

**GUIDE EN MATIÈRE DE
PROTECTION DES
RENSEIGNEMENTS PERSONNELS
DANS LE DÉVELOPPEMENT DES
SYSTÈMES D'INFORMATION**

À L'INTENTION DES MINISTÈRES ET
ORGANISMES PUBLICS

VERSION 1.0

20 **ANS**

LA LOI SUR L'ACCÈS
AUX DOCUMENTS
DES ORGANISMES PUBLICS
ET SUR LA PROTECTION
DES RENSEIGNEMENTS
PERSONNELS

DÉCEMBRE 2002

Conception et réalisation : Commission d'accès à l'information

Dépôt légal – 2002

Bibliothèque nationale du Québec

Bibliothèque nationale du Canada

ISBN 2-550-40206-5

CAI-DOC-003-02-F

Gouvernement du Québec 2002

Ce rapport est disponible sur le site Internet de la Commission à l'adresse suivante : www.cai.gouv.qc.ca

Tous droits réservés pour tous pays.

La reproduction par quelque procédé que ce soit et la traduction même partielles sont autorisées dans la mesure où la source est indiquée.

Le présent document n'a pas de valeur juridique. En cas de contradiction entre l'information contenue dans ce guide et les termes mêmes de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (L.R.Q., c. A-2.1), la loi prévaudra.

L'emploi du masculin a pour seul but d'alléger le texte. Dans tous les cas, il désigne aussi bien les femmes que les hommes quand le contexte s'y prête.

Le présent guide peut être reproduit en tout ou en partie à la condition d'en mentionner la source et de ne pas l'utiliser à des fins commerciales.

TABLE DES MATIÈRES


	Page
PRÉSENTATION	2
PRINCIPES SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS	
1. Assumer ses responsabilités face aux renseignements personnels.....	3
2. Déterminer les fins de la collecte de renseignements personnels.....	4
3. Limiter la collecte de renseignements personnels	5
4. Informer la personne concernée.....	6
5. Limiter l'accès aux renseignements personnels	7
6. Requérir le consentement à la communication entre organismes publics	9
7. Assurer la qualité des renseignements personnels.....	11
8. Garantir la sécurité des renseignements personnels	12
9. Assurer les droits d'accès et de rectification.....	14
10. Limiter la durée de conservation des renseignements personnels	14
CONCLUSION	15

PRÉSENTATION

Ce guide s'adresse à tous les organismes publics concernés par le développement de systèmes d'information. Il se veut d'abord une initiative tangible vers une meilleure prise en charge des mesures de protection des renseignements personnels dans le contexte d'une imputabilité des administrateurs publics. Il se veut également une réponse à ceux qui souhaitent mieux connaître la teneur des critères d'évaluation sur lesquels se base la Commission dans son appréciation des projets technologiques.

Le guide tend à faire ressortir de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (Loi sur l'accès) les obligations ou principes fondamentaux ayant trait spécifiquement à la protection des renseignements personnels, dans la foulée des *Lignes directrices* de l'Organisation de coopération et de développement économiques (OCDE)¹ et des *Principes* de l'Association canadienne de normalisation (ACNOR)².

Pour chacun des principes, le lecteur y trouvera des énoncés auxquels devrait pouvoir répondre un organisme public afin d'évaluer, au plan de la protection des renseignements personnels, le degré de conformité d'un système d'information technologique qu'il entend développer.

En marge de certains énoncés se retrouve une indication visuelle  dans le but d'attirer une attention particulière sur une problématique que la Commission voit poindre dans le traitement de ses dossiers. D'autres énoncés sont inscrits en **caractères gras** parce qu'ils ont été jugés déterminants dans le développement de tout système d'information contenant des renseignements personnels.

Nous sommes conscients que pour les initiés en matière de protection des renseignements personnels, le présent guide constituera davantage un rappel des principes directeurs en vigueur depuis l'adoption de la Loi sur l'accès, il y a vingt ans. Ces principes sont et demeurent plus que jamais d'actualité. La quête de meilleurs rendements dans le traitement de l'information, rendus possibles par le développement fulgurant des nouvelles technologies, amène de nouvelles applications de ces principes directeurs qu'il faut prendre en compte dès la conception de nouveaux systèmes d'information.

