Politique de confidentialité et de protection des renseignements personnels

Approuvé par le conseil d'administration le 18 avril 2024

Table des matières

1. RÈGLES D'INTERPRÉTATION

La présente politique de confidentialité et de protection des renseignements personnels s'inspire des lois de la province de Québec et son interprétation est soumise à ces mêmes lois.

2. OBJETS DE LA POLITIQUE

2.1. Objectifs de la politique et valeurs de gestion

La présente politique traite de la gestion et de la protection des informations jugées confidentielles à l'intérieur du Centre de soir Denise-Massé. Elle traite notamment des renseignements concernant :

- Ses donateurs et leurs données;
- Des informations liées aux activités de l'organisme;
- Des informations liées à la clientèle;
- Des informations concernant les membres du conseil d'administration;
- Des informations concernant les membres du personnel;
- Des informations liées aux stagiaires et aux bénévoles.

Elle s'applique aux relations entre toutes personnes : hommes ou femmes, administrateurs·trices, donateurs·trices, membres du personnel, membre de la clientèle, bénévoles, stagiaires, partenaires ainsi qu'à toutes les autres personnes travaillantes ou étant présentes dans les différents locaux du Centre de soir Denise-Massé.

Elle poursuit les objectifs suivants :

- Assurer le respect de la vie privée des personnes et la sécurité des informations personnelles;
- Se donner des balises concernant les échanges d'informations tant à l'intérieur qu'à l'extérieur des locaux de l'organisme.

2.2. Révision de la politique

La politique de confidentialité et de protection des renseignements personnels sera mise à jour par le conseil d'administration tous les trois (3) ans.

2.3. Obligation de confidentialité

Lors de l'embauche, la direction remet une copie de la politique de confidentialité et de protection des renseignements personnels à la personne salariée. L'employé·e est tenu·e de signer la présente politique ainsi que la déclaration relative à la confidentialité avant d'exercer sa fonction ou d'exécuter ses mandats auprès du Centre de soir Denise-Massé (Annexe 1).

L'obligation de confidentialité s'applique à la durée de la relation d'un·e employé·e, stagiaire, bénévole et/ou membre du conseil d'administration avec le Centre de soir Denise-Massé et survit à la fin de cette relation.

2.4. Responsable de l'application des normes de protection des renseignements personnels

La personne occupant le poste de coordination est la personne responsable d'assurer la protection des renseignements personnels. Elle assure la tenue du registre des incidents de confidentialité.

2.5. Modalité d'application

Toutes les dispositions de cette politique s'appliquent à l'ensemble du personnel du Centre de soir Denise-Massé ainsi qu'aux stagiaires, bénévoles et membres du conseil d'administration.

Si un·e administrateur·trice, employé·e, stagiaire ou bénévole a divulgué une information confidentielle, l'autorité compétente lui impose une sanction qui peut aller de la réprimande à l'exclusion.

2.6. Définitions

CAI : Commission d'accès à l'information du Québec

Confidentialité : Le fait de limiter ou d'interdire à d'autres personnes l'accès à des informations privées obtenues dans l'exercice de ses fonctions.

Confidentialité d'équipe : Le fait d'échanger avec l'ensemble du personnel du CSDM certaines informations à propos d'un·e ou des participant·e·s pour une meilleure intervention.

CSDM : Centre de soir Denise-Massé

Discrétion : L'aptitude à garder secrètes les confidences et les informations privées obtenues en dehors du cadre de travail afin de préserver le respect, l'amitié et la confiance.

Ensemble du personnel : Toute personne qui travaille pour le CSDM (employé·e) moyennant rémunération ou non, incluant la coordination, la direction, les stagiaires, les bénévoles et les membres du conseil d'administration.

Formulaire de signalement : Formulaire mis à la disposition de toustes afin d'informer la personne responsable des renseignements personnels d'un incident de confidentialité.

Incident de confidentialité : Tout accès non autorisé par la loi à un renseignement personnel, à son utilisation ou à sa communication, de même que sa perte ou toute autre forme d'atteinte à sa protection.

Participant·e : Toute personne qui fréquente le Centre de soir Denise-Massé.

