

POLITIQUE DE GESTION DES RENSEIGNEMENTS PERSONNELS

ADOPTÉE PAR LE COLLECTIF AUTONOME
DES CARREFOUR JEUNESSE-EMPLOI DU QUÉBEC

[Février 2009]



TABLE DES MATIÈRES

TABLE DES MATIÈRES	2
1. PRÉAMBULE	
1.1. Portée	3
1.2. Définitions	3
1.3. Objectifs	4
1.4. Contexte	5
2. PRINCIPES	
2.1. Faire preuve de transparence	7
2.2. Assumer ses responsabilités	7
2.3. Déterminer les fins de collecte de données	9
2.4. Limiter la collecte des données	9
2.5. Informer la personne concernée	9
2.6. Obtenir un consentement	10
2.7. Limiter l'utilisation, la communication et la conservation des données	11
2.8. Assurer l'exactitude et la qualité des informations	12
2.9. Garantir la sécurité des renseignements personnels	13
2.10. Assurer un droit d'accès et de rectification	14
2.11. Accueillir les plaintes contre le non-respect des principes	15
3. GESTION DES BANQUES DE DONNÉES	16
4. LISTE DES DOCUMENTS CONSULTÉS	17

1. PRÉAMBULE

1.1. Portée

Le présent document représente la Politique de gestion des renseignements personnels du Collectif autonome des CJE du Québec. Elle s'applique à tous les renseignements personnels ainsi qu'aux données et informations opérationnelles que les CJE possèdent au sujet de ses clients et ses employés.

Il incombe à tous les membres du Collectif autonome des CJE de la lire, la comprendre et la mettre en pratique. La politique décrit les exigences minimales concernant la protection des renseignements personnels. La mise en œuvre de ces exigences est assujettie à toute loi pertinente et peut être appliquée à tout renseignement personnel. Dans la mesure où les exigences minimales sont respectées, l'organisme peut adapter la norme à sa situation particulière. De plus, les politiques spécifiques et les pratiques peuvent varier suivant que les renseignements personnels se rapportent à des membres, à des employés, à des clients ou à d'autres personnes et ce, conformément aux particularités spécifiées dans différents protocoles ou par différents ordres professionnels.

Les onze principes qui constituent cette politique sont interdépendants. Les organismes sont libres d'adhérer au non à l'ensemble de ces principes. Même si les termes utilisés dans les articles qui suivent sont de nature obligatoire (p. ex. les termes «doit» et «il faut»), l'adhésion à cette politique est volontaire. Ceux qui adoptent la politique doivent comprendre et adhérer aux onze principes dans leur totalité. Cependant, ils peuvent adapter cette norme à leur situation spécifique tout en en conservant les fondements :

- a) en définissant la façon dont ils souscrivent aux onze principes susmentionnés;
- b) en élaborant un code qui leur est propre;
- c) en modifiant les commentaires pour fournir des exemples qui leur sont propres.

1.2. Définitions

Besoin de savoir : réflexion et décision concernant la pertinence de connaître une information en vue de servir les intérêts des personnes concernées.

Confidentialité : l'attribut des renseignements personnels ou non personnels qui devraient être vus seulement par les personnes qui, dans l'exercice de leur travail, ont un droit et une raison légitime pour cela. La confidentialité soutient les notions de « besoin de savoir ».

Collecte : Action de recueillir, d'acquérir ou d'obtenir des renseignements personnels de n'importe quelle source, y compris des tiers, par quelque moyen que ce soit.

Communication : Transmission des renseignements personnels à des personnes à l'intérieur ou à l'extérieur de l'organisme (voir définition d'organisme).

Consentement : Acquiescement libre à ce qui se fait ou est proposé. Le consentement peut être exprimé ou implicite. Le consentement exprimé se donne de façon explicite, de vive voix ou par écrit. Le consentement explicite est non équivoque et n'oblige pas l'organisme qui demande le consentement de la personne à l'inférer. Le consentement implicite survient lorsque les actes ou l'inaction de la personne permettent raisonnablement de déduire qu'il y a consentement.

