POLITIQUE SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

MUTUELLE D'ASSURANCE EN ÉGLISE
AGENCE EN ASSURANCE DE DOMMAGES

ADOPTÉE PAR : Conseil d'administration Résolution : 2023.04.12-5

Remplace la version antérieure : ca2019.12.12-2

MISE EN VIGUEUR : 12 avril 2023

TABLE DES MATIERES

1. PRÉAMBULE

Comme institution financière, la Mutuelle est tenue de respecter plusieurs obligations relatives à la protection et à la conservation de l'ensemble de l'information qu'elle détient. Plus particulièrement, à l'égard des renseignements personnels qu'elle détient dans le cadre de ses activités, la Mutuelle est assujettie à la Loi sur la protection des renseignements personnels dans le secteur privé (RLRQ c. P-39.1) (la « LPRP »).

La Mutuelle, comme la plupart des entreprises, conserve les renseignements en format numérique seulement. Conséquemment, la gestion de la sécurité des technologies de l'information est intimement liée à la protection des renseignements personnels.

2. DOCUMENTS RELIÉS

- Loi sur la protection des renseignements personnels dans le secteur privé
- Loi sur les assureurs
- Loi sur la distribution des produits et services financiers
- Règlement sur la tenue et la conservation des livres et registres
- Code civil du Québec
- Code d'éthique et de déontologie
- Règlement intérieur

- Politique de gouvernance
- Politique sur la gestion intégrée des risques
- Politique sur la prévention de la fraude et du risque de détournement
- Politique de gestion des contrats d'impartition
- Guide de l'employé

3. OBJECTIFS ET PORTÉE

La présente Politique vise à doter la Mutuelle d'un encadrement global afin d'assurer la protection des renseignements personnels qu'elle détient et à déterminer la procédure en suivre en cas de faille de sécurité.

Elle s'applique à toute information personnelle ainsi qu'à toute personne œuvrant pour la Mutuelle y compris les administrateurs, fournisseurs externes et les consultants et s'applique en tout temps.

De plus, la présente politique décrit spécifiquement le traitement des renseignements personnels et le protocole à suivre en cas de perte de ceux-ci.

L'objectif principal de cette politique est de communiquer la détermination et l'engagement de la Mutuelle à gérer avec efficacité et efficience les risques liés à la protection des renseignements personnels. Plus précisément, elle a pour but :

- D'assurer le respect de la vie privée des individus, notamment la confidentialité des renseignements à caractère nominatif relatifs aux membres sociétaires et leurs représentants, de même qu'aux réclamants et au personnel de la Mutuelle ;
- De renforcer la responsabilité collective et individuelle en diffusant l'information sur les principes directeurs et les bonnes pratiques en matière de gestion et de protection des renseignements personnels ;
- D'assurer le respect des lois et autres directives qui encadrent la protection des renseignements personnels par la Mutuelle.

4. DÉFINITIONS

4.1. 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.

4.2. Incident de confidentialité

L'une ou l'autre des situations suivantes :

- l'accès non autorisé par la loi à un renseignement personnel ;
- l'utilisation non autorisée par la loi d'un renseignement personnel ;
- la communication non autorisée par la loi d'un renseignement personnel ;

- la perte d'un renseignement personnel ou toute autre atteinte à la protection d'un tel renseignement[1].

5. ENGAGEMENT GÉNÉRAL

La Mutuelle s'engage à protéger les renseignements personnels qu'elle détient, à les détruire de façon appropriée selon les règles de conservation et de destructions des dossiers et à agir conformément aux articles 35 à 41 du Code civil du Québec et aux dispositions de la Loi sur la protection des renseignements personnels dans le secteur privé[2] (LPRP).

Pour ce faire, elle 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 autorisées.

6. MESURES DE PROTECTION

La Mutuelle met en place de façon continue différentes mesures afin de s'assurer de la protection des renseignements personnels[3].

Le processus de sélection des employés comprend les vérifications de probité. De plus, tous les employés doivent signer un engagement de confidentialité et s'engager à respecter le Code d'éthique et de déontologie de la Mutuelle au moment de leur embauche et périodiquement. Il en est de même pour les administrateurs.

La sélection des fournisseurs est rigoureuse et la bonne réputation est un critère important. Tout fournisseur ou consultant doit signer une entente de confidentialité, selon le cas, avant d'avoir accès à des renseignements personnels détenus par la Mutuelle.