Publication : Toute publication produite par le CSDM ou à laquelle il contribue, sous quelque forme que ce soit (verbal, écrit, audio, vidéo, informatisé ou autre).

Registre des incidents de confidentialité : L'ensemble des renseignements consignés sur des incidents déclarés et concernant les circonstances de l'incident, le nombre de personnes visées, l'évaluation de la gravité du risque de préjudice et les mesures prises en réaction à l'incident. Les dates pertinentes y figurent aussi : survenance de l'incident, détection par l'organisation, transmission des avis (s'il y a lieu), etc.

Risque sérieux de préjudices : Le risque évalué à la suite d'un incident de confidentialité qui pourrait porter préjudice aux personnes concernées. Ce risque est analysé par la personne responsable des renseignements personnels. Pour tout incident de confidentialité, la personne responsable évalue la gravité du risque de préjudice pour les personnes concernées en estimant « la sensibilité des renseignements concernés », « les conséquences appréhendées de leur utilisation » et « la probabilité qu'ils soient utilisés à des fins préjudiciables ».

Renseignements confidentiels : Tout renseignement fourni ou communiqué au CSDM sous quelque support que ce soit (verbal, écrit, audio, vidéo, informatisé ou autre) qui concerne un·e participant·e,

un·e employé·e ou un·e administrateur·trice et qui peut être utilisé pour l'identifier, y compris : son nom, son numéro de téléphone, son adresse, son courriel, son numéro d'assurance sociale, une pièce d'identité, le fait qu'il ou elle ait été ou soit un·e participant·e ou un·e participant·e potentiel·le, son genre et toute information concernant sa santé. Pour plus de certitude :

- Les renseignements qui ne permettent pas d'identifier un individu dans le cadre d'un témoignage ne sont pas des renseignements confidentiels ;

- Les données statistiques ne sont pas des renseignements confidentiels puisqu'elles ne permettent pas d'identifier un individu ;

- Les photographies ou enregistrements qui ne permettent pas d'identifier un individu ne constituent pas un renseignement confidentiel relatif à cet individu.

Service ou activité : Tout service que le CSDM rend à un individu à la demande de celui-ci, ou toute activité à laquelle il participe.

3. COLLECTE ET USAGE DES RENSEIGNEMENTS CONFIDENTIELS

3.1. Modalités de collecte des renseignements personnels

Le CSDM peut seulement recueillir les renseignements confidentiels qui sont nécessaires aux fins du dossier et peut utiliser les renseignements confidentiels seulement à ces fins.

Les renseignements confidentiels peuvent seulement être recueillis auprès de la personne concernée, à moins que celle-ci consente à ce que la cueillette soit réalisée auprès d'autrui ou que la loi l'autorise.

3.2. Dossier de l'ensemble du personnel

Le CSDM peut, au besoin, constituer un ou des dossiers contenant des renseignements confidentiels concernant les employé·e·s, les stagiaires, les bénévoles et les administrateurs·trices. La constitution de tels dossiers a pour objet de :

- Maintenir les coordonnées à jour ;
- Documenter des situations de travail ou de bénévolat ;
- Permettre, dans le cas des employé·e·s rémunéré·e·s, la réalisation des tâches administratives requises ou permises par la loi (impôt sur le revenu, assurances collectives, etc.).

3.3. Dossiers des participant·e·s

Le CSDM peut, au besoin, constituer un ou des dossiers contenant des renseignements confidentiels concernant les participant·e·s. La constitution de tels dossiers a pour objet de permettre au CSDM de réaliser une activité ou de fournir un service.

3.4. Photographies et enregistrements

Toute personne a le choix d'accepter ou non d'être photographié ou d'être enregistré (audio/vidéo) lors des différentes activités du CSDM.

Les photographies ou enregistrements qui permettent d'identifier un individu comme employé·e du CSDM ne constituent pas un renseignement confidentiel relatif à cette personne.

3.5. Publication des photographies et enregistrements

Sous réserve de l'article 3.4, le CSDM doit avoir l'autorisation écrite des personnes concernées pour procéder à la publication de photo ou d'enregistrement où ils·elles apparaissent.

