GUIDE D'APPLICATION CONCERNANT LES RÈGLES ENCADRANT LA GOUVERNANCE À L'ÉGARD DES RENSEIGNEMENTS PERSONNELS

OCTOBRE 2023

Votre gouvernement

Québec

Cette publication a été réalisée par Direction de l'accès à l'information
et de la protection des renseignements personnels
en collaboration avec la Direction des communications.

Une version adaptée de ce document est offerte en ligne.
Si vous éprouvez des difficultés techniques, veuillez communiquer
avec la Direction de l'accès à l'information et de la protection
des renseignements personnels au daiprp@mce.gouv.qc.ca.

Pour plus d'information :

Direction des communications
du ministère du Conseil exécutif
2e étage, secteur 800
875, Grande Allée Est
Québec (Québec) G1R 4Y8

Téléphone : 418 781-9530
Courriel : communic@mce.gouv.qc.ca
Site Web : www.quebec.ca/gouvernement/ministere/conseil-executif

Dépôt légal – Octobre 2023
Bibliothèque et Archives nationales du Québec
ISBN 978-2-550-95590-0 (version électronique)

TABLE DES MATIÈRES

INTRODUCTION

En vertu de l'article 63.3 de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (RLRQ, chapitre A-2.1, ci-après « Loi sur l'accès »), un organisme public doit publier sur son site Internet des règles encadrant sa gouvernance à l'égard des renseignements personnels (ci-après « règles de gouvernance »). Ces règles doivent être approuvées par son comité sur l'accès à l'information et la protection des renseignements personnels[1].

Notons également que l'exigence d'établir des règles de gouvernance est intimement associée au principe de responsabilité prévu à l'article 52.2 de la Loi sur l'accès. En vertu de cet article, un organisme public est responsable de la protection des renseignements personnels qu'il détient.

Afin d'aider les organismes publics à se conformer à ses exigences légales, le Secrétariat à la réforme des institutions démocratiques, à l'accès à l'information et à la laïcité a préparé le présent guide.

OBJECTIFS DU GUIDE

Le présent guide doit être considéré comme un document de soutien qui sert à alimenter la réflexion d'un organisme public dans l'élaboration de ses règles de gouvernance. Ce guide n'est pas prescriptif ni exhaustif, et son utilisation ne peut pas garantir la conformité à la loi.

Ce guide se concentre sur les règles de gouvernance en lien avec la protection des renseignements personnels. Néanmoins, un organisme public peut mettre en place des règles de gouvernance qui impliqueront également d'autres domaines connexes à la protection des renseignements personnels (ex. : sécurité de l'information, gestion des risques, gestion documentaire, etc.). Une approche multidisciplinaire peut contribuer à renforcer la protection des renseignements personnels.

1. Pour les organismes publics exclus de l'obligation de former le comité sur l'accès à l'information et la protection des renseignements personnels, conformément au Règlement excluant certains organismes publics de l'obligation de former un comité sur l'accès à l'information et la protection des renseignements personnels, les règles doivent être approuvées par le responsable de la protection des renseignements personnels ou, dans le cas d'une municipalité, d'un ordre professionnel ou d'un centre de services scolaire, par le directeur général (article 4 du règlement précédemment mentionné).

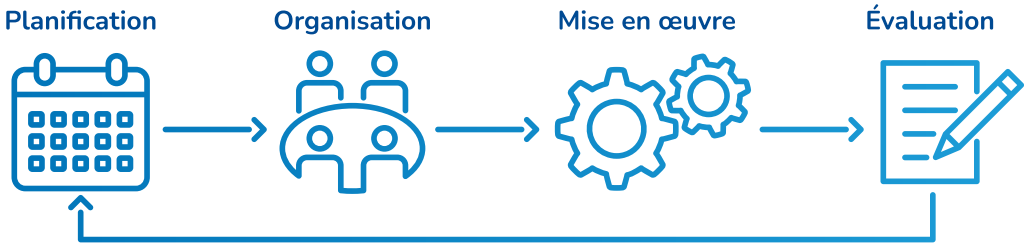
COMMENT ÉTABLIR LES RÈGLES DE GOUVERNANCE DE VOTRE ORGANISATION ?

Chaque organisme public doit établir des règles de gouvernance qui sont propres au contexte dans lequel il évolue. Il doit donc adapter les éléments de ce guide à sa propre réalité. En effet, plusieurs éléments peuvent influencer les règles de gouvernance d'un organisme public, tels que sa taille, ses activités, ses ressources, sa clientèle, les renseignements personnels qu'il détient, les traitements de renseignements personnels effectués[2], le ou les régimes juridiques applicables, les normes qu'il applique, etc.

À titre d'exemple, un organisme public qui effectue très peu de communications de renseignements personnels dans le cadre de ses activités pourrait encadrer l'ensemble des communications dans un seul document. Un autre organisme public, qui effectue régulièrement des communications de renseignements personnels, pourrait décider de mettre en place des directives précises pour différents types de communications (ex. : communications à des fins d'étude, de recherche ou de production de statistiques, communications nécessaires à l'exercice d'un mandat ou à l'exécution d'un contrat de service ou d'entreprise, etc.). Un organisme public qui détient des renseignements personnels pour des attributions différentes pourrait adapter ses règles de gouvernance en fonction de ses attributions.

Par ailleurs, certains thèmes suggérés dans ce guide pourraient ne pas être pertinents pour certains organismes publics. Par exemple, un organisme public qui n'aura pas recours à l'anonymisation de renseignements personnels ou à la biométrie n'aura pas besoin d'élaborer des règles de gouvernance concernant ces thèmes.

Pour établir les règles de gouvernance, une démarche en quatre étapes est suggérée[3].



2. Un traitement de renseignements personnels fait référence aux opérations réalisées impliquant des renseignements personnels (ex. : collecte, utilisation, communication, conservation, destruction, etc.).

3. Cet aspect s'inspire du document « Cadre de gouvernance de la protection des renseignements personnels (PRP) – Loi 25 » produit par l'Association des professionnels en accès à l'information et en protection de la vie privée (AAPI).

Planification

Un organisme public devrait d'abord faire la planification de ses règles de gouvernance. Pour ce faire, il devrait connaître dans quel environnement il évolue en matière de protection des renseignements personnels. À cette étape, il est donc suggéré d'identifier les renseignements personnels détenus par l'organisme public et de les classifier, d'identifier les traitements de renseignements personnels et les exigences légales ainsi que les normes s'appliquant aux renseignements personnels détenus.

Ces éléments permettront notamment à l'organisme public de déterminer ses objectifs et ses orientations stratégiques en matière de protection des renseignements personnels et d'organiser leur protection au sein de l'organisme.

Même s'il est préférable de réaliser l'ensemble de ces éléments pour établir des règles de gouvernance, il est possible d'établir de telles règles sans les avoir tous complétés. En effet, en fonction de la réalité de chaque organisme public, il est possible que ces travaux puissent s'étaler sur une période plus au moins longue. De plus, il s'agit d'éléments qui doivent idéalement être effectués en continu. La démarche suggérée étant un cycle, les règles de gouvernance peuvent donc être bonifiées à chaque cycle en fonction de l'avancement des travaux.