Organisme : Terme qui comprend les associations, les entreprises, les œuvres de bienfaisance, les clubs, les organismes gouvernementaux, les institutions, les ordres professionnels et les syndicats. Ainsi, il inclut les Carrefour Jeunesse-Emploi autant que le Collectif Autonome des CJE du Québec ou tout autre organisme qui choisiraient d'adopter cette politique.

Renseignements personnels : Tout renseignement au sujet d'une personne et qui permet de l'identifier. Le nom, l'âge, le sexe, l'adresse, la source de revenu, le numéro d'assurance sociale, les renseignements financiers et médicaux sont, entre autres, des renseignements considérés comme personnels.

Utilisation : Traitement, manipulation et extraction de renseignements personnels au sein d'un organisme.

1.3. Objectifs

Le but premier de l'élaboration de cette politique est son application dans les organismes membres du CACJEQ afin de donner l'assurance que la gestion des renseignements personnels au sein des CJE est en conformité avec La Loi sur la protection des renseignements personnels, particulièrement les articles 4 à 8 (Communément désignés sous le nom Code des pratiques équitables en matière d'information) et que l'utilisation, la divulgation, la conservation et l'élimination des renseignements personnels en respectent les clauses. La politique a pour objet

d'aider les organismes à élaborer et à appliquer les directives et les pratiques nécessaires à une gestion saine et éthique des renseignements personnels.

1.4. Contexte

Le Collectif Autonome des CJE du Québec connaît l'importance de la protection de la vie privée. Les nouvelles technologies et les pratiques de consommations commerciales et de services soulèvent des questions au sujet du respect du droit à la vie privée et du droit des individus de contrôler l'utilisation et la communication de renseignements personnels qui les concernent. Les membres du CACJÉQ se sont engagés à accomplir leur mission et prendre leurs actions dans le respect des normes d'éthique et d'intégrité les plus strictes par la mise en œuvre de méthodes honnêtes et éprouvées en matière de gestion des renseignements personnels.

Par l'entremise de la Politique de la protection des renseignements personnels, les membres affirment cette engagement face à leur conseil d'administration, leurs employés, leurs clientèles et leurs différents partenaires quant à bien déterminer leurs besoins de renseignements personnels, à protéger l'information qu'ils possèdent et à se conformer aux lois qui encadrent la protection de la vie privée.

Tous les employés de des CJE sont appelés à collecter, utiliser ou communiquer des renseignements personnels. Pour se faire, ils doivent respecter les dispositions de la politique en matière de protection des renseignements personnels.

Le Collectif autonome des CJE du Québec reconnaît sa responsabilité à l'égard des renseignements personnels détenus par ses membres, y compris ceux confiés à des tiers à des fins de traitement. Le Collectif autonome des CJE du Québec prend l'engagement d'établir une politique visant à assurer le caractère confidentiel des renseignements personnels par la mise en place de procédures et de mesures de sécurité les plus strictes afin de protéger les renseignements personnels confiés. Ces mesures, qui comprennent des moyens de protection matériels, administratifs et technologiques sont constamment mises à jour et font l'objet de vérifications internes par les organismes.

Le Collectif Autonome des CJE du Québec déploie des efforts concertés dans le but d'améliorer la manipulation des renseignements personnels qu'il détient au sujet de ses clients et employés et plusieurs projets ont été mis en œuvre pour renforcer la protection des renseignements personnels et garantir qu'ils sont consultés et utilisés à des fins

légitimes. Des politiques et des procédures couvrant tous les aspects de la gestion des renseignements personnels ont été mises en place; certaines sont autonomes et d'autres sont intégrées aux politiques et aux procédures de sécurité.

Un comité a été créé en matière la protection des renseignements personnels et l'élaboration de cette politique de gestion de la protection des renseignements personnels n'est que le début des travaux permettant une redéfinition et une clarification de la notion de protection des renseignements personnels. Un plan global de communication, de sensibilisation et de formation est recommandé pour garantir que tous les employés reçoivent une formation et une information opportunes et adéquates sur la législation, les politiques et les procédures liées à l'utilisation et à la protection des renseignements personnels dans leur secteur d'activités.

Dans un souci d'agir avec diligence, éthique et en conformité avec la loi, ces réflexions constituent les piliers de la protection de la vie privée. Ainsi, la planification et gouvernance stratégiques, la gestion du risque, les changements culturels et l'assurance de conformité retiennent l'attention des membres concernant les aspects liés à la reddition de comptes.