Les mesures de sécurité appliquées par la Mutuelle sont principalement celles-ci :

- Les documents papier contenant des renseignements personnels sont toujours conservés sous clé et les locaux de la Mutuelle sont sécurisés. Il en est de même pour tout disque dur, clé USB ou autre contenant de telles informations.
- Tous les dossiers informatiques de la Mutuelle se trouvent sur les serveurs de l'hébergeur. Celui-ci déploie des moyens informatiques et physiques contre les intrusions et l'accès aux données.
- Les ordinateurs portables ou ordinateurs personnels utilisés dans le cadre du travail ne doivent contenir aucun renseignement personnel visé par la présente politique.
- 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,

[1] LPRP, art. 3.6 et 10 à 12
[2] Loi sur la protection des renseignements personnels dans le secteur privé (RLRQ P-39.1)
[3] LPRP, art. 3.2

les informations doivent être détruites du portable dès le retour dans l'environnement informatique de la Mutuelle.

- Les serveurs de la Mutuelle sont protégés des accès par différentes protections. D'abord, les employés de la Mutuelle doivent avoir un code d'usager valide ainsi que deux facteurs d'identifications.
- Les employés n'ont accès qu'aux répertoires et aux différentes applications ou différents modules qui sont nécessaires à 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.

7. PERSONNE RESPONSABLE DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

Le directeur général est désigné d'office par la LPRP à titre de responsable de la protection des renseignements personnels[4]. Comme la Loi le permet, il délègue cette au secrétaire de la Mutuelle.

Le titre et les coordonnées de la personne désignées sont publiés sur le site internet de la Mutuelle.

8. CONSTITUTION DES DOSSIERS

La Mutuelle ne recueille que les renseignements personnels qui sont nécessaires aux fins de l'objet de la constitution du dossier[5]. 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 cueillette d'information doit être mentionné à la personne concernée et être inscrit au dossier, et ce, avant ou au moment de la collection des renseignements personnels[6]. Lorsque les renseignements sont demandés verbalement, l'employé faisant la collecte d'information doit expliquer la raison de cette collecte. En cas de formulaire, celui-ci doit indiquer dans quel but les renseignements personnels sont collectés. Si la Mutuelle venait à changer le but de la collecte initiale des renseignements, celle-ci doit obtenir le consentement de la personne concernée préalablement.

La personne concernée 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[7].

[4] LPRP, art. 3.1
[5] Ligne directrice sur les critères de probité et de compétence, Politique d'encadrement des administrateurs et dirigeants et Code d'éthique et de déontologie
[6] LPRP, art 4 et 5
[7] LPRP, art. 8.

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

- **Dossier d'employé :** pour traiter de différentes obligations pour chaque employé, 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 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, tel que requis par les différentes législations.
- **Dossier d'administrateur :** pour traiter de différentes obligations relatives à son poste tel 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, tel que requis par les différentes législations.
- **Dossier des membres :** L'information nécessaire dans la gestion de son dossier d'assurance et du respect des différentes législations à laquelle la Mutuelle est assujettie.
- **Dossiers d'indemnisation :** lorsque 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 :** 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 pour permettre à la Mutuelle de vérifier ses références.

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

La Mutuelle recueille les renseignements personnels auprès de la personne concernée après s'être assurée de son consentement libre et éclairé. Elle peut les recueillir auprès d'un tiers, avec le consentement de la personne concernée à moins qu'une législation applicable autorise la cueillette auprès d'autrui.

La Mutuelle conserve le dossier d'un employé ou d'un administrateur de la Mutuelle tant qu'il est en fonction et pendant une période raisonnable à la suite de son départ, en respect avec les exigences législatives.

Le dossier d'un membre est conservé tant qu'il est actif et pendant une période raisonnable à la suite de son départ, compte tenu des dispositions législatives à cet égard[8]. 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

[8] Règlement sur la tenue et la conservation des livres et registres et législation fiscale, entre autres

exemple, les cas d'abus). Les dossiers de réclamations sont conservés tant que la réclamation est active et pendant une période raisonnable par la suite en respect avec les exigences législatives.