Identifier les renseignements personnels détenus et les classifier

Un organisme public devrait procéder à l'inventaire des renseignements personnels qu'il détient, que leur conservation soit assurée par l'organisme ou par un tiers. Il devrait bien documenter le tout en décrivant le renseignement personnel, en précisant l'endroit où il est stocké ou conservé, en indiquant l'unité administrative responsable, en spécifiant, le cas échéant, s'il s'agit d'un renseignement personnel sensible ou à caractère public, etc. À noter que les renseignements personnels peuvent être regroupés lorsque les informations les concernant sont identiques. Un processus devrait être mis en place pour réaliser cet exercice en continu, ou du moins à intervalle régulier (ex. : aux deux ans).

Cet exercice se distingue de l'inventaire des fichiers de renseignements personnels prévu à l'article 76 de la Loi sur l'accès. En effet, il ne s'agit pas d'identifier les fichiers de renseignements personnels, mais l'ensemble des renseignements personnels détenus par l'organisme public. Ces deux démarches se veulent complémentaires.

Par ailleurs, cet exercice pourrait être une excellente occasion d'effectuer une évaluation des renseignements personnels détenus par l'organisme public.

Par exemple, l'organisme public pourrait vérifier si les renseignements personnels lui sont toujours nécessaires.

Après avoir identifié les renseignements personnels détenus, l'organisme public devrait procéder à leur classification[4]. Cet élément devrait être ajouté à l'inventaire des renseignements personnels, ce qui permettra d'identifier rapidement le niveau de protection à accorder aux renseignements et, ainsi, à mieux définir les processus et les mesures de protection et de sécurité à mettre en place pour les protéger.

En ce qui concerne les organismes publics assujettis à la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (RLRQ, chapitre G-1.03), ils devront appliquer le modèle de classification prévu à l'article 12.6 de cette loi. Un organisme public qui n'est pas assujetti à cette loi pourrait quand même s'en inspirer pour réaliser sa classification.

Identifier les traitements de renseignements personnels

Afin d'avoir un portrait complet de la situation et de favoriser sa conformité aux exigences légales, un organisme public devrait identifier l'ensemble des traitements de renseignements personnels au sein de son organisation.

Cet exercice devrait notamment préciser les différents traitements de renseignements personnels, les renseignements ou les catégories de renseignements personnels traités, les objectifs poursuivis par ces traitements, les catégories de personnes de l'interne ou de l'externe qui traitent ces renseignements personnels, les délais de conservation et le flux des renseignements personnels de leur point d'origine jusqu'à leur destination (ex. : circulation à l'interne, communication à un autre organisme public, communication à l'extérieur du Québec, etc.).

Cela peut être colligé, par exemple, dans un registre ou dans un ou plusieurs schémas. Cet exercice permet notamment à l'organisme public d'identifier où sont ses plus grands enjeux en matière de protection des renseignements personnels et, ainsi, définir les processus à mettre en place pour mieux les contrôler.

Par exemple, un organisme public, constatant qu'il effectue de nombreuses collectes de renseignements personnels, pourrait décider d'inscrire dans une directive un processus de validation de toutes nouvelles démarches de collectes de renseignements personnels auprès de la personne responsable de la protection des renseignements personnels. Ce processus permettrait de s'assurer, notamment, de recueillir uniquement les renseignements personnels qui sont nécessaires à l'exercice de ses attributions ou à la mise en œuvre d'un programme dont il a la gestion.

4. Attribution d'une mention qui permet de caractériser la valeur et l'importance stratégique d'une donnée détenue par une organisation et, conséquemment, le niveau de protection à lui accorder (source : Office québécois de la langue française).

Identifier les exigences légales s'appliquant aux renseignements personnels détenus

En plus de la Loi sur l'accès, un organisme public peut être assujetti à d'autres exigences légales en lien avec les renseignements personnels qu'il détient. Il peut s'agir de dispositions spécifiques d'une loi ou de régimes particuliers (ex. : renseignements de santé et de services sociaux, dossier fiscal, etc.).

Un organisme public devrait connaître l'environnement légal en lien avec les renseignements personnels qu'il détient. Ainsi, il pourra s'assurer que les règles de gouvernance permettent de respecter l'ensemble des exigences légales.

Identifier les normes s'appliquant aux renseignements personnels détenus

Outre les exigences légales, certaines normes peuvent s'appliquer aux renseignements personnels détenus par un organisme public. Ce dernier devrait identifier ces normes afin d'en tenir compte dans l'élaboration de ses règles de gouvernance.

Par exemple, un organisme public pourrait s'être engagé à respecter certaines clauses dans le cadre d'un contrat ou d'une entente en lien avec la collecte ou la communication de renseignements personnels. Il pourrait également avoir à considérer des documents normatifs externes qui concernent la protection des renseignements personnels (ex. : lignes directrices de la Commission d'accès à l'information). Il est également possible que des documents normatifs internes ou gouvernementaux contiennent certaines règles à respecter par l'organisme public (ex. : Directive gouvernementale sur la sécurité de l'information). Par ailleurs, un organisme public pourrait souhaiter respecter certaines normes reconnues pour contribuer à la protection des renseignements personnels (ex. : normes ISO).

Déterminer les objectifs et les orientations stratégiques en matière de protection des renseignements personnels

Après avoir réalisé les démarches lui permettant de mieux comprendre son environnement, un organisme public devrait déterminer ses objectifs et ses orientations stratégiques en matière de protection des renseignements personnels. Un exercice de cette nature pourrait se faire sous la responsabilité du comité sur l'accès à l'information et la protection des renseignements personnels et il devrait nécessiter la participation de tous les intervenants qui peuvent être concernés par la protection des renseignements personnels.

Il devrait également déterminer les principaux rôles et responsabilités des différents acteurs au sein de l'organisme (ex. : comité sur l'accès à l'information et la protection des renseignements personnels, personne responsable de la protection des renseignements personnels, membres du personnel[5], etc.).

5. Dans le cadre de ce guide, les termes « membres du personnel » incluent les dirigeants, les gestionnaires, les employés, les étudiants, les stagiaires et toute autre personne relevant de l'organisme public.

Ces éléments devraient être inscrits dans une politique en matière de protection des renseignements personnels.

Politique en matière de protection des renseignements personnels et plan d'action

La politique en matière de protection des renseignements personnels est un document important pour un organisme public. Elle permet de décrire les engagements de l'organisme public en cette matière. De cette politique découleront normalement d'autres documents (ex. : directives, guides, etc.) qui permettront de mieux définir les règles et les processus à respecter par les membres du personnel de l'organisme public. Cette politique devrait notamment préciser :

- les objectifs et les orientations stratégiques de l'organisme public en lien avec sa mission et la protection des renseignements personnels ;
- les principes directeurs en lien avec le cycle de vie des renseignements personnels sur lesquels devront s'appuyer tous les documents qui découleront de la politique ;
- les principaux rôles et responsabilités (qui pourront être détaillés davantage dans les documents qui découleront de la politique).