2. PRINCIPES

2.1. Premier principe - Faire preuve de transparence

L'organisme doit mettre à la disposition de toute personne qui le désire, les renseignements précis et à jour sur ses politiques et ses pratiques concernant la gestion des renseignements personnels. Une personne devrait pouvoir obtenir sans efforts déraisonnables l'information dont elle a besoin et les renseignements doivent être fournis sous une forme généralement compréhensible.

Parmi les informations qui se doivent d'être accessibles, on retrouve:

- a) les nom, fonction et adresse professionnelle de la personne responsable de la politique et des pratiques de l'organisme et à qui il faut acheminer les plaintes et les demandes de renseignements ;
- b) la procédure pour avoir accès aux renseignements personnels que possède l'organisme;
- c) une description du genre de renseignements personnels que possède l'organisme, y compris une explication générale de l'usage auquel ils sont destinés;
- d) une copie de toute brochure ou autre document d'information expliquant la politique, les normes ou les codes de l'organisme;
- e) la nature des renseignements personnels communiqués aux organismes associés et les procédures d'autorisation concernant ces communications.

Un organisme peut rendre l'information concernant sa politique et ses pratiques accessibles de diverses façons. La méthode choisie est fonction de la nature des activités de l'organisme et d'autres considérations.

2.2. Deuxième principe : Assumer ses responsabilités

L'organisme est responsable de tous les renseignements personnels qu'il a en sa possession, sous sa garde ou dont il a la gestion, y compris les renseignements confiés à une tierce partie aux fins de traitement. Ces renseignements comprennent les renseignements personnels que le CJE a obtenus directement des clients ou d'organisations partenaires (par exemple, d'autres organismes sans but lucratif, des ministères, des commissions scolaires, etc.). Il doit donc, par voie contractuelle ou autre, fournir un degré comparable de protection aux renseignements qui sont en cours de traitement par une tierce partie.

Un organisme est responsable de respecter les politiques et directives régissant la protection des renseignements personnels dont il a la gestion et il doit désigner une ou des personnes qui devront s'assurer du respect de l'ensemble des principes énoncés dans cette politique :

Les politiques et directives liées aux principes, incluent:

- a) l'adoption de politiques et de procédures visant à protéger adéquatement les renseignements personnels;
- b) la mise en place des procédures pour recevoir les plaintes et les demandes de renseignements et y donner suite;
- c) la sensibilisation du personnel et des bénévoles quant aux politiques adoptées et aux pratiques de l'organisme ainsi que du rôle et des responsabilités qui leur incombent relativement au maintien de la confidentialité des renseignements personnels;
- d) la nomination d'un responsable de la protection des renseignements personnels, chargé de la surveillance des questions relatives à la protection des renseignements personnels.

Les politiques, les lignes directrices et les procédures relatives à la manutention et à la protection des renseignements personnels sont disponibles, et les employés en sont informés et (ou) ont reçu une formation pertinente à ces questions. De même, la vérification, le contrôle, l'évaluation des risques et des contrôles liés à la manutention et à la protection des renseignements personnels sont faits régulièrement. En ce sens, les gestionnaires se doivent d'être responsables de la sensibilisation accrue des employés à l'égard de leurs responsabilités envers la protection de la vie privée et des renseignements personnels.

L'organisme devrait élaborer, communiquer et mettre en œuvre à tous les niveaux et dès que possible un cadre d'imputabilité pour la manipulation des renseignements personnels tenant compte des interrelations et du partage des renseignements personnels autant à l'interne qu'à l'externe. Ce cadre devrait s'appuyer sur quatre piliers : la planification et la gouvernance stratégiques, la gestion du risque, les changements culturels et l'assurance de conformité.

La connaissance et la compréhension des attentes constituent un aspect important de la politique de gestion de la protection des renseignements personnels. Tout nouvel employé doit signer une entente de confidentialité ou un engagement au secret professionnel, qu'il soit membre d'un ordre professionnel ou non. En outre, les employés qui doivent accéder à des renseignements personnels doivent être informés des enjeux liés à la protection des

renseignements personnels au cours de leur formation initiale, en insistant sur la divulgation des renseignements personnels et les conflits d'intérêts.