9. DÉTENTION ET UTILISATION DES RENSEIGNEMENTS PERSONNELS

Le caractère confidentiel des renseignements personnels doit être assuré, et ce, peu importe le support utilisé. Les documents papier sont conservés dans des endroits sécurisés. Les documents électroniques sont conservés dans des répertoires avec accès restreints et font l'objet de différentes mesures de sécurité informatique additionnelles appropriées.

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.

Tout projet d'acquisition, de fusion, de développement et de refonte de système d'information ou de prestation électronique de services impliquant la collecte, l'utilisation, la communication, la conservation ou la destruction de renseignements personnels doit faire l'objet d'une évaluation de protection des facteurs relatifs à la vie privée à l'aide de la personne responsable de la protection des renseignements personnels[9].

10. 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 de la protection des renseignements personnels* 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.

11. 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

[9] LPRP, art. 3.3

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 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.

12. 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 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.

13. REGISTRE DES INCIDENTS DE CONFIDENTIALITÉ

La Mutuelle conserve un registre de tous les Incidents de confidentialité[10]. Ce registre fait état de la date et de la nature de l'incident, la portée des atteintes, les actions à l'égard des personnes dont les renseignements personnels ont potentiellement été compromis et les mesures prises pour remédier à l'incident et éviter que de nouveaux incidents de même nature ne se reproduisent[11].

[10] LPRP, art. 3.8
[11] LPRP, art. 3.5

Les incidents de confidentialité peuvent résulter de :

- 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.

14. OBLIGATION D'INFORMER LES AUTORITÉS

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 sérieux »[12]. Elle peut également aviser toute personne ou tout organisme susceptibles de diminuer ce risque, en ne lui communiquant que les renseignements personnels nécessaires à cette fin sans le consentement de la personne concernée. Dans ce dernier cas, le responsable de la protection des renseignements personnels doit enregistrer la communication.

Un « préjudice sérieux » 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'occasions 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.

15. OBLIGATION D'INFORMER LES PERSONNES CONCERNÉES

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.

Cependant, une personne dont un renseignement personnel est concerné par l'incident n'a pas à être avisée tant que cela serait susceptible d'entraver une enquête faite par une personne ou par un organisme qui, en vertu de la loi, est chargée de prévenir, détecter ou réprimer le crime ou les infractions aux lois.

[12] LPRP, art. 3.5

16. PROTOCOLE EN CAS D'INCIDENT DE CONFIDENTIALITÉ

En cas d'incident de confidentialité, de la perte ou d'un vol de renseignements personnels, la Mutuelle applique le protocole suivant :

16.1. 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 :

    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 si l'incident correspond aux critères législatifs
    c. Autorité des marchés financiers, selon le cas.

16.2. 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.

16.3. 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.

16.4. 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[13] :

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 l'incident présente un risque qu'un préjudice sérieux soit causé ;
d. Autorité des marchés financiers ;
e. 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).

[13] Basé sur l'exemple *Avis aux personnes touchées – Lettre type* du secrétariat du Conseil du trésor du Canada

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.

16.5. 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 procédure spécifique en matière de traitement d'une perte ou d'un vol de renseignements personnels au sein de la Mutuelle ;

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.

16.6. 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.

17. PROCÉDURES

17.1. 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.

17.2. 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.

17.3. 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 demande, 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.

17.4. 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.

18. PLAINTE POUR NON-RESPECT DES OBLIGATIONS DE LA MUTUELLE

18.1. Réception d'une plainte

La personne qui désire porter plainte doit le faire par écrit à l'adresse suivante :

Me Colette St-Martin
Responsable de la protection des renseignements personnels
Compagnie Mutuelle d'assurance en Église
1155, rue Metcalfe, suite 1562
Montréal (Québec) H3B 2V6

Téléphone : 514 395-4969 poste 2231
Télécopieur : 514 861-8921

Tout employé, mandataire ou administrateur qui est saisi d'une plainte doit la référer dès réception à la personne responsable de la protection des renseignements personnels.

La personne désignée accuse réception de la plainte par écrit dans les cinq jours ouvrables suivant sa réception.