Un organisme public peut également mettre en place un plan d'action afin de déterminer ses priorités en matière de protection des renseignements personnels (ex. : réalisation d'activités ou ajustements qui contribueront à améliorer la protection des renseignements personnels). Un plan d'action permet d'identifier les actions prioritaires et d'établir un échéancier stratégique pour les mettre en œuvre en fonction des ressources disponibles. Une reddition de comptes concernant ce plan d'action devrait être effectuée.

Principe de responsabilité

En vertu de l'article 52.2 de la Loi sur l'accès, un organisme public est responsable de la protection des renseignements personnels qu'il détient, que leur conservation soit assurée par l'organisme ou par un tiers. En vertu de ce principe de responsabilité, un organisme public doit être en mesure de prouver, en tout temps, qu'il respecte ses obligations en matière de protection des renseignements personnels. Pour ce faire, un organisme public doit être en mesure de rendre compte de sa conformité en produisant une documentation exhaustive décrivant l'ensemble des mesures qu'il applique et en obtenant les documents nécessaires permettant de démontrer qu'il respecte ses obligations[6].

Les règles de gouvernance devraient donc mettre en place les processus nécessaires pour que l'organisme public puisse démontrer le respect de ses obligations en matière de protection des renseignements personnels.

6. Pour des exemples de documents qui permettent à un organisme public de démontrer qu'il se conforme à la Loi sur l'accès, vous pouvez consulter le document *Principe de responsabilité d'un organisme public à l'égard de la protection des renseignements personnels.*

Par exemple, un organisme public devrait instaurer un processus pour conserver les évaluations des facteurs relatifs à la vie privée qu'il réalise, les consentements qu'il obtient, les analyses de la nécessité de la collecte d'un renseignement personnel qu'il effectue, etc.

Par ailleurs, un organisme public devrait mettre en place des mécanismes de reddition de comptes à l'interne et de contrôle des mesures prises en matière de protection des renseignements personnels (ex. : vérification interne).

Organisation

Après avoir réalisé sa planification, un organisme public devra s'atteler à l'organisation de ses activités en matière de protection des renseignements personnels.

L'organisation consiste à déterminer les rôles et les responsabilités des différents acteurs au sein de l'organisme public en lien avec les traitements de renseignements personnels et à définir les règles et les processus concernant ces traitements. Cela permettra notamment aux membres du personnel de l'organisme public de savoir ce qu'ils doivent faire dans le cadre d'un traitement de renseignements personnels afin de respecter les exigences légales, les normes et les mesures définies par l'organisme public. Un exercice de cette nature pourrait se faire sous la responsabilité du comité sur l'accès à l'information et la protection des renseignements personnels et il devrait nécessiter la participation de tous les intervenants qui peuvent être concernés par la protection des renseignements personnels (ex. : responsable de la protection des renseignements personnels, responsable de la sécurité de l'information, responsable de la gestion documentaire, membres du personnel, unité administrative détentrice des renseignements personnels, etc.).

Les règles de gouvernance de l'organisme public seront donc définies dans le cadre de l'étape de l'organisation, à l'exception de la politique en matière de protection des renseignements personnels.

Définir les rôles et responsabilités

Les rôles et responsabilités des différents acteurs au sein de l'organisme public doivent être mentionnés dans les différents documents qui constitueront les règles de gouvernance de l'organisme public.
À ce moment, les rôles et responsabilités devront être plus détaillés que ceux mentionnés dans la politique en matière de protection des renseignements personnels. Avant de les mentionner dans les règles de gouvernance, un organisme public devrait avoir fait une réflexion globale sur les rôles et responsabilités à confier aux différents acteurs en matière de protection des renseignements personnels.

Par exemple, il est possible de confier plus de responsabilités au comité sur l'accès à l'information et la protection des renseignements personnels et à la personne responsable de la protection des renseignements personnels que celles prévues par la Loi sur l'accès. Par exemple, le comité pourrait être consulté concernant des questions complexes sur l'interprétation de la Loi sur l'accès et le responsable pourrait participer à la validation des contrats et des ententes comprenant une communication de renseignements personnels.

Par ailleurs, la protection des renseignements personnels relève de l'ensemble de l'organisme public. Il faut donc confier certaines responsabilités, sauf celles prévues par la loi, à d'autres acteurs que le comité et la personne responsable de la protection des renseignements personnels (ex. : unité administrative détentrice des renseignements personnels, responsable de la sécurité de l'information, responsable de la gestion documentaire, affaires juridiques, responsable de projet, membres du personnel, etc.).

Par exemple, le responsable d'un projet pourrait coordonner les travaux en lien avec la réalisation d'une évaluation des facteurs relatifs à la vie privée.

L'organisme public doit définir les rôles et responsabilités en considérant notamment sa taille, ses activités, ses ressources, les clientèles servies, les renseignements personnels qu'il détient, les traitements de renseignements personnels effectués, etc. Il doit également s'assurer de la cohérence de ces rôles et responsabilités avec ceux en lien avec des domaines connexes à la protection des renseignements personnels (ex. : sécurité de l'information).

Thèmes à aborder et éléments de contenu

La présente sous-section suggère différents thèmes qui devraient être couverts par les règles de gouvernance d'un organisme public. Ces thèmes sont liés aux différentes exigences légales qu'un organisme public doit respecter pour être conforme à la Loi sur l'accès[7]. En effet, les règles de gouvernance servent à encadrer la protection des renseignements personnels au sein d'un organisme et à indiquer aux membres du personnel ce qu'ils doivent faire dans le cadre d'un traitement de renseignements personnels afin de respecter les exigences légales, les normes et les mesures définies par l'organisme public.

Cependant, comme mentionné au début du guide, certains thèmes suggérés pourraient ne pas être pertinents pour certains organismes publics. D'ailleurs, les thèmes de la présente sous-section sont subdivisés en deux, soit ceux qui s'appliquent normalement à tous les organismes publics et ceux qui ne s'appliquent pas nécessairement à tous les organismes publics. Ceci est mentionné à titre indicatif seulement. Chaque organisme public doit faire sa propre évaluation selon le contexte dans lequel il évolue.

Par ailleurs, il n'est pas nécessaire de faire un document pour chaque thème ; il est possible de couvrir plusieurs thèmes en un seul. Il pourrait même être possible de couvrir l'ensemble de ces thèmes en un seul document, par exemple, dans le cas d'un petit organisme public qui détient peu de renseignements personnels. Il est également possible d'intégrer un thème dans un document normatif existant (ex. : un organisme public pourrait insérer le processus de traitement des plaintes relatif à la protection des renseignements personnels dans sa politique générale sur le traitement des plaintes). En fait, chaque organisme public peut établir sa propre stratégie pour l'organisation de ses règles de gouvernance. De plus, rappelons que chaque organisme public doit établir des règles de gouvernance qui sont propres au contexte dans lequel il évolue et doit donc adapter les éléments de ce guide à sa propre réalité.

Cette sous-section suggère également certains éléments de contenu qui devraient être inclus dans un document qui aborde les thèmes suggérés. Un organisme public devrait établir des règles et un processus avec des rôles et responsabilités pour ces éléments de contenu. Rappelons cependant que ce guide n'est pas prescriptif ni exhaustif.