4. GESTION DES RENSEIGNEMENTS CONFIDENTIELS

La direction et la coordination sont autorisées à accéder à tout renseignement confidentiel que détient le CSDM. Les autres membres du personnel sont autorisé·e·s à accéder aux renseignements confidentiels dans la mesure où cet accès est nécessaire à la réalisation d'une tâche dans l'exercice de leurs fonctions.

Seule la personne responsable du dossier de suivi d'un·e participant·e pour les programmes PAAS-Action, les services TAC et les ateliers d'autogestion est autorisée à accéder aux renseignements confidentiels que le CSDM détient dans le cadre de cette activité ou de ce service. La direction générale et la coordination du CSDM peut toutefois y accéder dans la mesure où cela est nécessaire.

5. CONSERVATION DES RENSEIGNEMENTS PERSONNELS

5.1. Engagement du CSDM

Les membres du personnel ayant accès aux dossiers en vertu de l'article 4 s'obligent à :

- Déterminer les fins de la collecte, un intérêt sérieux et légitime doit motiver la constitution d'un dossier sur une personne ;

- Limiter la collecte de renseignements personnels aux renseignements nécessaires aux fins déterminées. En cas de doute, un renseignement personnel est réputé non nécessaire;

- Recueillir les renseignements personnels par des moyens légaux et légitimes. Sauf exception, la collecte doit se faire auprès de la personne concernée;

- Informer la personne concernée, avant de constituer un dossier :
  - De l'objet du dossier;
  - De l'utilisation qui sera faite des renseignements personnels;
  - Des catégories de personnes qui y auront accès au sein de l'entreprise;
  - De l'endroit où ils seront détenus;
  - De ses droits d'accès et de rectification.

- S'assurer que les renseignements confidentiels soient gardés à l'abri de tout dommage physique ou accès non autorisé ;

- S'assurer que tous les documents électroniques comportant des renseignements confidentiels, incluant ceux copiés sur un appareil de stockage portatif, soient cryptés et protégés par des mots de passe. Ces mots de passe doivent être modifiés deux fois par année, ainsi qu'à chaque fois que les personnes ayant accès aux dossiers concernés sont remplacées ;

- Garder les renseignements confidentiels en format papier dans des classeurs pouvant être verrouillés et s'assurer que les classeurs soient verrouillés en dehors des heures de bureau ou en l'absence de leurs responsables;

5.2. Propriété des documents

Les dossiers constitués en vertu de cette politique sont la propriété du CSDM.

6. DESTRUCTION DES RENSEIGNEMENTS CONFIDENTIELS

6.1. Durée de conservation des documents

Sous réserve de l'article 6.2, les renseignements confidentiels ne sont conservés que tant et aussi longtemps que l'objet pour lequel ils ont été recueillis n'a pas été accompli, à moins que l'individu concerné ait consenti à ce qu'il en soit autrement. Ces renseignements confidentiels sont ensuite détruits de façon à ce que les données y figurant ne puissent plus être reconstituées.

6.2. Durée de conservation des dossiers d'employé·e·s

Les dossiers concernant les membres du personnel sont conservés pour une période de dix (10) ans suite à la fin du lien d'emploi.

6.3. Durée de conservation des témoignages

Pour plus de certitude, les renseignements confidentiels concernant un individu ayant offert un témoignage, tels que son nom et ses coordonnées, sont détruits une fois le témoignage publié ou diffusé, à moins que l'individu ait préalablement consenti à ce que les renseignements confidentiels le concernant soient conservés pour permettre au CSDM de le recontacter dans le futur. Pour plus de certitude, chaque utilisation du témoignage d'une personne doit être approuvée par celle-ci.

7. DIVULGATION DES RENSEIGNEMENTS CONFIDENTIELS À UN TIERS

Autre que dans les situations où la loi le requiert et sous réserve des autres dispositions du présent article 7, les renseignements confidentiels ne peuvent être divulgués à un tiers qu'après l'obtention du consentement écrit, manifeste, libre et éclairé de la personne concernée. Un tel consentement ne peut être donné que pour une fin spécifique et pour la durée nécessaire à la réalisation de cette dernière.