2.3. Troisième principe – Déterminer les fins de la collecte des données

Les fins et les raisons pour lesquelles des renseignements personnels sont recueillis doivent être déterminées par l'organisme avant ou au moment de la collecte. Il lui incombe de démontrer explicitement en quoi les renseignements visés par la collecte revêtent un caractère indispensable.

Avant de se servir de renseignements personnels à des fins non précisées antérieurement, les nouvelles fins doivent être précisées au préalable avant de les utiliser. À moins que les nouvelles fins auxquelles les renseignements sont destinés ne soient prévues par une loi, il faut obtenir le consentement de la personne concernée avant d'utiliser les renseignements pour cette nouvelle fin.

2.4. Quatrième principe - Limiter la collecte des données

L'organisme ne doit recueillir que les renseignements nécessaires aux fins mentionnées, sans être arbitraire. On doit restreindre tant la quantité que la nature des renseignements recueillis à ce qui est nécessaire pour réaliser les fins déterminées. Ainsi, l'organisme ne peut recueillir que les seuls renseignements personnels nécessaires à l'exercice de ses attributions ou à la mise en œuvre d'un programme dont il a la gestion. La collecte d'information doit être honnête et licite.

L'exigence selon laquelle les organismes sont tenus de recueillir des renseignements personnels de façon honnête et licite a pour objet de les empêcher de tromper les gens et de les induire en erreur quant aux fins auxquelles les renseignements sont recueillis. Cette obligation sous-entend que le consentement à la collecte de renseignements ne doit pas être obtenu par un subterfuge.

2.5. Cinquième principe - Informer la personne concernée

L'information concernant les fins auxquelles ils sont destinés, le traitement et la conservation de celle-ci ainsi que tout changement subséquent relatif à l'utilisation doit être transmise avant ou

au moment de la collecte. Les personnes qui recueillent des renseignements personnels devraient être en mesure d'expliquer à la personne concernée à quelles fins sont destinés ces renseignements. Selon la façon dont se fait la collecte, cette précision peut être communiquée de vive voix ou par écrit. Par exemple, on peut indiquer ces fins sur un formulaire de demande de renseignements.

2.6. Sixième principe - Obtenir le consentement

Toute personne doit être informée et consentir à toute collecte, utilisation ou communication de renseignements personnels qui la concernent. Il faut obtenir le consentement de la personne concernée avant de recueillir des renseignements personnels à son sujet et d'utiliser ou de communiquer les renseignements recueillis.

Généralement, un organisme obtient le consentement des personnes concernées relativement à l'utilisation et à la communication des renseignements personnels au moment de la collecte. Dans certains cas, un organisme peut obtenir le consentement concernant l'utilisation ou la communication des renseignements après avoir recueilli ces renseignements, mais avant de s'en servir, par exemple, quand il veut les utiliser à des fins non précisées antérieurement. À ce moment, il doit s'assurer d'obtenir le consentement pour la modification de l'utilisation par une autorisation spécifique. Pour que le consentement soit valable, les fins doivent être énoncées de façon que la personne puisse raisonnablement comprendre de quelle manière les renseignements seront utilisés ou communiqués.

Un organisme ne peut pas, pour le motif qu'il fournit un bien ou un service, exiger d'une personne qu'elle consente à la collecte, à l'utilisation ou à la communication de renseignements autres que ceux qui sont nécessaires pour réaliser les fins légitimes et explicitement indiquées.

La forme du consentement que l'organisme cherche à obtenir peut varier selon les circonstances et la nature des renseignements. Pour déterminer la forme que prendra le consentement, les organismes doivent tenir compte de la sensibilité des renseignements. Si certains renseignements sont toujours considérés comme sensibles, par exemple le numéro d'assurance sociale, les dossiers médicaux et le revenu, tous les renseignements peuvent devenir sensibles suivant le contexte. En général, l'organisme devrait chercher à obtenir un consentement explicite si les renseignements sont susceptibles d'être considérés comme sensibles. Lorsque les renseignements sont moins sensibles, un consentement implicite serait normalement jugé approprié.