7. Rappelons que les organismes publics peuvent être assujettis à d'autres exigences légales en matière de protection des renseignements personnels que celles prévues par la Loi sur l'accès et que les règles de gouvernance devraient en tenir compte. Par ailleurs, vous trouverez sur le site Internet du Secrétariat à la réforme des institutions démocratiques, à l'accès à l'information et à la laïcité différents documents pour aider les organismes publics à appliquer la Loi sur l'accès : Publications | Gouvernement du Québec (quebec.ca) et Protection des renseignements personnels | Gouvernement du Québec (quebec.ca).

Voici la liste des thèmes qui s'appliquent normalement à tous les organismes publics :

Collecte de renseignements personnels

Un organisme public qui recueille des renseignements personnels doit se conformer à différentes exigences légales (ex. : articles 64 et 65 de la Loi sur l'accès).

Éléments de contenu :

- Évaluation de la nécessité de la collecte ;
- Collecte pour un autre organisme public dans le cadre d'une collaboration (incluant l'évaluation des facteurs relatifs à la vie privée, l'entente et la transmission de celle-ci à la Commission d'accès à l'information) ;
- Informer les personnes concernées lors d'une collecte ;
- Répondre à une demande d'information adressée par une personne concernée.

Politique de confidentialité

Un organisme public qui recueille par un moyen technologique des renseignements personnels doit publier sur son site Internet et diffuser, par tout moyen propre à atteindre les personnes concernées, une politique de confidentialité rédigée en termes simples et clairs (article 63.4 de la Loi sur l'accès[8]).

Éléments de contenu :

- Évaluation de la nécessité de la collecte par un moyen technologique ;
- Règles concernant les témoins de connexion, pixels de suivis, etc. ;
- Détermination du contenu d'une politique de confidentialité ;
- Modification d'une politique de confidentialité ;
- Consultation du comité sur l'accès à l'information et la protection des renseignements personnels.

8. Il faudra également considérer le contenu et les modalités déterminés par règlement. Le projet Règlement sur les politiques de confidentialité des organismes publics recueillant des renseignements personnels par un moyen technologique a été publié par la Gazette officielle du Québec le 12 juillet 2023.

Accès aux renseignements personnels dans l'exercice des fonctions

Un organisme public doit s'assurer qu'un renseignement personnel est accessible uniquement aux personnes qui ont la qualité pour le recevoir lorsque ce renseignement est nécessaire à l'exercice de leurs fonctions (article 62 de la Loi sur l'accès).

Éléments de contenu :

- Gestion des accès (ex. : autorisation, révision, révocation, etc.) selon le type d'accès (ex. : accès physique, accès aux systèmes, à distance, etc.) ;
- Gestion des accès à privilèges (ex. : administrateur, superutilisateur, etc.) ;
- Journalisation des accès.

Utilisation des renseignements personnels

Sauf exception, un organisme public doit utiliser un renseignement personnel qu'aux fins pour lesquelles il a été recueilli, à moins d'obtenir le consentement de la personne concernée (article 65.1 de la Loi sur l'accès).

Éléments de contenu :

- Déterminer les fins pour lesquelles un renseignement personnel a été recueilli ;
- Utilisation avec le consentement de la personne concernée ;
- Utilisation sans le consentement de la personne concernée ;
- Inscription au registre prévu à l'article 67.3 de la Loi sur l'accès.

Communication de renseignements personnels

Un organisme public peut communiquer un renseignement personnel avec le consentement de la personne concernée. Toutefois, il peut communiquer un renseignement personnel sans le consentement de cette personne dans les cas prévus par la loi (article 59 de la Loi sur l'accès).

Éléments de contenu :

- Évaluation de la nécessité de communiquer un renseignement personnel ;
- Communication avec le consentement de la personne concernée ;
- Communication sans le consentement de la personne concernée ;
- Inscription au registre prévu à l'article 67.3 de la Loi sur l'accès.

Communication en vue de protéger une personne ou un groupe de personnes identifiable

Un organisme public peut communiquer un renseignement personnel, sans le consentement des personnes concernées, en vue de protéger une personne ou un groupe de personnes identifiable lorsqu'il existe un motif raisonnable de croire qu'un risque sérieux de mort ou de blessures graves, lié notamment à une disparition ou à un acte de violence, dont une tentative de suicide, menace cette personne ou ce groupe et que la nature de la menace inspire un sentiment d'urgence. La personne ayant la plus haute autorité au sein de l'organisme public doit, par directive, établir les conditions et les modalités suivant lesquelles les renseignements peuvent être communiqués par le personnel de l'organisme (article 59.1 de la Loi sur l'accès[9]).

Éléments de contenu :

- Évaluation de la nécessité de communiquer un renseignement personnel ;
- Conditions et modalités suivant lesquelles les renseignements peuvent être communiqués par le personnel de l'organisme ;
- Inscription dans un registre propre à l'article 59.1 de la Loi sur l'accès.

Communication de renseignements personnels lors d'un mandat ou à l'exécution d'un contrat de service ou d'entreprise

Un organisme public peut, sans le consentement de la personne concernée, communiquer un renseignement personnel à toute personne ou à tout organisme si cette communication est nécessaire à l'exercice d'un mandat ou à l'exécution d'un contrat de service ou d'entreprise confié par l'organisme public à cette personne ou à cet organisme (article 67.2 de la Loi sur l'accès).

Éléments de contenu :

- Évaluation de la nécessité de communiquer un renseignement personnel ;
- Inclure des exigences concernant la protection des renseignements personnels dans les documents d'appel d'offres ;
- Conclure un mandat ou un contrat par écrit avec les clauses requises sur le plan de la protection des renseignements personnels ;
- Obtenir les engagements de confidentialité ;
- Acquérir des avis concernant toute violation ou tentative de violation d'une obligation relative à la confidentialité ;
- Vérification de la protection des renseignements personnels auprès du mandataire, du fournisseur ou du prestataire de services ;
- Inscription au registre prévu à l'article 67.3 de la Loi sur l'accès.

9. Le libellé utilisé est celui de l'article 59.1 de la Loi sur l'accès, tel que modifié par la Loi sur les renseignements de santé et de services sociaux et modifiant diverses dispositions législatives. Avant l'entrée en vigueur de cette modification (date à fixer par le gouvernement), veuillez vous référer à la Loi sur l'accès.

Communication de renseignements personnels exigés par le Protecteur du citoyen ou par assignation, citation à comparaître, mandat ou ordonnance d'une personne ou d'un organisme ayant le pouvoir de contraindre à leur communication

Un organisme public doit répondre aux demandes de communication de documents ou de renseignements exigés par le Protecteur du citoyen ou par assignation, citation à comparaître, mandat ou ordonnance d'une personne ou d'un organisme ayant le pouvoir de contraindre à leur communication (paragraphe 3 de l'article 171 de la Loi sur l'accès).