7.1. Divulgation sans consentement

Les renseignements confidentiels peuvent être divulgués sans le consentement de la personne concernée si la vie ou la vie d'autrui, la santé ou la sécurité de celle-ci est gravement menacée. La divulgation doit alors être effectuée de la façon la moins préjudiciable pour la personne concernée.

7.2. Divulgation de défense

Tel que permis par la loi, le CSDM peut divulguer des renseignements confidentiels nécessaires à sa défense ou à celle de son personnel contre toute réclamation ou poursuite intentée contre le CSDM ou son personnel, par ou de la part d'un·e participant·e, d'un·e employé·e, ou de l'une de ses personnes héritières, exécutrices testamentaires, ayants droit ou cessionnaires, y compris toute réclamation émanant de l'assureur d'un·e participant·e ou d'un·e employé·e.

8. COMMUNICATION DE RENSEIGNEMENTS CONFIDENTIELS À LA PERSONNE CONCERNÉE

8.1. Accès aux renseignements confidentiels

Sous réserve de l'article 8.2, toute personne a le droit de connaître les renseignements confidentiels que le CSDM a reçus, recueillis et conserve à son sujet, d'avoir accès à de tels renseignements et de demander que des rectifications soient apportées à ceux-ci.

8.2. Limitation de l'accès aux renseignements confidentiels

Le CSDM doit restreindre l'accès aux renseignements confidentiels lorsque la loi le requiert ou lorsque la divulgation révélerait vraisemblablement des renseignements confidentiels au sujet d'un tiers.

8.3. Demande d'accès aux renseignements confidentiels

Les participant·e·s ou les membres du personnel désirant avoir accès aux renseignements confidentiels les concernant doivent en faire la demande par écrit et la transmettre à la direction du CSDM. Cette demande doit contenir les éléments suivants :

- La date de la demande ;

- La liste des informations désirées ;
- La raison de la demande d'accès ;
- La signature de la personne faisant la demande.

8.4. Délai de traitement

Une demande d'accès d'un·e participant·e ou d'un·e membre du personnel en lien avec les articles 8.1 et 8.3 doit être traitée dans un délai maximal de 30 jours.

8.5. Modalités d'accès aux renseignements confidentiels

L'accès aux renseignements confidentiels doit se faire lors d'une rencontre préalablement établie, en présence de la direction du CSDM pour les membres du personnel et les administrateurs·trices et en présence de la direction ou de la coordination et d'un membre du personnel pour les participant·e·s.

8.6. Recours en cas de refus

Comme prévu par la loi, la personne s'étant vu refuser l'accès ou la rectification des renseignements confidentiels la concernant peut déposer une plainte auprès de la CAI pour l'examen du désaccord dans les 30 jours du refus du CSDM d'accéder à sa demande ou de l'expiration du délai pour y répondre.

9. INCIDENTS DE CONFIDENTIALITÉ

9.1. Constat

Lorsqu'une personne constate un incident de confidentialité, elle doit informer avec diligence la personne responsable de la protection des renseignements confidentiels afin qu'il soit inscrit au Registre. La personne doit, pour ce faire, compléter un formulaire de signalement et l'acheminer ensuite à la personne responsable.

9.2. Formulaire de signalement (Annexe 2)

Doit être colligé dans le formulaire de signalement :

- Une description des renseignements personnels touchés par l'incident ou, si cette information est inconnue, les raisons pour lesquelles il est impossible de fournir une telle description ;
- Une brève description des circonstances de l'incident ;
- La date ou la période à laquelle a eu lieu l'incident (ou une approximation si cette information n'est pas connue) ;
- La date ou la période à laquelle l'organisation s'est aperçue de l'incident ;
- Le nombre de personnes concernées par l'incident (ou une approximation si cette information n'est pas connue).

9.3. Évaluation (Annexe 3)

La personne responsable de la protection des renseignements confidentiels juge si l'incident présente un « risque sérieux de préjudice ». Les renseignements ainsi que les mesures à prendre afin de diminuer le risque qu'un préjudice sérieux soit causé aux personnes concernées sont versés au Registre.