Le consentement peut revêtir différentes formes, par exemple:

- a) on peut se servir d'un formulaire de demande de renseignements pour obtenir le consentement, recueillir des renseignements et informer la personne de l'utilisation qui sera faite des renseignements. En remplissant le formulaire et en le signant, la personne donne son consentement à la collecte de renseignements et aux usages précisés;
- b) on peut prévoir une case où la personne pourra indiquer en cochant qu'elle refuse que ses nom et adresse soient communiqués à d'autres organismes. Si la personne ne coche pas la case, il sera présumé qu'elle consent à ce que les renseignements soient communiqués à des tiers;
- c) le consentement peut être donné de vive voix lorsque les renseignements sont recueillis par téléphone; ou
- d) le consentement peut être donné au moment où le service est utilisé.

Une personne peut retirer son consentement en tout temps, sous réserve de restrictions prévues par une loi ou un contrat et d'un délai raisonnable. L'organisme devrait informer la personne des conséquences d'un tel retrait.

Si la personne a moins de 14 ans, l'autorisation peut être donnée par le titulaire de l'autorité parentale.

2.7. Septième principe - Limiter l'utilisation, la communication et la conservation des données

Les renseignements personnels ne doivent pas être utilisés ou communiqués à des fins autres que celles auxquelles ils ont été recueillis à moins que la personne concernée n'y consente ou que la loi ne l'exige. On ne doit conserver les renseignements personnels qu'aussi longtemps que nécessaire pour la réalisation des finalités déterminées. Ainsi les différents types de données auront des durées d'utilisation, de communication et de conservation différentes, en fonction de leurs fins.

Le furetage est un type particulier de violation du principe du « besoin de savoir » et est défini comme étant la consultation de renseignements personnels sur un individu pour des motifs autres que des motifs professionnels légitimes. Même si l'employé n'a obtenu aucun avantage personnel en consultant les renseignements ou n'avait pas l'intention d'utiliser les renseignements à des fins illicites, cette action doit être interdite.

La direction de tout organisme devrait s'assurer que les personnes qui donnent et qui obtiennent l'accès à des renseignements personnels comprennent la nature et l'application du

principe du « besoin de savoir », de même que les conséquences de violation telles le « furetage » et les divulgations illicites.

Les organismes devraient élaborer des lignes directrices et appliquer des procédures pour la conservation des renseignements personnels. Ces lignes directrices devraient préciser les durées minimales et maximales de conservation. On doit conserver les renseignements personnels servant à prendre une décision au sujet d'une personne suffisamment longtemps, selon le type de données, pour permettre à la personne concernée d'exercer son droit d'accès à l'information après que la décision a été prise. Un organisme peut être assujéti à des exigences prévues par la loi ou par des ordres professionnels en ce qui concerne les périodes de conservation.

On devrait détruire, effacer ou dépersonnaliser les renseignements personnels dont on n'a plus besoin aux fins précisées ou lorsque l'objet pour lequel il a été recueilli est accompli. Les organismes devraient élaborer des lignes directrices et appliquer des procédures régissant la destruction des renseignements personnels (sous réserve de la Loi sur les archives).

Un renseignement personnel demeure inaccessible tant que la personne concernée n'a pas consenti à sa divulgation. Par conséquent, seuls les organismes que la personne concernée autorise auront accès à ses renseignements personnels. Lorsqu'il y a communication de renseignements personnels, l'organisme doit s'assurer que celle-ci soit faite selon les principes reconnus dans cette politique.

Les procédures de destruction doivent tenir compte de l'ensemble des principes de la présente politique. Ainsi, les papiers contenant des informations personnelles et confidentielles sur un jeune adulte sont déchetés au préalable avant d'être mis au recyclage. Au moment du retrait ou de la destruction des renseignements personnels, on doit veiller à empêcher les personnes non autorisées d'y avoir accès. Lorsque du matériel contenant des renseignements personnels sur les clients du ministère ou d'autres individus est envoyé ou détruit par des entreprises dans le cadre d'un contrat, ce contrat doit indiquer spécifiquement la responsabilité de l'entreprise de protéger la confidentialité des renseignements personnels sous son contrôle.

2.8. Huitième principe — Assurer l'exactitude et la qualité des informations

Les renseignements personnels doivent être aussi exacts, complets et à jour afin de servir adéquatement aux fins pour lesquelles ils ont été recueillis. Ainsi, il est possible que la mise à jour ne soit pas nécessaire, voire non-recommandée.