Ce document se veut un outil pratique et évolutif. Il est probable qu'aux yeux de certains sa mise en œuvre paraîtra laborieuse ou exigeante alors qu'elle apportera aux autres la touche d'éclaircissements attendue. Suivant la nature des projets et des mesures de protection prévues pour les renseignements personnels, on peut imaginer en effet que chaque ministère et organisme fasse une lecture du guide qui soit singulière et novatrice. Souhaitons que ces utilisations suscitent des échanges interactifs avec le personnel de la Commission aux fins de l'améliorer.

En terminant, les visées pédagogiques de ce guide ne doivent pas faire oublier que la Loi sur l'accès demeure la seule assise légale sur laquelle se fonde la Commission dans ses avis. Nous verrons dans le futur à mettre à jour le contenu des prochaines pages de manière à ce qu'il s'harmonise aux décisions de la Commission.

¹ Organisation de coopération et de développement économiques, Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel, <http://www.oecd.org/FR/document/0,,FR-document-43-1-no-24-22735-43,00.html>

² Association canadienne de normalisation, [Code canadien de protection des renseignements personnels](http://www.csa.ca/standards/privacy/code/Default.asp?language=French), <http://www.csa.ca/standards/privacy/code/Default.asp?language=French>

PRINCIPES SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS



1. Assumer ses responsabilités face aux renseignements personnels

articles 8 et 59

Chaque organisme public a la responsabilité d'assurer le caractère confidentiel des renseignements personnels qu'il détient. D'office, la loi va même jusqu'à conférer les fonctions de protection des renseignements personnels à la personne ayant la plus haute autorité au sein de votre organisme.

Votre organisme dispose d'une somme de renseignements personnels qui constituent un capital informationnel à haut risque. Toute fuite ou tout mauvais usage de ceux-ci risque de porter atteinte à leur intégrité et à leur confidentialité en plus de nuire à la personne concernée. Pour contrer cette éventualité, des mesures de protection adéquates doivent être implantées, lesquelles supposent l'adoption et l'application de politiques de confidentialité évolutives et en constant raffinement. À cette fin, le responsable de la protection des renseignements personnels joue un rôle prépondérant dans la promotion et l'application des dispositions de la Loi sur l'accès au sein de votre organisme, appuyé dans sa démarche par ceux et celles qui recueillent, conservent, communiquent, traitent ou détruisent ces renseignements.

CONCRÈTEMENT

-  1.1 Une analyse de risques axée spécifiquement sur la protection des renseignements personnels évalue la performance des mesures adoptées dans votre projet et les conclusions d'analyse sont intégrées dans le développement du projet.
-  1.2 Le responsable de la protection des renseignements personnels de votre organisme est mis à contribution dans le développement de votre projet.
- 1.3 La protection des renseignements personnels est encadrée au sein de votre organisme par des politiques, directives, normes, procédures et autres instructions (accès distant, messagerie électronique, Internet, etc.). Vous êtes en mesure de dresser la liste des documents pertinents et d'indiquer la date de leur dernière révision.
- 1.4 Votre organisme dispose d'une politique de confidentialité.
- 1.5 Le personnel de votre organisme est sensibilisé et formé à la protection des renseignements personnels. Votre organisme dispose d'un programme de formation et de sensibilisation à la confidentialité explicitant les responsabilités de l'organisme, ses obligations, les règles d'éthique au travail, etc.
- 1.6 Votre organisme s'acquitte de ses obligations à l'égard des renseignements personnels en mettant à la disposition de son personnel les mécanismes de protection requis.
- 1.7 Si des tierces parties interviennent dans le projet, elles respectent les mêmes exigences de confidentialité que celles qui prévalent au sein de votre organisme.
- 1.8 Votre projet comporte des mécanismes en vue de gérer les plaintes ou les questions relatives à la protection des renseignements personnels.

2. Déterminer les fins de la collecte de renseignements personnels

article 64

Avant d'entreprendre toute collecte d'information, vous devez définir les raisons pour lesquelles vous comptez recueillir et utiliser un renseignement personnel. Ces motifs doivent être en accord avec les mandats, attributions et programmes relevant de votre organisme.

La mise en œuvre de ce principe constitue un préalable incontournable à l'application des autres principes. L'obligation d'identifier les raisons qui conduisent à une collecte de renseignements personnels permettra par la suite :

- *de délimiter le type et le nombre de renseignements personnels à recueillir;*
- *d'informer la personne concernée des raisons qui justifient la collecte de renseignements;*
- *de déterminer la fréquence de leur mise à jour;*
- *de limiter leur utilisation;*
- *de fixer, à terme, le moment de leur destruction.*

CONCRÈTEMENT

2.1 Vous identifiez les dispositions particulières des lois, règlements ou programmes légitimant votre collecte de renseignements personnels.

