, la possibilité de les combiner avec d'autres renseignements, les personnes concernées, etc.;
2. Déterminer le contexte de l'incident incluant :

a. la cause (ex. le caractère délibéré ou non de la perte ou du vol de renseignements personnels, l'erreur humaine, une faille informatique, etc.);

b. les auteurs connus ou probables des renseignements personnels perdus ou subtilisés (ex. organisation criminelle, public en général, etc.);

c. l'étendue de la situation (nombre de personnes touchées et secteurs touchés);

d. le caractère systémique ou non de la disparition des renseignements personnels (particulièrement lorsque la perte n'est pas générée directement par une intervention humaine);

e. une évaluation de la probabilité qu'un événement similaire se reproduise.

3. 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.);
4. Évaluer le caractère réversible ou non de la situation, dont la possibilité de récupérer les renseignements personnels;
5. Évaluer si les mesures immédiates prises étaient adéquates pour limiter l'atteinte et les compléter si nécessaire;
6. Déterminer les préjudices potentiels, notamment en évaluant les possibilités d'utilisation future des renseignements personnels par des personnes malveillantes, notamment pour le vol d'identité;
7. Déterminer les priorités et identifier les actions à prendre à partir des résultats de l'évaluation de ces risques.

ÉTAPE 4 : AVISER LES ORGANISATIONS ET PERSONNES CONCERNÉES

1. Déterminer qui doit être mis au courant de la perte ou du vol de renseignements personnels en fonction de l'évaluation des risques :

    a. 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;

    b. Personnes concernées : Si la perte ou le vol de renseignements personnels présente un risque de préjudice pour les personnes concernées, celles-ci devraient en être avisées sans tarder. Il ne s'agit pas d'alarmer, mais de prévenir afin de leur permettre de prendre les mesures pertinentes pour protéger leurs renseignements personnels;

AVIS AUX PERSONNES CONCERNÉES PAR UNE PERTE OU UN VOL DE LEURS RENSEIGNEMENTS PERSONNELS :

Selon les circonstances, il pourrait s'avérer nécessaire d'aviser les personnes victimes de la perte ou du vol de leurs renseignements personnels.

Cet avis pourrait inclure certains des éléments suivants:

- Le contexte de l'incident et le moment où il s'est produit ainsi qu'une description de la nature des renseignements personnels touchés ou potentiellement touchés, sans dévoiler de renseignements personnels spécifiques;
- Une description sommaire des mesures prises afin de limiter ou de prévenir tout préjudice, ainsi que la liste des personnes qui ont été informées de la situation (Service de police, Commission d'accès à l'information, etc.);
- Les actions prises par les organismes et les entreprises pour aider les personnes concernées (Service d'aide et d'information, Abonnement alerte crédit, etc.);
- Les mesures que les personnes concernées peuvent prendre afin de réduire les risques de préjudice ou pour mieux se protéger (référence au document « Le vol d'identité » disponible à la Commission d'accès à l'information);
- Les autres documents d'information générale conçus pour aider les personnes à se prémunir contre le vol d'identité;
- Les coordonnées d'un interlocuteur de l'organisation qui peut répondre aux questions et à qui il est possible d'effectuer tout signalement;

Les principales mesures qui seront prises pour éviter que la situation ne se reproduise (changement de pratique ou de processus, la formation du personnel, la révision ou l'élaboration de politiques, une vérification, un suivi périodique, etc.).

c. Commission 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 solution;

d. 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).

2. Désigner les personnes responsables d'aviser les intervenants externes identifiés précédemment ainsi que le moment et le moyen (lettre, courriel, téléphone);
3. 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.

ÉTAPE 5 : ÉVALUATION APPROFONDIE DE LA SITUATION ET PRÉVENTION

1. Approfondir l'analyse des circonstances de la perte ou du vol des renseignements personnels et effectuer une description chronologique des événements et des actions prises face à cet incident, incluant les dates et les intervenants concernés;
2. Répertorier et examiner 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;

3. Vérifier si ces normes, politiques ou directives internes ont été suivies par les personnes impliquées, identifier les raisons pour lesquelles elles n'ont pas été suivies, le cas échéant;
4. S'il s'agit d'une erreur de procédure ou d'une défaillance opérationnelle, les consigner au dossier de sécurité et adapter les processus pour éviter qu'un tel incident ne survienne à nouveau;
5. Évaluer la nécessité d'élaborer une politique en matière de traitement d'une perte ou d'un vol de renseignements personnels au sein de l'organisme ou de l'entreprise;
6. Formuler les recommandations relatives aux solutions à moyen et long terme et aux stratégies de prévention;
7. S'assurer de la réelle nécessité, pour l'organisme ou l'entreprise, de la collecte des renseignements personnels concernés;
8. Prévoir le suivi devant être accordé.

ÉTAPE 6 : SUIVI

Il est important d'effectuer le suivi :

- du processus de traitement qui doit être appliqué lors d'une perte ou d'un vol de renseignements personnels et des résultats obtenus afin de l'améliorer, s'il y a lieu;
- des mesures de sécurité requises à la suite de l'incident et de leur performance;
- de la communication de l'information pertinente à la Commission d'accès à l'information et au service de police impliqué, le cas échéant.

SECTION 6 - DISPOSITIONS FINALES

La présente Politique remplace toute version antérieure ou tout document antérieur au même effet.

La présente politique doit être révisée tous les trois (3) ans, ou au besoin, lors de modifications législatives.

Elle entre en vigueur dès son adoption par le conseil d'administration.