Éléments de contenu :

- Réception d'une demande provenant du Protecteur du citoyen ou d'une personne ou d'un organisme ayant un pouvoir de contrainte ;
- Analyse de la demande pour déterminer les renseignements personnels à communiquer ;
- Procéder à la communication conformément à la demande (ex. : déposé au tribunal).

Conservation et destruction de renseignements personnels

Un organisme public doit veiller à ce que les renseignements personnels qu'il conserve soient à jour, exacts et complets pour servir aux fins pour lesquelles ils sont recueillis ou utilisés (article 72 de la Loi sur l'accès). Lorsque les fins pour lesquelles un renseignement personnel a été recueilli ou utilisé sont accomplies, l'organisme public doit le détruire, sous réserve de la Loi sur les archives (RLRQ, chapitre A-21.1) ou du Code des professions (RLRQ, chapitre C-26) (article 73 de la Loi sur l'accès).

Éléments de contenu :

- Établir les délais de conservation et le calendrier de conservation conformément à la Loi sur les archives ;
- Déterminer les mesures pour que les renseignements personnels soient à jour, exacts et complets pour servir aux fins pour lesquelles ils sont recueillis ou utilisés ;
- Définir les mesures pour conserver et détruire sécuritairement les renseignements personnels.

Inventaire et fichiers de renseignements personnels

Un organisme public doit établir et maintenir à jour un inventaire de ses fichiers de renseignements personnels (article 76 de la Loi sur l'accès).

Éléments de contenu :

- Établir les fichiers de renseignements personnels conformément à l'article 71 de la Loi sur l'accès ;
- Créer l'inventaire des fichiers de renseignements personnels conformément à l'article 76 de la Loi sur l'accès ;
- Maintenir à jour les fichiers et l'inventaire des fichiers.

Traitement d'une demande d'accès à des renseignements personnels ou d'une demande de rectification

Le responsable de la protection des renseignements personnels d'un organisme public doit donner suite à une demande de communication ou de rectification avec diligence et au plus tard dans les délais prévus par la Loi sur l'accès (article 98 de la Loi sur l'accès).

Éléments de contenu :

- Repérage des renseignements personnels visés par la demande ;
- Assistance pour identifier le document susceptible de contenir les renseignements recherchés ;
- Transmission de l'accusé de réception ;
- Traitement d'une demande d'accès, d'une demande de rectification, d'une demande d'accès en lien avec le droit à la portabilité, d'une demande d'accès concernant une personne décédée et d'une demande de rectification concernant une personne décédée ;
- Frais de transcription, de reproduction et de transmission des renseignements personnels ;
- Communication, dans les délais requis, de la décision du responsable de la protection des renseignements personnels ;
- Demande d'enregistrement d'une demande de rectification et communication d'une copie des renseignements personnels modifiés, d'une attestation de retrait des renseignements personnels ou de l'enregistrement ;
- Conservation des renseignements personnels faisant l'objet d'une demande, le temps requis pour permettre au demandeur d'épuiser ses recours ;
- Révision devant la Commission d'accès à l'information et appel.

Processus de traitement des plaintes relatives à la protection des renseignements personnels

Les règles de gouvernance d'un organisme public doivent prévoir un processus de traitement des plaintes relatives à la protection des renseignements personnels (article 63.3 de la Loi sur l'accès).

Éléments de contenu :

- Réception d'une plainte ;
- Consultation des intervenants concernés par la plainte et des ressources nécessaires pour analyser la plainte ;
- Traitement de la plainte et suivi auprès de la personne plaignante ;
- Le cas échéant, apporter les ajustements nécessaires à la suite de la plainte.

Gestion des consentements

Un consentement prévu à la Loi sur l'accès doit notamment être conforme à l'article 53.1 de la Loi sur l'accès[10].

Éléments de contenu :

- Établir dans quels cas un consentement est nécessaire et qui peut donner le consentement (ex. : titulaire de l'autorité parentale) ;
- Informations à communiquer pour obtenir un consentement ;
- Façons de s'assurer du respect des critères de validité d'un consentement ;
- Moyens à utiliser pour obtenir le consentement (ex. : formulaire papier, moyen technologique, etc.) ;
- Validation d'un consentement avant son utilisation ;
- Assistance aux personnes concernées pour aider à comprendre la portée du consentement ;
- Conservation d'une preuve des consentements ;
- Gestion des retraits de consentements.

Mesures pour assurer la protection des renseignements personnels

Un organisme public doit prendre les mesures de sécurité propres à assurer la protection des renseignements personnels collectés, utilisés, communiqués, conservés ou détruits et qui sont raisonnables compte tenu, notamment, de leur sensibilité, de la finalité de leur utilisation, de leur quantité, de leur répartition et de leur support (article 63.1 de la Loi sur l'accès).

10. Il faudra également considérer les lignes directrices de la Commission d'accès à l'information sur les critères de validité du consentement.

Éléments de contenu :

- Analyse des risques qui tient compte notamment de la sensibilité et de la quantité des renseignements personnels afin d'établir les mesures appropriées ;
- Établir des mesures organisationnelles (ex. : séparation des tâches, télétravail, utilisation des appareils de l'employeur, etc.) ;
- Instaurer des mesures en lien avec le volet humain (ex. : procéder à une vérification des antécédents judiciaires [si nécessaire], faire signer un engagement de confidentialité, etc.) ;
- Prendre des mesures physiques (ex. : contrôle d'accès physique, protection contre les sinistres, mesures pour assurer la sécurité du matériel contre le vol, etc.) ;
- Élaborer des mesures technologiques et techniques (ex. : chiffrement, contrôle des accès aux systèmes, séparation des environnements, processus de sauvegarde des données, mesures d'authentification, gestion des mots de passe, etc.) ;
- Effectuer des tests d'intrusion ;
- Réviser régulièrement les mesures pour assurer la protection des renseignements personnels.

Projets de système d'information ou de prestation électronique de services impliquant des renseignements personnels

Un organisme public doit procéder à une évaluation des facteurs relatifs à la vie privée de tout projet d'acquisition, de développement et de refonte de système d'information ou de prestation électronique de services impliquant des renseignements personnels (article 63.5 de la Loi sur l'accès).

Éléments de contenu :

- Tenir compte de la protection des renseignements personnels et de la protection de la vie privée dès le début d'un projet ;
- Réaliser une évaluation des facteurs relatifs à la vie privée ;
- Consultation du comité sur l'accès à l'information et la protection des renseignements personnels (à différents moments, et ce, du début jusqu'à la fin du projet) ;
- Suggestions de mesures de protection et de sécurité par le comité sur l'accès à l'information et la protection des renseignements personnels ;
- Déterminer l'accompagnement requis en matière de protection des renseignements personnels pour le projet (ex. : selon la sensibilité des renseignements personnels, selon les risques identifiés, etc.) ;
- Inclure des règles concernant la protection des renseignements personnels dans les documents d'appels d'offres et les contrats en lien avec un projet ;
- Permettre qu'un renseignement personnel informatisé recueilli auprès de la personne concernée soit communiqué à cette dernière dans un format technologique structuré et couramment utilisé (droit à la portabilité).