2.2 Vous destinez chaque renseignement personnel à un usage déterminé et vous reliez cet usage aux attributions de votre organisme ou à la mise en œuvre d'un programme dont votre organisme a la gestion.

2.3 Chaque renseignement personnel est utilisé pour une finalité autorisée.

2.4 Chaque fichier de renseignements personnels est créé ou maintenu pour une finalité autorisée.

2.5 Si vous confiez la collecte des renseignements personnels à une tierce partie externe à votre organisme, vous vous assurez que ce tiers respectera les fins de collecte établies.



2.6 Si votre projet constitue une refonte de systèmes existants, vous vous assurez que :

- la finalité de chacun des systèmes antérieurs soit connue;
- le nouveau système reconduise la finalité des systèmes antérieurs;
- toute collecte d'information additionnelle respecte la finalité des systèmes antérieurs.



2.7 Si vous créez des dépôts de renseignements personnels à des fins d'usage interne, en marge des principaux fichiers de renseignements personnels (p. ex. profils d'utilisateurs, journalisation des accès, données de surveillance, etc.), vous êtes en mesure de justifier la finalité de ces dépôts : gestion du personnel, gestion financière, tables de pilotage, sauvegardes et relèves, outils d'apprentissage, etc.



2.8 Si vous créez un entrepôt de données à partir notamment de fichiers de renseignements personnels, vous vous assurez de respecter le cloisonnement des fichiers qui comportent des finalités distinctes.



3. Limiter la collecte de renseignements personnels

article 64

Vous ne pouvez recueillir que les seuls renseignements personnels nécessaires à l'exercice des attributions de votre organisme ou à la mise en œuvre d'un programme dont il a la gestion. Il vous incombe de démontrer explicitement en quoi les renseignements visés par la collecte revêtent un caractère indispensable.

Votre regard doit porter ici sur le type et le nombre des renseignements personnels colligés. Vous devez justifier la nécessité de les recueillir, interroger leur provenance, anticiper les conséquences de leur détention, etc.

CONCRÈTEMENT

- 3.1 **Les renseignements personnels recueillis sont indispensables à l'exercice des attributions de l'organisme ou à la mise en œuvre d'un programme dont il a la gestion.**
- 3.2 **Les fins visées par la collecte ne peuvent être atteintes sans l'obtention de chacun des renseignements personnels.**
- 3.3 Vous identifiez les actions, décisions ou recommandations qui découlent des renseignements personnels recueillis.
- 3.4 La quantité de renseignements personnels à recueillir ne peut être réduite sans compromettre la finalité du fichier qui les contient.
-  3.5 Vous déclarez à la Commission les fichiers où sont versés les renseignements personnels recueillis, y compris ceux contenant des données de journalisation ou de surveillance.
- 3.6 Si vous avez recours à des identifiants généraux, tels le numéro d'assurance sociale, le numéro d'assurance maladie, le numéro de permis de conduire, le certificat d'identité électronique ou autres, vous êtes autorisés à les recueillir en vertu de dispositions légales ou d'ententes spécifiques.
- 3.7 Vous recueillez les renseignements personnels par l'intermédiaire de tierces personnes seulement s'il vous est impossible de les obtenir directement de la personne concernée.
- 3.8 Lors de la collecte de renseignements personnels, vous validez avec une assurance suffisante l'identité de la personne concernée, qu'elle soit physiquement présente ou non, sans pour autant recueillir de renseignements additionnels.
-  3.9 Si vous devez recueillir de l'information sur le poste informatique des internautes (témoins ou *cookies*, fichiers temporaires, pixels invisibles ou *web bugs*, etc.), vous êtes en mesure d'en démontrer la nécessité.

En se rappelant que...

La Commission privilégie l'adoption de pratiques favorisant autant que possible l'anonymat des personnes concernées. À défaut de pouvoir y parvenir, l'emploi de pseudonymes se révèle une alternative indiquée.



4. Informer la personne concernée

article 65

Vous avez l'obligation d'informer adéquatement la personne concernée avant qu'elle vous fournisse les renseignements personnels attendus. Vous devez faire preuve de transparence à son égard en lui communiquant les raisons de la collecte et les traitements accordés aux informations demandées.