L'accusé de réception doit contenir au moins les éléments d'information suivants :

- Une description de la plainte ou de la demande reçue précisant le préjudice subi ou potentiel, le reproche fait à la Mutuelle et la mesure corrective demandée ;
- Le nom et les coordonnées de la personne responsable de la protection des renseignements personnels ;
- Dans le cas d'une information incomplète, un avis mentionnant la nécessité de transmettre de l'information complémentaire dans les quinze (15) jours, à défaut de quoi la plainte sera réputée avoir fait l'objet d'un désistement ;
- Une copie de la Politique ;
- Un avis informant le plaignant :

- De son droit de demander en tout temps le transfert de son dossier à la Commission de protection des renseignements personnels, s'il est insatisfait de la réponse ou du traitement de sa plainte ;

- Que la Commission peut offrir des services de règlement des différends, si les parties y consentent, rappelant au plaignant que la médiation est un processus de résolution à l'amiable d'un conflit dans lequel une tierce personne (le médiateur) intervient auprès des parties pour les aider à parvenir à un accord ;

- Que le dépôt d'une plainte à la Commission n'interrompt pas la prescription relative aux poursuites devant les tribunaux civils.

18.2. Création et maintien du dossier de la plainte

La réception d'une plainte entraîne la constitution d'un dossier de plainte. Les dossiers de plainte sont conservés dans un répertoire sécurisé prévu à cet effet.

Le dossier de plainte doit comprendre les documents suivants :

- La plainte écrite du plaignant ou, si la plainte est verbale, le document qui la constate ;
- Le résultat du processus du traitement de la plainte (l'analyse et les documents de soutien) ;
- Une copie de la réponse finale et motivée transmise par écrit au plaignant.

18.3. Enquête et réponse

La personne désignée à cet effet par le secrétaire corporatif est tenue de procéder à une enquête à la suite de la réception d'une plainte. Le secrétaire corporatif peut requérir que l'enquête soit conduite par les services juridiques.

Le traitement de la plainte doit être effectué dans un délai raisonnable, soit dans les quarante-cinq (45) jours suivant la réception de tous les renseignements nécessaires à son étude.

À l'issue de l'enquête, la personne responsable transmet au plaignant une réponse finale écrite et motivée.

Lorsque les préoccupations soulevées par le plaignant ou certains aspects de celle-ci ne relèvent pas de la présente politique ou relèvent d'une autre instance au sein de la Mutuelle, la réponse peut comporter une proposition au plaignant afin que ses préoccupations lui soient transférées.

18.4. Transmission du dossier à la Commission d'accès à l'information

Lorsque le plaignant n'est pas satisfait de l'examen de sa plainte par la Mutuelle ou du résultat de cet examen, il peut demander de transférer son dossier de plainte à la Commission d'accès à l'information. Le dossier doit être transféré dans les trente (30) jours du refus de la demande ou de l'expiration du délai pour y répondre à moins que la Commission, pour un motif raisonnable, ne la relève du défaut de respecter ce délai.

La Mutuelle peut demander à la Commission de l'autoriser à ne pas tenir compte de demandes manifestement abusives par leur nombre, leur caractère répétitif ou systématique ou de demandes qui, de l'avis de la Commission, ne sont pas conformes à l'objet de la présente loi. Elle peut aussi demander à la Commission de circonscrire la demande du requérant ou de prolonger le délai dans lequel elle doit répondre.

18.5. Création et maintien d'un registre

Un registre des plaintes est établi aux fins de l'application de la Politique. Sa mise à jour est sous la responsabilité du secrétaire corporatif.

Toute plainte correspondant à la définition de cette expression doit, peu importe le niveau d'intervention impliqué dans le traitement de cette plainte, faire l'objet d'une inscription au registre, notamment toute plainte formulée par écrit.

19. IMPUTABILITÉS, RÔLES ET RESPONSABILITÉS

19.1. Conseil d'administration

Le conseil d'administration a les responsabilités suivantes :

- Promouvoir une culture de protection des renseignements personnels ;
- Adopter la présente politique.

19.2. Direction générale

Le directeur général a les responsabilités suivantes :

- Mettre en place des mesures de protection des renseignements personnels ;
- Assurer l'application constante et rigoureuse de la présente Politique ;
- 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 ;
- Assurer la publication des renseignements de cette politique sur le site Web de la Mutuelle ainsi que les éléments requis par les lois applicables ;
- Assurer la formation du personnel et la transmission de l'information relative à la présente politique et aux pratiques de la Mutuelle.

19.3. 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 courriels 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 courriels 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.

19.4. Fournisseurs de services informatiques

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

20. 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.