Évaluation des facteurs relatifs à la vie privée

En vertu de la Loi sur l'accès, un organisme public peut être amené à devoir réaliser des évaluations des facteurs relatifs à la vie privée (articles 63.5, 64, 67.2.1, 68 et 70.1 de la Loi sur l'accès).

Éléments de contenu :

- Identifier dans quels cas il est nécessaire de réaliser une évaluation des facteurs relatifs à la vie privée ;
- Indiquer comment procéder à une évaluation des facteurs relatifs à la vie privée au sein de l'organisme public ;
- Établir un ou des gabarits de rapport pour une évaluation des facteurs relatifs à la vie privée ;
- Faire approuver une évaluation des facteurs relatifs à la vie privée ;
- Assurer un suivi des évaluations des facteurs relatifs à la vie privée (ex. : registre) et conserver une copie des rapports.

Plan de formation et de sensibilisation que l'organisme offre à son personnel en matière de protection des renseignements personnels

Les règles de gouvernance d'un organisme public doivent inclurent une description des activités de formation et de sensibilisation que l'organisme offre à son personnel en matière de protection des renseignements personnels (article 63.3 de la Loi sur l'accès)[11].

Éléments de contenu :

- Établir un plan de formation et de sensibilisation ;
- Documenter les activités de formation et de sensibilisation offertes et en informer les membres du personnel ;
- Consigner les activités de formation et de sensibilisation réalisées en conservant les données requises pour démontrer la mise en œuvre du plan (ex. : date de l'activité, durée de l'activité, description des membres du personnel ciblés, nombre de participants, description de l'activité, moyen utilisé, etc.).

11. Il est possible de combiner la protection des renseignements personnels et l'accès aux documents dans le même plan de formation et de sensibilisation. En vertu de l'article 2 du Règlement sur la diffusion de l'information et sur la protection des renseignements personnels, le sous-ministre ou le dirigeant d'un organisme public doit veiller à la sensibilisation et à la formation des membres du personnel et des membres du personnel de direction ou d'encadrement de l'organisme public sur les obligations et les pratiques en matière d'accès à l'information.

Gestion des incidents de confidentialité

Un organisme public qui a des motifs de croire que s'est produit un incident de confidentialité impliquant un renseignement personnel qu'il détient doit prendre les mesures raisonnables pour diminuer les risques qu'un préjudice soit causé et éviter que de nouveaux incidents de même nature ne se produisent. Si l'incident présente un risque qu'un préjudice sérieux soit causé, l'organisme doit, avec diligence, aviser la Commission d'accès à l'information. Il doit également aviser toute personne dont un renseignement personnel est concerné par l'incident. Un organisme public doit tenir un registre des incidents de confidentialité (articles 63.8 à 63.11 de la Loi sur l'accès)[12].

Éléments de contenu :

- Évaluation de la situation liée à un incident de confidentialité (circonstances de l'incident, renseignements personnels impliqués, nombre de personnes visées, identifier le problème, etc.) ;
- Prendre les mesures raisonnables pour diminuer les risques qu'un préjudice soit causé et éviter que de nouveaux incidents de même nature ne se produisent ;
- Évaluation du risque qu'un préjudice soit causé (sérieux ou non) et consultation du responsable de la protection des renseignements personnels ;
- Le cas échéant, aviser la Commission d'accès à l'information ;
- Le cas échéant, aviser les personnes concernées par l'incident, sous réserve de ne pas entraver une enquête faite par une personne ou par un organisme qui, en vertu de la loi, est chargé de prévenir, détecter ou réprimer le crime ou les infractions aux lois ;
- Déterminer si une communication de renseignements personnels à une personne ou à un organisme est nécessaire afin de diminuer le risque qu'un préjudice sérieux soit causé et, le cas échéant, enregistrer la communication ;
- Inscrire l'incident au registre.

Informations à diffuser en lien avec la protection des renseignements personnels

En vertu de la Loi sur l'accès (ex. : articles 63.3 et 63.4) et, pour les organismes publics visés, du Règlement sur la diffusion de l'information et sur la protection des renseignements personnels (RLRQ, chapitre A-2.1, r. 2, ci-après « Règlement sur la diffusion »), un organisme doit diffuser des informations en lien avec la protection des renseignements personnels[13].

12. Il faut également considérer le Règlement sur les incidents de confidentialité.

13. Cela pourrait également inclure l'ensemble des renseignements et documents prévus au Règlement sur la diffusion.

Éléments de contenu :

- Diffusion :
  - des règles de gouvernance ;
  - des politiques de confidentialité et, le cas échéant, des avis de modifications ;
  - du nom de la personne responsable de la protection des renseignements personnels et des coordonnées permettant de communiquer avec elle.
- Le cas échéant, diffusion des informations en lien avec la protection des renseignements personnels visés par le Règlement sur la diffusion ;
- Le cas échéant, inclure dans le rapport annuel de gestion ou d'activités un bilan des demandes de communication, des demandes de rectification et des activités relatives à la protection des renseignements personnels réalisées au sein de l'organisme public.

Voici la liste des thèmes qui ne s'appliquent pas nécessairement à tous les organismes publics :

Identification, localisation et profilage

Un organisme public qui recueille des renseignements personnels auprès de la personne concernée en ayant recours à une technologie comprenant des fonctions permettant de l'identifier, de la localiser ou d'effectuer un profilage doit respecter certaines exigences (article 65.0.1 de la Loi sur l'accès).

Éléments de contenu :

- Évaluation de la nécessité de la collecte ayant recours à une technologie comprenant des fonctions permettant d'identifier, de localiser ou d'effectuer un profilage ;
- Informations à transmettre à la personne concernée ;
- Protection par défaut (désactivation des fonctions), activation des fonctions par la personne concernée ou par l'obtention de son consentement.

Utilisation de renseignements dépersonnalisés à des fins d'étude, de recherche ou de production de statistiques

Un organisme public peut utiliser un renseignement personnel, sans le consentement de la personne concernée, lorsque son utilisation est nécessaire à des fins d'étude, de recherche ou de production de statistiques et qu'il est dépersonnalisé (paragraphe 4 du deuxième alinéa de l'article 65.1 de la Loi sur l'accès)[14].

14. À noter que le paragraphe 4 du deuxième alinéa de l'article 65.1 de la Loi sur l'accès offre une possibilité supplémentaire pour un organisme public d'utiliser des renseignements personnels, sans le consentement des personnes concernées, à des fins d'étude, de recherche ou de production de statistiques dans la mesure où ils sont dépersonnalisés. Pour utiliser des renseignements personnels à des fins d'étude, de recherche ou de production de statistiques, il n'est cependant pas nécessaire de recourir au paragraphe 4 du deuxième alinéa de l'article 65.1 de la Loi sur l'accès. Il est toujours possible de s'appuyer sur une autre base légale pour utiliser un renseignement personnel à ces fins, sans obligation de le dépersonnaliser.

Éléments de contenu :

- Évaluation de la nécessité de l'utilisation à des fins d'étude, de recherche ou de production de statistiques ;
- Dépersonnalisation des renseignements personnels ;
- Évaluation des risques d'identification d'une personne physique à partir de renseignements dépersonnalisés ;
- Mesures raisonnables afin de limiter les risques d'identification d'une personne physique à partir de renseignements dépersonnalisés.