Quel que soit le moyen technologique par lequel vous comptez joindre les personnes concernées, votre choix doit faire en sorte que tous reçoivent facilement une information compréhensible. Le recours accentué aux applications Web comme outils de collecte d'information ne vous soustrait pas à l'obligation d'expliquer clairement les raisons de votre démarche. Au contraire, il requiert que vous communiquiez à vos informateurs les risques associés à la transmission de renseignements sensibles sur le réseau Internet et vous oblige à de nouvelles précautions en matière de sécurité — l'authentification des parties dans la communication, l'intégrité des renseignements communiqués, la validité des consentements électroniques, etc.

CONCRÈTEMENT

- 4.1 **Vous adoptez des mécanismes particuliers pour informer la personne concernée des éléments prévus à l'article 65 de la Loi sur l'accès (voir note 3), en prenant soin d'utiliser des termes simples et usuels.**
- 4.2 Vous précisez quelles sont les conséquences pour la personne concernée ou pour le tiers, selon le cas, d'un refus de répondre à la demande de renseignements.
- 4.3 Vous indiquez la marche à suivre pour qu'une personne puisse accéder ou rectifier un renseignement personnel la concernant.
- 4.4 Si la collecte est effectuée par un intermédiaire mandataire, cet intermédiaire maintient vos obligations relatives à l'article 65 de la Loi sur l'accès.
- 4.5 Vous prenez une forme d'engagement particulière auprès de la personne concernée afin de l'assurer que vous n'utiliserez ses renseignements personnels que pour les usages projetés et les finalités recherchées.
-  4.6 **Si les renseignements personnels sont recueillis par le biais d'un formulaire électronique ou d'un autre document comparable, vous affichez les informations requises par l'article 65 prioritairement et préalablement à toute collecte de renseignements personnels.**
-  4.7 Vous avisez clairement les internautes de l'usage que vous faites des témoins (*cookies*) et autres traitements similaires effectués à leur insu, en indiquant quelles informations sont recueillies. Vous utilisez un langage simple et usuel.
- 4.8 Par l'entremise de son site Web, votre organisme affiche de manière évidente le contenu de sa politique de confidentialité.

³ 65. Quiconque, au nom d'un organisme public, recueille un renseignement nominatif auprès de la personne concernée ou d'un tiers doit au préalable s'identifier et l'informer:

1° du nom et de l'adresse de l'organisme public au nom de qui la collecte est faite;

2° de l'usage auquel ce renseignement est destiné;

3° des catégories de personnes qui auront accès à ce renseignement;

4° du caractère obligatoire ou facultatif de la demande;

5° des conséquences pour la personne concernée ou, selon le cas, pour le tiers, d'un refus de répondre à la demande;

6° des droits d'accès et de rectification prévus par la loi.

Toutefois, une personne dûment autorisée par un organisme public qui détient des dossiers ayant trait à l'adoption de personnes et qui recueille un renseignement relatif aux antécédents d'une personne visée dans l'un de ces dossiers ou permettant de retrouver un parent ou une personne adoptée n'est pas tenue d'informer la personne concernée ou le tiers de l'usage auquel est destiné le renseignement ni des catégories de personnes qui y auront accès. Les règles suivant lesquelles la collecte de renseignements nominatifs doit être faite sont prescrites par règlement du gouvernement. Le présent article ne s'applique pas à une enquête de nature judiciaire, ni à une enquête ou à un constat faits par une personne qui, en vertu de la loi, est chargée de prévenir, détecter ou réprimer le crime ou les infractions aux lois.




5. Limiter l'accès aux renseignements personnels

articles 62 et 76

La loi prévoit qu'un renseignement personnel ne sera accessible qu'aux seules personnes ayant la qualité pour le recevoir au sein d'un organisme public lorsque ce renseignement est nécessaire à l'exercice de leurs fonctions. Partant du fait qu'un renseignement personnel est confidentiel, il vous revient d'élaborer les mécanismes internes appropriés afin d'éviter que tous aient accès sans restriction à l'ensemble des renseignements disponibles.