La personne responsable identifie les mesures raisonnables à mettre en place pour réduire le risque de préjudice et pour prévenir de nouveaux incidents.

9.4. Communication aux personnes concernées (Annexe 4)

Si l'incident de confidentialité signalé présente un risque sérieux de préjudice après évaluation, la personne responsable avise la CAI et les personnes concernées de tout incident à l'aide du formulaire approprié.

9.5. Registre des incidents de confidentialité

Tout incident de confidentialité constaté au sein du CSDM doit être inscrit au Registre. Celui-ci doit conserver les informations sur un incident de confidentialité pour une période de cinq (5) ans.

10. MANQUEMENT À L'OBLIGATION DE CONFIDENTIALITÉ

10.1. Principes

Un membre du personnel manque à son obligation de confidentialité lorsque cette personne :

- Communique des renseignements confidentiels à des individus n'étant pas autorisés à y avoir accès ;
- Discute de renseignements confidentiels à l'intérieur ou à l'extérieur du CSDM alors que des individus n'étant pas autorisés à y avoir accès sont susceptibles de les entendre ;
- Laisse des renseignements confidentiels sur papier ou support informatique à la vue dans un endroit où des individus n'étant pas autorisés à y avoir accès sont susceptibles de les voir ;
- Fait défaut de suivre les dispositions de cette politique.

10.2. Mesures

Advenant un manquement à l'obligation de confidentialité, des mesures disciplinaires appropriées, pouvant aller jusqu'à la résiliation du contrat de travail ou de toute autre relation avec le CSDM seront prises à l'égard de la partie contrevenante et des mesures correctives seront adoptées au besoin afin de prévenir qu'un tel scénario ne se reproduise.

11. RECOURS

11.1. Plaintes

S'il s'avère que les renseignements confidentiels d'une personne ont été utilisés de façon contraire à une disposition de cette politique, cette personne peut déposer une plainte auprès de la direction générale du CSDM ou auprès du conseil d'administration du CSDM si la plainte concerne la direction.

ANNEXE 1 : DÉCLARATION RELATIVE À LA CONFIDENTIALITÉ

L'engagement du CSDM et des membres du personnel :

- Assurer la sécurité et la confidentialité des renseignements obtenus;
- Mettre en place des mécanismes afin de protéger les informations confidentielles;
- Assurer le traitement confidentiel des plaintes;
- Recueillir seulement les données nécessaires ou utiles;
- Appliquer la politique de confidentialité dans le respect des valeurs du CSDM;
- Agir avec respect et transparence lors de l'application de cette politique et dans le respect des lois en vigueur.

Normes de discrétion

Toute personne qui, au sein du CSDM, a des échanges qui ne sont pas liés à l'exercice de ses fonctions doit agir avec discrétion. De ce fait, elle doit:

- Respecter la vie privée des personnes;
- Ne pas divulguer l'information confidentielle obtenue au sein du CSDM ou lors d'activités;
- Savoir garder les informations sensibles des personnes qui se confient;
- Agir selon les valeurs du CSDM.

Obligations du CSDM

Les membres du personnel du CSDM s'engage :

- À conserver ou transmettre de manière sécuritaire toutes informations confidentielles qu'ils détiennent dans le cadre de leur fonction.
- À remettre à la fin de leur mandat toutes informations, documents reliés aux renseignements personnels auxquels ils ont eu accès durant leur mandat.

Je, soussigné·e, déclare avoir pris connaissance de la déclaration relative à la confidentialité du Centre de soir Denise-Massé et à agir dans le respect de celle-ci dans le cadre de mes fonctions.

_____

Signature de la personne

Date de signature : _____

ANNEXE 2 : INCIDENT DE CONFIDENTIALITÉ : FORMULAIRE DE SIGNALEMENT

Comme prévu dans la Politique de confidentialité et de protection des renseignements personnels du Centre de soir Denise-Massé, vous devez remplir ce formulaire de signalement aussitôt que vous constatez un incident de confidentialité et le remettre à la personne responsable.