Le degré d'exactitude et de mise à jour ainsi que le caractère complet des renseignements personnels dépendront de l'usage auquel ils sont destinés, compte tenu des intérêts de la personne. Les renseignements doivent être suffisamment exacts, complets et à jour pour réduire au minimum la possibilité que des renseignements erronés soient utilisés pour prendre une décision à son sujet.

Les renseignements personnels qui servent en permanence, y compris les renseignements qui sont communiqués à des tiers, devraient normalement être exacts et à jour à moins que des limites se rapportant à l'exactitude de ces renseignements ne soient clairement établies.

2.9. Neuvième principe — Garantir la sécurité des renseignements personnels

Les renseignements personnels doivent être protégés au moyen de mesures de sécurité correspondant à leur degré de sensibilité. Ces mesures de sécurité doivent protéger les renseignements personnels contre la perte ou le vol ainsi que contre l'accès, la communication, la copie, l'utilisation ou la modification non autorisées. Les organismes doivent protéger les renseignements personnels quelle que soit la forme sous laquelle ils sont conservés.

La nature des mesures de sécurité variera en fonction du degré de sensibilité des renseignements personnels recueillis, de la quantité, de la répartition et du format des renseignements personnels ainsi que des méthodes de conservation.

Les méthodes de protection devraient comprendre:

- a) des moyens matériels : le verrouillage des classeurs et la restriction de l'accès aux bureaux;
- b) des mesures administratives : des autorisations sécuritaires, un accès sélectif, des ententes de confidentialité avec les employés et les différents protocoles;
- c) des mesures technologiques : l'usage de mots de passe et du chiffrement, base de données, pare-feu, logiciel de préservation, etc. On devrait définir clairement et mettre en pratique des procédures de gestion de tous les codes d'accès et des profils qui permettent d'accéder à des renseignements personnels. De même, on devrait fournir de la documentation sur la nature des renseignements personnels auxquels les employés ont accès.
- d) des mesures organisationnelles ; rangement de dossiers et politique de transport des dossiers, encadrement des échanges professionnels et des discussions au sujet des services rendus aux clients, disponibilité de bureaux privés et fermés pour les entrevues,

e) des mesures contractuelles : des ententes de confidentialités avec les tiers engagés pour fournir des services à l'organisme et auxquels sont transmis les renseignements personnels soient tenus par contrat de respecter l'esprit de la présente politique de protection des renseignements personnels (firme comptable, service informatique, destruction des données, entretien des locaux, etc.)

Les mesures de sécurité utilisées pour la protection des données sont réexaminées régulièrement pour tenir compte de l'évolution ou des changements organisationnels de l'organisme.

Lorsque la vie d'une personne est en danger, toutes les mesures nécessaires doivent être prises. Même si des informations jugées confidentielles doivent être dévoilées, tout doit être fait pour sauvegarder la vie de la personne, sans toutefois mettre la sienne en danger.

2.10. Dixième principe — Assurer un droit d'accès et de rectification

Un organisme doit informer toute personne qui en fait la demande de l'existence de renseignements personnels qui la concernent, de la source de ces renseignements, de l'usage qui en est fait, du fait qu'ils ont été communiqués à des tiers, et lui permettre de les consulter. Il sera aussi possible de contester l'exactitude et l'état complet des renseignements et y faire apporter les corrections appropriées.

L'organisme peut demander à la personne de fournir des preuves suffisantes de son identité avant de lui permettre l'accès à des informations concernant l'existence, l'utilisation ou la communication des renseignements personnels. Ces preuves ne seront utilisées qu'à cette seule fin.

L'organisme qui fournit le relevé des tiers à qui il a communiqué des renseignements personnels au sujet d'une personne devrait être le plus précis possible.

Un organisme qui reçoit une demande de communication de renseignements personnels doit répondre dans un délai raisonnable et à un coût minime, sinon nul pour la personne. Les renseignements demandés doivent être fournis sous une forme généralement compréhensible. Si une partie des informations ne pouvaient être transmises pour des raisons légales, elles devront être clairement expliquées à la personne.