Décision fondée exclusivement sur un traitement automatisé de renseignements personnels

Un organisme public qui utilise des renseignements personnels afin que soit rendue une décision fondée exclusivement sur un traitement automatisé de ceux-ci doit se conformer à certaines exigences en matière de transparence et permettre à la personne concernée de présenter ses observations à un membre du personnel de l'organisme public en mesure de réviser la décision (article 65.2 de la Loi sur l'accès).

Éléments de contenu :

- Déterminer dans quels cas recourir à l'utilisation de renseignements personnels afin que soit rendue une décision fondée exclusivement sur un traitement automatisé de ceux-ci ;
- Évaluation de la nécessité de la collecte ;
- Conformité de l'utilisation des renseignements personnels à l'article 65.1 de la Loi sur l'accès ;
- Informer la personne faisant l'objet d'une telle décision ;
- Répondre à une demande d'information adressée par une personne concernée ;
- Permettre à la personne concernée de présenter ses observations à un membre du personnel de l'organisme public en mesure de réviser la décision.

Communication de renseignements personnels à des fins d'étude, de recherche ou de production de statistiques

Un organisme public peut communiquer des renseignements personnels sans le consentement des personnes concernées à une personne ou à un organisme qui souhaite utiliser ces renseignements à des fins d'étude, de recherche ou de production de statistiques (articles 67.2.1 à 67.2.3 de la Loi sur l'accès).

Éléments de contenu :

- Recevoir les demandes des personnes ou organismes qui souhaitent utiliser des renseignements personnels à des fins d'étude, de recherche ou de production de statistiques ;
- Réaliser une évaluation des facteurs relatifs à la vie privée ;
- Évaluation de la nécessité de communiquer un renseignement personnel et déterminer si la communication peut s'effectuer selon l'évaluation des facteurs relatifs à la vie privée ;
- Conclure une entente avec les clauses nécessaires avec la personne ou l'organisme ;
- Transmission de l'entente à la Commission d'accès à l'information ;
- Obtenir les engagements de confidentialité ;
- Acquérir des avis concernant le non-respect de toute condition prévue à l'entente, de tout manquement aux mesures de protection prévues à l'entente et de tout événement susceptible de porter atteinte à la confidentialité des renseignements ;
- Inscription au registre prévu à l'article 67.3 de la Loi sur l'accès.

Communication de renseignements personnels en vertu de l'article 68 de la Loi sur l'accès

Un organisme public peut, sans le consentement de la personne concernée, communiquer un renseignement personnel à différentes fins prévues à l'article 68 de la Loi sur l'accès.

Éléments de contenu :

- Réaliser une évaluation des facteurs relatifs à la vie privée ;
- Évaluation de la nécessité de communiquer un renseignement personnel et déterminer si la communication peut s'effectuer selon l'évaluation des facteurs relatifs à la vie privée ;
- Conclure une entente comprenant les clauses nécessaires avec la partie qui recevra les renseignements personnels ;
- Transmission de l'entente à la Commission d'accès à l'information ;
- Inscription au registre prévu à l'article 67.3 de la Loi sur l'accès.

Communication de renseignements personnels à l'extérieur du Québec

Avant de communiquer à l'extérieur du Québec un renseignement personnel, un organisme public doit se conformer à certaines exigences et s'assurer que le renseignement bénéficiera d'une protection adéquate (article 70.1 de la Loi sur l'accès).

Éléments de contenu :

- Inclure des règles concernant la communication de renseignements personnels à l'extérieur du Québec dans les documents d'appel d'offres ;
- Réaliser une évaluation des facteurs relatifs à la vie privée ;
- Analyser le régime juridique applicable dans l'État où les renseignements seraient communiqués ;
- Déterminer si les renseignements personnels bénéficieraient d'une protection adéquate, notamment au regard des principes de protection des renseignements personnels généralement reconnus ;
- S'assurer que la communication fait l'objet d'une entente écrite qui tient compte notamment des résultats de l'évaluation des facteurs relatifs à la vie privée et des modalités convenues dans le but d'atténuer les risques identifiés dans le cadre de cette évaluation.

Anonymisation de renseignements personnels

Un organisme public peut anonymiser un renseignement personnel pour l'utiliser à des fins d'intérêt public (article 73 de la Loi sur l'accès)[15].

Éléments de contenu :

- Établir les fins pour lesquelles des renseignements personnels sont anonymisés ;
- Déterminer si les fins sont d'intérêt public ;
- Recourir à des ressources spécialisées en matière d'anonymisation ;
- Analyser les risques de réidentification ;
- Établir les techniques d'anonymisation à utiliser et qui sont généralement reconnues comme les meilleures pratiques dans le domaine ;
- S'assurer que les renseignements sont bien anonymisés ;
- Établir un registre des renseignements anonymisés ;
- Évaluer régulièrement les renseignements anonymisés afin de s'assurer qu'ils le demeurent.

15. Il faudra également considérer les critères et les modalités déterminés par règlement.

Protection par défaut

Un organisme public qui recueille des renseignements personnels en offrant au public un produit ou un service technologique disposant de paramètres de confidentialité doit s'assurer que, par défaut, ces paramètres assurent le plus haut niveau de confidentialité, sans aucune intervention de la personne concernée (article 63.7 de la Loi sur l'accès).

Éléments de contenu :

- Prendre en compte la protection par défaut dès le début d'un projet ;
- Déterminer les mesures pour assurer la protection par défaut (plus haut niveau de confidentialité, sans aucune intervention de la personne concernée) dans le cadre d'un produit ou d'un service technologique offert au public disposant de paramètres de confidentialité ;
- Établir les mesures pour permettre à la personne concernée de modifier facilement les paramètres de confidentialité.

Mesures de protection à prendre à l'égard des renseignements personnels recueillis ou utilisés dans le cadre d'un sondage

Les règles de gouvernance d'un organisme public doivent inclurent les mesures de protection à prendre à l'égard des renseignements personnels recueillis ou utilisés dans le cadre d'un sondage (article 63.3 de la Loi sur l'accès).

Éléments de contenu :

- Évaluation de la nécessité de recourir à un sondage ;
- Évaluation de la nécessité de la collecte de renseignements personnels dans le cadre d'un sondage et, le cas échéant, de la communication de renseignements personnels à un prestataire de services ;
- Évaluation de l'aspect éthique du sondage ;
- Informations à transmettre aux participants ;
- Mesures :
  - de protection contractuelles ou autres à mettre en place lorsque le sondage est confié à un prestataire de service ;
  - pour assurer la participation volontaire au sondage des participants ;
  - pour assurer la confidentialité des participants ;
  - pour assurer la confidentialité des participants lors de la diffusion des résultats du sondage.

Vidéosurveillance

Un organisme public doit procéder à une évaluation des facteurs relatifs à la vie privée de tout projet d'acquisition, de développement et de refonte de système d'information ou de prestation électronique de services impliquant des renseignements personnels (article 63.5 de la Loi sur l'accès).
Un projet de système de vidéosurveillance est visé par l'article 63.5 de la Loi sur l'accès.