Les informations colligées seront versées au registre des incidents sur la confidentialité. À partir de ces informations, la personne responsable évaluera si l'incident présente « un risque de préjudice sérieux » pour les personnes concernées et remplira une déclaration à la Commission de l'accès à l'information, si nécessaire. Des mesures pour contrôler et prévenir le type d'incident déclaré seront ensuite déployées.

Un incident de confidentialité correspond à tout accès, utilisation ou communication non autorisés par la loi d'un renseignement personnel, de même qu'à la perte d'un renseignement personnel ou à toute autre atteinte à sa protection.

Par exemple, un incident de confidentialité pourrait se produire lorsque:

- Un membre du personnel consulte un renseignement personnel sans autorisation;
- Un membre du personnel communique des renseignements personnels au mauvais destinataire;
- L'organisation est victime d'une cyberattaque : hameçonnage, rançongiciel, etc.

Date et période de l'incident de confidentialité

Date de l'incident : _____

Date de la découverte de l'incident : _____

L'incident a eu lieu sur une période de : _____

Type d'incident de confidentialité (identifier avec un "x" le type d'incident) :

☐Accès non autorisé par la loi à un renseignement personnel

☐Utilisation non autorisée par la loi d'un renseignement personnel

☐Communication non autorisée par la loi d'un renseignement personnel

☐Perte d'un renseignement personnel ou toute autre atteinte à la protection d'un tel renseignement

Causes et circonstances de l'incident (identifier avec un "x" les causes ou circonstances :

☐Altération délibérée

☐Communication accidentelle

☐Communication délibérée sans autorisation

☐Consultation non autorisée

☐Cyberattaque (virus, logiciel espion, etc.)

☐Défaillance technique

☐Destruction accidentelle

☐Destruction volontaire sans autorisation

☐Divulgation accidentelle

☐Divulgation délibérée sans autorisation

☐Erreur humaine

☐Hameçonnage (phishing)

☐Ingénierie sociale (technique de manipulation pour obtenir des rens. pers.)

☐Perte d'accès aux renseignements

☐Perte de renseignements

☐Rançongiciel

☐Utilisation incompatible

☐Vol de renseignements

☐Autre, précisez :

_____

_____

_____

_____

Sur quel support les renseignements personnels étaient-ils conservés au moment de l'incident ?

☐Ordinateur de bureau

☐Dispositif amovible électronique

☐Papier

☐Clé USB

☐Serveur

☐CD

☐Bande sonore

☐Téléphone portable

☐Infonuagique (cloud)

☐Tablette

☐Vidéosurveillance

☐Ordinateur portable

☐Photo

☐Autre, précisez :

_____

_____

Personnes concernées par l'incident de confidentialité

Nombre de personnes concernées par l'incident : _____

Si possible, indiquez le nombre de personnes concernées par l'incident selon leur lien avec l'organisation :

_____

_____

Identification des renseignements personnels visés par l'incident de confidentialité (identifier avec un x pour chaque renseignement).

☐Nom

☐Prénom

☐Adresse du domicile

☐Date de naissance

☐Numéro de téléphone au domicile

☐Numéro du cellulaire

☐Adresse courriel personnelle

☐Numéro de permis de conduire

☐Numéro d'assurance sociale

☐Numéro d'assurance maladie

☐Numéro de passeport

☐Salaire Fonction / occupation

☐Renseignements sur des employés, ou bénéficiaires

☐Renseignements médicaux

☐Renseignements génétiques

☐Renseignements scolaires / académiques

☐Renseignements bancaires / numéro de compte / institution / placements / hypothèque

☐Numéro de carte de crédit

☐Numéro d'identification personnel (NIP)

☐Nom du détenteur

☐Code de sécurité à trois chiffres

☐Numéro de carte de débit

☐Numéro d'identification personnel (NIP)

☐Nom du détenteur

☐Autres renseignements personnels, précisez :

_____

_____

_____

_____

☐Impossible de fournir une description des renseignements personnels visés. Expliquez :