Vous devez déterminer quels renseignements sont jugés indispensables au regard des tâches et des fonctions à accomplir par chaque membre de votre personnel. Ces privilèges d'accès sont identifiés de façon conjointe par les autorités, les gestionnaires et les ressources humaines en fonction des renseignements et des dossiers spécifiques auxquels chaque employé doit référer dans l'exécution de ses tâches. Rappelons que la nécessité d'accès vise à éviter que des personnes, étant par ailleurs habilitées à prendre connaissance d'un renseignement personnel, ne le fassent à titre gratuit ou par simple curiosité.

CONCRÈTEMENT

- 5.1 **Vous inscrivez dans la déclaration de fichier correspondante les catégories d'employés (agents de bureau, agents de recherche, conseillers, analystes en informatique, etc.) qui doivent recourir aux renseignements personnels.**
 - 5.1.1 **Les mandats, tâches ou fonctions accomplis par ces catégories d'emploi au sein de l'organisme rendent indispensable l'utilisation de chaque renseignement personnel.**
 - 5.2.1 **La fréquence d'utilisation des renseignements personnels correspond aux mandats attribués à ces catégories d'employés.**
- 5.2 L'accès aux renseignements personnels a été restreint dans le temps aux seuls moments requis.
- 5.3 Vous définissez la portée des privilèges d'accès (lecture, écriture, suppression, etc.) selon la définition de tâches des employés.
- 5.4 Les renseignements personnels destinés à des fins d'usage interne (voir 2.7) ne sont accessibles qu'aux seules personnes ayant la qualité pour les recevoir, au moment où ces renseignements leur sont nécessaires.
-  5.5 Vous construisez des jeux de données fictives ou anonymes lors de la formation des nouveaux employés.
-  5.6 Vous construisez des jeux de données fictives ou anonymes dans les environnements de développement (unitaire, fonctionnel, intégration, etc.) ou d'entretien d'un système.
-  5.7 Vous imposez aux informaticiens (administrateurs de réseau, administrateurs de base de données, libraires, etc.) un accès limité aux stricts renseignements personnels nécessaires.

En se rappelant que...

1. En dépit du mouvement de concentration des traitements et des données qui s'opère au sein des organisations publiques, la gestion des renseignements personnels ne doit pas s'opposer à l'idée du cloisonnement de l'information qui sous-tend la Loi sur l'accès comme moyen privilégié de garantir la confidentialité des renseignements personnels.
2. Une utilisation conséquente des technologies de l'information doit, par le biais d'une analyse de risques, contrôler la facilité avec laquelle elles permettent la dissémination, la duplication ou le partage des renseignements personnels, multipliant par le fait même les probabilités d'accès non autorisés aux données confidentielles, les risques de mauvais usages, de fuites ou de péremption de l'information.

6. Requérir le consentement à la communication entre organismes publics

articles 53 et 59

Un renseignement personnel demeure inaccessible tant que la personne concernée n'a pas consenti à sa divulgation⁴. Par conséquent, seuls les organismes que la personne concernée autorise auront accès à ses renseignements personnels. Le consentement concerne strictement la communication de renseignements personnels; il doit être formulé de manière manifeste, libre, éclairée, spécifique, limitée dans le temps et peut être résilié à tout moment.

Le droit à la vie privée sous-entend qu'une personne dispose d'un certain contrôle sur la circulation des renseignements la concernant. Vous devez donc vous assurer qu'une information personnelle ne pourra circuler sans l'autorisation préalable de la personne concernée, en évaluant notamment les moyens par lesquels vous obtenez ce consentement, les limites que vous lui attribuez et l'usage que vous en faites.

CONCRÈTEMENT

6.1 Vous pouvez démontrer que le consentement à la communication des personnes concernées est :

- Manifeste — attesté par un document (technologique ou papier);
- Libre — exprimé sans conditions, contraintes, menaces ou promesses;
- Éclairé — formulé en ayant conscience de sa portée;
- Spécifique — autorisant la communication d'un renseignement personnel donné, à des personnes données, à des fins données et à un moment donné;
- Limité dans le temps — valide pour la durée requise à la réalisation des fins pour lesquelles il est demandé.