Lorsqu'une personne démontre que des renseignements personnels sont inexacts ou incomplets, l'organisme doit apporter les modifications nécessaires à ces renseignements après avoir pris les mesures nécessaires de validation. Selon la nature des renseignements qui font l'objet de la contestation, l'organisme doit corriger, supprimer ou ajouter des renseignements. S'il y a lieu, l'information modifiée doit être communiquée à des tiers ayant accès à l'information en question.

Lorsqu'un différend n'est pas réglé à la satisfaction de la personne concernée, l'organisme devrait enregistrer le fond de la plainte rejetée. S'il y a lieu, les tierces parties ayant accès à l'information en question devraient être informées du fait que le différend n'a pas été réglé.

Les demandes d'accès aux renseignements personnels sont considérées comme étant formelles ou informelles. Une demande formelle est une demande reçue par écrit et fondée sur la Loi sur la protection des renseignements personnels ou une demande qu'on a présentée en utilisant le formulaire officiel de l'organisme, s'il y a lieu.

2.11. Onzième principe – Accueillir les plaintes de non-respect des principes

Toute personne doit être en mesure de se plaindre du non-respect des principes énoncés ci-dessus en communiquant avec les responsables de les faire respecter au sein de l'organisme concerné.

L'organisme doit informer les personnes de l'existence de ce droit et il doit établir des mécanismes pour recevoir les plaintes et les demandes de renseignements concernant ses politiques et pratiques de gestion des renseignements personnels et y donner suite. Le mécanisme du processus de plaintes devrait être facilement accessible et simple à utiliser.

Un organisme doit faire enquête sur toutes les plaintes. Si une plainte est jugée fondée dans le cadre du processus d'examen des plaintes interne ou externe, l'organisme doit prendre les mesures appropriées, y compris la modification de ses politiques et de ses pratiques si c'est nécessaire.

3. GESTION DES BANQUES DE DONNÉES

Les banques ou bases de données sont constituées à partir des renseignements personnels des clients des organismes. La constitution ou l'acquisition (c'est-à-dire le prêt, le transfert ou l'achat) d'une banque de données comportant des renseignements personnels ne peut être entrepris avant que les onze principes précédents n'aient été complétés avec certitude.

Ainsi, une base de données doit être administrée selon ces onze principes et une politique organisationnelle doit être mise en place afin de recueillir les informations suivantes :

- le nom de la banque de données,
- l'identité de la personne responsable de la banque et qui en est imputable,
- l'origine du financement qui permet la création et le fonctionnement de la banque de données, s'il y a lieu,
- les objectifs et les fins de constitution de la banque de données,
- la nature des données qui seront versées dans la banque (ex : données démographiques, sociales, de services, etc.),
- les modalités selon lesquelles les données seront recueillies,
- le mode d'identification des données,
- les mesures de sécurité qui permettront d'en assurer la confidentialité,
- le mode et le délai projeté de conservation des données.

La personne responsable de la banque est tenue de soumettre un rapport annuel des activités de la banque de données et de n'en soustraire que les informations déterminées par les fins recherchées et préalablement identifiées. Tous les renseignements personnels versés dans une banque de données et faisant l'objet d'un rapport, doivent être traités par le responsable de façon dénominalisée, c'est-à-dire qu'en aucun temps, il ne sera possible à un tiers de faire le lien entre les renseignements personnels et les participants qui les ont fournis.

4. LISTE DES DOCUMENTS CONSULTÉS

Charte québécoise des droits et libertés de la personne

Charte canadienne des droits et libertés

Code civil du Québec

Loi sur la protection des renseignements personnels (L.R. 1985, P-21)

Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (L.R.Q., Ch. A-2.1)

Loi sur la protection des renseignements personnels dans le secteur privé (L.R.Q., Ch. P-39.1)

Loi sur la protection des documents personnels et les documents électroniques au Canada (2000, ch. 5)

Loi concernant le cadre juridique des technologies de l'information (L.R., 2001, ch. 32)

Guide d'élaboration de normes sur la gestion des banques de données, MSSS, mai 2004

Guide à l'intention des entreprises et des organisations : protection des renseignements personnels : vos responsabilités, Commissariat à la protection de la vie privée au Canada, 2004

Guide au sujet de la loi sur les renseignements personnels et les documents électronique : Vos droits en matière de vie privée, Commissariat à la protection de la vie privée au Canada, 2004