_____

_____

_____

_____

Personne déclarant l'incident : _____

Fonction : _____

Moyen de communication : _____

ANNEXE 3 : INCIDENT DE CONFIDENTIALITÉ : QUESTIONNAIRE D'ÉVALUATION DU « RISQUE SÉRIEUX DE PRÉJUDICE GRAVE »

Évaluer si l'incident présente un risque de préjudice sérieux [1]

Pour tout incident de confidentialité, l'organisation doit évaluer la gravité du risque de préjudice pour les personnes concernées. Pour ce faire, elle doit considérer, notamment :

- Quelle est la sensibilité des renseignements concernés ?
- Quelles sont les conséquences appréhendées de leur utilisation ?
- Quelle est la probabilité qu'ils soient utilisés à des fins préjudiciables ?

1. **Renseignements sensibles**
   - Documents financiers ;
   - Dossiers médicaux ;
   - Les renseignements personnels que l'on communique de manière courante ne sont généralement pas considérés comme sensibles (nom, adresse) ;
     - Sauf si le contexte en fait des renseignements sensibles : nom, adresses associé·e·s à des périodiques spécialisés ou à des activités qui les identifient.

2. **Préjudice grave**
   - Humiliation ;
   - Dommage à la réputation ou aux relations ;
   - Perte de possibilité d'emploi ou d'occasion d'affaires ou d'activités professionnelles ;
   - Perte financière ;
   - Vol d'identité ;
   - Effet négatif sur le dossier de crédit ;
   - Dommage aux biens ou leur perte ;

3. **Pour déterminer la probabilité d'un mauvais usage**
   - Qu'est-il arrivé et quels sont les risques qu'une personne subisse un préjudice en raison de l'atteinte ?
   - Qui a eu accès aux renseignements personnels ou aurait pu y avoir accès ?
   - Combien de temps les renseignements personnels ont-ils été exposés ?
   - A-t-on constaté un mauvais usage des renseignements ?
   - L'intention malveillante a-t-elle été démontrée (vol, piratage) ?
   - Les renseignements ont-ils été exposés à des entités ou à des personnes susceptibles de les utiliser pour causer un préjudice ou qui représentent un risque pour la réputation de la ou des personnes touchées ?

Si l'analyse fait ressortir un risque de préjudice sérieux, l'organisation doit aviser la Commission et les personnes concernées de l'incident. Dans le cas contraire, elle doit tout de même poursuivre ses travaux pour réduire les risques et éviter qu'un incident de même nature se produise à nouveau.

[1] [1] Le questionnaire respecte le **Règlement sur les incidents de confidentialité**

ANNEXE 4 : INCIDENT DE CONFIDENTIALITÉ : CONTENU DE LA COMMUNICATION AUX PERSONNES CONCERNÉES

Tel qu'indiqué à l'article 9.4 de la présente politique, un organisme doit aviser « avec diligence » toutes les personnes dont les renseignements personnels ont été touchés par un incident de confidentialité. Cet avis doit être envoyé directement aux personnes concernées. Toutefois, le **Règlement sur les incidents de confidentialité** prévoit des situations où la communication peut se faire exceptionnellement par le biais d'un avis public, dont lorsque le fait de transmettre l'avis est susceptible de représenter une difficulté excessive pour l'organisme ou d'accroître le préjudice causé aux personnes concernées..

Contenu obligatoire de la communication

Comme c'est le cas pour l'avis écrit à la CAI, l'avis écrit aux personnes concernées doit contenir les éléments suivants :

- Une description des renseignements personnels touchés par l'incident ou, si cette information est inconnue, les raisons pour lesquelles il est impossible de fournir une telle description ;
- Une brève description des circonstances de l'incident ;
- La date ou la période à laquelle a eu lieu l'incident (ou une approximation si cette information n'est pas connue) ;
- Une brève description des mesures que l'organisme a prises ou entend prendre suivant l'incident dans le but de réduire les risques de préjudice ;
- Les mesures que l'organisme suggère à la personne concernée de prendre dans le but de réduire/atténuer les risques de préjudice ;
- Les coordonnées de la personne auprès de laquelle la personne concernée peut obtenir de plus amples renseignements à propos de l'incident.