- 6.2 Vous identifiez les différentes façons d'obtenir le consentement à la communication auprès de la personne concernée : en sa présence, par Internet, par la poste ou par d'autres voies.
- 6.3 Le consentement à la communication provient directement de la personne concernée.
- 6.4 Vous conservez les preuves de consentement à la communication et les échangez entre parties communicantes.
- 6.5 Vous validez la signature du consentement à la communication.
- 6.6 Lorsqu'il y a communication de renseignements personnels, l'organisme receveur satisfait au critère de *nécessité* dont il est question aux principes 0 et 5.
- 6.7 Vous déterminez dans quelles circonstances et de quelle manière communiquer un renseignement personnel à un autre organisme.
- 6.8 Si vous avez recours à des services externes pour la gestion spécifique de renseignements personnels, vous vous assurez que la protection des renseignements personnels chez ce prestataire de services répondra à vos exigences, qu'il y ait ou non communication de renseignements au sens de l'article 67.2 de la Loi sur l'accès.
- 6.9 Toutes les communications de renseignements personnels sans consentement sont inscrites au registre tenu à cette fin, incluant celles effectuées dans le cadre de mandats à l'externe et pour lesquels vous disposez d'une entente écrite qui

⁴ Certaines exceptions précisées par la Loi sur l'accès autorisent la communication de renseignements personnels sans le consentement préalable des personnes concernées (voir les articles 59, 59.1, 67, 67.1, 67.2, 68 et 68.1).

précise les dispositions légales et les mesures qui s'appliquent aux renseignements personnels communiqués (article 67.2).

En se rappelant que...

1. Le consentement à la communication vient autoriser la circulation d'un renseignement personnel entre organismes publics dans la mesure où ce renseignement est nécessaire aux attributions de ces organismes ou à la mise en œuvre d'un programme dont ils ont la gestion.
2. Les principes 2, 5 et 6 reprennent chacun à leur manière l'idée que la dispersion des renseignements personnels et le cloisonnement administratif des organismes détenant ces mêmes renseignements représentent les meilleurs gages de confidentialité. Cloisonnement et dispersion évitent que des profils sur les individus ne puissent être dressés par l'État et constituer ainsi une réelle menace à la reconnaissance des droits des individus. Le recours obligatoire au consentement à la communication doit être perçu comme un contrôle favorisant non pas la propagation des renseignements personnels, mais bien le maintien de leur répartition.


7. Assurer la qualité des renseignements personnels

article 72

Un renseignement personnel doit être maintenu à jour, être exact et complet afin de servir adéquatement aux fins pour lesquelles il a été recueilli. Vous devez donc identifier préalablement les renseignements personnels devant être mis à jour et consigner par la suite les dernières dates auxquelles ils auront été rectifiés. De cette manière, les renseignements personnels évolueront tout au long de leur cycle de vie conformément à la situation des personnes concernées.

Du fait des décisions que vous êtes appelés à prendre au sujet des personnes, il importe que la détention de renseignements personnels au sein de votre organisme respecte certaines obligations particulières. En outre, la collecte de tout nouveau renseignement personnel, rendue nécessaire pour des raisons de mise à jour, doit être conforme au principe sur la limitation de la collecte énoncé antérieurement.

CONCRÈTEMENT

- 7.1 Vous savez depuis combien de temps chaque renseignement personnel a été recueilli.
- 7.2 Vous connaissez la fréquence d'utilisation de chaque renseignement personnel.
- 7.3 Vous identifiez les renseignements personnels qui nécessitent une mise à jour.
- 7.4 Vous établissez des mécanismes pour gérer les mises à jour d'un renseignement personnel au cours de son cycle de vie.
-  7.5 Vous établissez des mécanismes pour gérer les mises à jour d'un renseignement personnel dupliqué ou répliqué (p. ex. sites miroirs).
- 7.6 La fréquence des mises à jour des renseignements personnels respecte leur fréquence d'utilisation (p. ex. un traitement annuel unique ne justifierait pas *a priori* des mises à jour mensuelles).
- 7.7 Un renseignement personnel est mis à jour par des employés attitrés et selon des modalités convenues.
- 7.8 Les mises à jour par échange de renseignements personnels sans consentement sont préalablement autorisées par la Commission, par des ententes ou par des dispositions légales particulières.
- 7.9 Vous vous assurez qu'une demande de modification d'un renseignement personnel proviendra bien de la personne concernée.







8. Garantir la sécurité des renseignements personnels

articles 53, 69 et 76

Des mesures de protection appropriées doivent assurer efficacement la sécurité d'un renseignement personnel, autant lors de sa mise en circulation⁵ que pendant toute la durée de sa détention. Vous devez préserver simultanément la confidentialité, la disponibilité et l'intégrité⁶ d'un renseignement personnel par le biais de moyens proportionnels aux conséquences possibles de sa divulgation.









Protection des renseignements personnels et sécurité informatique ne s'avèrent pas synonymes. D'une part, si certaines mesures de sécurité contribuent au respect de la confidentialité, d'autres en revanche constituent de véritables intrusions dans la vie privée des personnes. Il vous revient de déterminer au préalable si les contrôles que vous envisagez s'accordent avec le droit à la vie privée des utilisateurs. D'autre part, une mesure de sécurité efficace peut être insuffisante pour assurer la protection des renseignements personnels. Une transmission électronique, par exemple, peut être sécurisée de façon à préserver le caractère confidentiel de son contenu, mais être acheminée à une personne non autorisée à accéder aux renseignements qui y figurent. D'où le besoin d'évaluer la pertinence et l'efficacité des moyens de sécurité mis en œuvre afin de réserver aux renseignements personnels un usage qui respecte la finalité de leur collecte.

CONCRÈTEMENT

-  8.1 Vous établissez des mesures de sécurité applicables tout au long du cycle de vie d'un renseignement personnel, de sa collecte à sa destruction en passant par ses différentes utilisations. À titre indicatif :
 - mesures physiques : contrôles d'accès aux salles de serveurs, aux salles de câblage, au système d'alarme, etc.
 - mesures technologiques : identifiants et mots de passe, chiffrement, coupe-feu, anonymisation, pseudonymisation, etc.
 - mesures administratives : autorisations sécuritaires, accès sélectif, formation des employés, ententes de non-divulgation, etc.
-  8.2 Vous informez de façon complète et non ambiguë le personnel concerné des mesures de surveillance et de contrôle dont il fait l'objet et vous lui indiquez l'identité des personnes autorisées à accéder aux informations issues de ces mesures, en précisant les circonstances dans lesquelles elles y accéderont.
-  8.3 Vous êtes en mesure d'expliquer les mesures de sécurité inhérentes à votre prestation électronique de services en regard des risques encourus par les renseignements personnels.
-  8.4 Vous fixez des mesures de contrôle *a priori* touchant l'accès aux fichiers informatisés.
-  8.5 Vous gérez et contrôlez les accès à distance.
-  8.6 Vous gérez et contrôlez l'information qui circule par le biais des ordinateurs portables.

⁵ Voir l'article 34 de la Loi concernant le cadre juridique des technologies de l'information.

⁶ Voir la Directive sur la sécurité de l'information numérique et des échanges électroniques dans l'administration gouvernementale.

-  8.7 Vous contrôlez par des mesures particulières la sécurité des extrants : extractions, copies, impressions, copies de sécurité, notes personnelles.
-  8.8 Vous cryptez d'une manière sûre les renseignements personnels qui doivent être communiqués.
-  8.9 Si votre projet requiert une identification à distance, votre procédé d'authentification vous permet de valider avec une assurance suffisante l'identité de la personne avec qui vous communiquez, considérant la sensibilité des renseignements personnels engagés tout au long de la communication.
-  8.10 Vous adoptez des mesures vous garantissant l'intégrité des renseignements personnels communiqués.
-  8.11 Vous vous assurez que tout prestataire de services agissant à titre d'intermédiaire dans une communication de renseignements personnels fournira un niveau de sécurité égal ou supérieur au vôtre à l'égard des supports, de la technologie et du lieu d'entreposage des renseignements personnels.
-  8.12 Vous journalisez tous les accès aux renseignements personnels afin d'être en mesure d'identifier, si nécessaire, quels utilisateurs y ont eu accès pendant une période déterminée. Vous contrôlez rigoureusement l'accès aux fichiers de journalisation.
-  8.13 Vous analysez les fichiers de journalisation de manière anonyme et à intervalles réguliers, en vous souciant d'ajuster et de varier les critères d'analyse.
-  8.14 Vous vous préparez aux cyberattaques provenant tant de l'interne que de l'externe.

En se rappelant que...

1. Le cryptage ou chiffrement constitue une mesure de sécurité particulière pour préserver temporairement la confidentialité d'un renseignement personnel durant sa transmission ou son entreposage. Un renseignement personnel crypté demeure confidentiel du fait que sa transformation reste passagère et réversible.
2. Un fichier ne peut être qualifié d'anonyme lorsqu'il est possible par un moyen ou un autre d'identifier une personne, lorsqu'un moyen de déduction logique permet de reconstituer une identité à partir de plusieurs renseignements anonymes, lorsque le mécanisme d'anonymisation est réversible ou lorsqu'un pseudonyme remplace un identifiant. Faute d'anonymat, les obligations de protection conférées par la loi aux renseignements personnels demeurent applicables.


9. Assurer les droits d'accès et de rectification

articles 83, 84 et 89

Un renseignement personnel doit pouvoir être accessible et rectifié. Vous devez informer toute personne qui en fait la requête de l'existence des renseignements personnels qui la concernent et de la possibilité de les consulter ou d'en obtenir copie, quel que soit le support.

Vous devez identifier quels dispositifs ont été prévus pour répondre adéquatement aux demandes formulées par les personnes concernées relativement à l'accès aux renseignements personnels, de même qu'à leur rectification.

CONCRÈTEMENT

- 9.1 **Vous prévoyez des mécanismes pour rendre facilement accessibles à une personne tous les renseignements personnels la concernant, de façon à lui permettre de les consulter et de les corriger dans la mesure prévue par la loi.**
- 9.2 Vous examinez l'identité des auteurs de demandes d'accès ou de rectification, que ces demandes se fassent à distance ou en personne.
- 9.3 Les renseignements personnels sont rendus disponibles aux personnes concernées sur des supports facilitant leur obtention (papier ou technologique).
-  9.4 Vous propagez dans les fichiers concernés (p. ex. duplicata) toute rectification apportée à un renseignement personnel.






10. Limiter la durée de conservation des renseignements personnels

articles 73 et 102.1

Vous êtes tenus de détruire irréversiblement tout renseignement personnel lorsque l'objet pour lequel il a été recueilli est accompli. Cette obligation, qui vise à réduire la probabilité que des renseignements personnels soient utilisés à des fins autres que celles auxquelles ils étaient destinés, est assortie d'une réserve importante : la *Loi sur les archives*, et plus précisément, le calendrier de conservation de l'organisme.

Un organisme ne peut conserver les renseignements personnels qu'il détient au-delà des délais prescrits par le calendrier de conservation, quel que soit le support utilisé. Vos échéances de conservation doivent tenir compte des demandes d'accès que pourrait invoquer la personne concernée à la suite des décisions prises à son sujet, mais se limiter cependant au strict intervalle de temps requis pour que le renseignement personnel puisse jouer le rôle auquel il est destiné.

CONCRÈTEMENT

-  10.1 **Vous fixez un calendrier de conservation à tous les renseignements personnels que vous détenez, quels que soient leurs supports.**
-  10.2 La destruction d'un renseignement personnel entraîne celle de toutes ses copies.
-  10.3 Vous détruisez vos renseignements personnels de manière irréversible.
-  10.4 Même si les renseignements personnels sont versés dans un fichier de conservation distinct (p. ex. un entrepôt de données), vous les soumettez à un calendrier de conservation et les détruisez à terme.
-  10.5 Durant leur conservation, vous rendez les renseignements personnels anonymes ou masqués par un pseudonyme pour mieux en préserver la confidentialité.

CONCLUSION

La Loi sur l'accès formule à l'administration publique des devoirs et des obligations de protection bien spécifiques envers les citoyens et citoyennes qui fournissent des renseignements personnels. Afin de faciliter et d'encourager l'adoption d'initiatives respectueuses de la loi dans le développement des systèmes d'information, la Commission a jugé opportun de rédiger le présent guide à l'attention des ministères et organismes publics.

Chacun des dix principes décrits dans les pages précédentes énonce un des fondements de la Loi sur l'accès en matière de protection des renseignements personnels. Aucun ne peut être jugé facultatif, secondaire ou désuet. La concrétisation de ces principes, en revanche, connaît depuis vingt ans une transformation constante et rien ne laisse croire qu'il en sera autrement dans le futur.

Pour cette raison, ce guide visait à faire connaître aux concepteurs, aux gestionnaires et aux responsables de la protection des renseignements personnels, les bases sur lesquelles la Commission s'appuie pour évaluer la conformité des systèmes d'information qui lui sont soumis. L'objectif sera véritablement atteint dans la mesure où le guide aura fait valoir avec une teinte plus actuelle l'importance des mesures de sécurité et de confidentialité applicables aux renseignements personnels.

Vos commentaires sont attendus!

*Faites-nous les parvenir à l'adresse cai.communications@cai.gouv.qc.ca, en inscrivant **GUIDE** dans l'objet du message.*