Éléments de contenu (en surplus de ceux prévus pour les projets de système d'information ou de prestation électronique de services impliquant des renseignements personnels) :

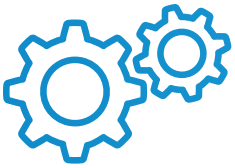
- Évaluation de la nécessité de recourir à la vidéosurveillance et de recueillir des images ;
- Décrire les besoins de recourir à la vidéosurveillance pour la sécurité ;
- Analyser des solutions alternatives moins intrusives évaluées et indiquer pourquoi elles n'ont pas été retenues ;
- Mettre en place les caméras nécessaires et de manière à limiter les impacts sur la vie privée des personnes (ex. : enregistrements à des moments précis selon les besoins en matière de sécurité, éviter de filmer les zones où les attentes en matière de vie privée sont plus élevées, limiter le champ de vision des caméras, etc.) ;
- Informer les personnes concernées de la présence de caméras et, le cas échéant, de l'enregistrement (ex. : par une affiche) et des coordonnées pour transmettre des questions ;
- Déterminer les mesures pour limiter l'accès aux images et l'utilisation de celles-ci ;
- Déterminer les mesures pour assurer la sécurité des images.

Biométrie

Un organisme public doit procéder à une évaluation des facteurs relatifs à la vie privée de tout projet d'acquisition, de développement et de refonte de système d'information ou de prestation électronique de services mettant en cause des renseignements personnels (article 63.5 de la Loi sur l'accès). Un projet de système d'information ou de prestation électronique de services intégrant de la biométrie est visé par l'article 63.5 de la Loi sur l'accès. Un organisme public est également assujetti aux exigences concernant la biométrie prévues à la Loi concernant le cadre juridique des technologies de l'information (RLRQ, chapitre C-1.1, ci-après « LCCJTI »).

Éléments de contenu (en surplus de ceux prévus pour les projets de système d'information ou de prestation électronique de services impliquant des renseignements personnels) :

- Évaluation de la nécessité de recueillir des renseignements personnels biométriques ;
- Décrire la situation problématique à résoudre ;
- Analyser les solutions alternatives moins intrusives évaluées et indiquer pourquoi elles n'ont pas été retenues ;
- Divulguer le procédé permettant de saisir des caractéristiques ou des mesures biométriques et la création d'une banque de caractéristiques ou de mesures biométriques à la Commission d'accès à l'information (conformément aux articles 44 et 45 de la LCCJTI) ;
- Obtenir le consentement exprès de la personne concernée (article 44 de la LCCJTI) ;
- Établir une solution alternative en cas de refus de consentir ou de retrait du consentement ;
- Faire appel au minimum de caractéristiques ou de mesures biométriques pour identifier une personne ;
- Ne pas recueillir les caractéristiques ou les mesures biométriques à l'insu de la personne concernée ;
- Ne pas utiliser les renseignements personnels biométriques à d'autres fins ;
- Mettre en place des mesures de protection et de sécurité (ex. : convertir le renseignement personnel biométrique en code, et ce, de façon irréversible) ;
- Destruction des renseignements personnels biométriques.



Mise en œuvre

Un organisme public peut mettre en place de bonnes règles de gouvernance, mais celles-ci auront peu de valeur si elles ne sont pas mises en œuvre adéquatement par les membres de son personnel.

En plus de rendre les règles de gouvernance facilement accessibles pour les membres de son personnel, un organisme public doit offrir de la formation et de la sensibilisation, en plus de s'assurer de bien encadrer les membres de son personnel.

Formation et sensibilisation

Tous les membres du personnel d'un organisme public doivent être adéquatement formés en matière de protection des renseignements personnels. Cela implique notamment de les former sur les exigences légales, mais aussi sur les règles de gouvernance de l'organisme public. En effet, les membres du personnel doivent connaître leurs rôles et leurs responsabilités pour assurer la protection des renseignements personnels. Ils doivent maîtriser les règles et les processus de l'organisme public liés aux différents traitements de renseignements personnels dans lesquels ils pourraient participer dans le cadre de leurs fonctions.

Un organisme public devrait donc mettre en place un plan de formation et de sensibilisation pour les membres de son personnel. Ce plan devrait débuter dès l'embauche d'une nouvelle personne pour s'assurer que celle-ci se conforme rapidement aux exigences légales et aux règles de gouvernance. L'ensemble des membres du personnel devraient être formés et sensibilisés régulièrement pour assurer la mise en œuvre adéquate des règles de gouvernance.

Encadrer et outiller les membres du personnel

En plus de la formation et de la sensibilisation, un organisme public devrait s'assurer de bien encadrer les membres de son personnel et leur fournir les outils nécessaires pour qu'ils puissent remplir adéquatement leurs responsabilités.

Un organisme public pourrait avoir besoin de fournir des instructions de travail précises pour s'assurer que les membres de son personnel se conforment aux exigences légales et à ses règles de gouvernance. On peut penser, par exemple, à des instructions de travail pour quelqu'un qui œuvre au service à la clientèle afin de procéder à l'authentification d'une personne qui veut obtenir des informations en lien avec son dossier personnel.

Les membres du personnel doivent également être outillés pour bien exercer leurs fonctions. Si, par exemple, une personne a la responsabilité de mettre en place les mesures de sécurité nécessaires pour assurer la protection des renseignements personnels, celle-ci ne pourra pas exercer pleinement sa responsabilité si l'organisme public ne lui fournit pas les outils technologiques appropriés.

Évaluation

Un organisme public devrait évaluer ses pratiques en matière de protection des renseignements personnels. Cette évaluation est nécessaire afin de compléter la démarche proposée précédemment (planification, organisation, mise en œuvre et évaluation). Ensuite, la planification doit être revue afin de relancer la démarche. Les règles de gouvernance devraient être mises à jour régulièrement afin de contribuer davantage aux objectifs et orientations stratégiques de l'organisme public en matière de protection des renseignements personnels et pour s'assurer de demeurer conformes aux différentes exigences légales. Des processus de reddition de comptes et des mesures d'évaluation devraient donc être mis en place.

Reddition de comptes

Pour procéder à l'évaluation de ses pratiques en matière de protection des renseignements personnels, un organisme public devrait se doter d'un processus de reddition de comptes. Celui-ci pourrait, par exemple, être sous la responsabilité du comité sur l'accès à l'information et la protection des renseignements personnels.

Il s'agit de rendre compte des activités de l'organisme public afin d'obtenir des informations clés pour planifier les ajustements à effectuer pour améliorer la protection des renseignements personnels.

Par exemple, un organisme pourrait faire un suivi au comité sur l'accès à l'information et la protection des renseignements personnels des incidents de confidentialité qui présentent un risque qu'un préjudice sérieux soit causé, des plaintes retenues en lien avec la protection des renseignements personnels, des inspections et des enquêtes effectuées par la Commission d'accès à l'information, des risques relevés en lien avec la protection des renseignements personnels, etc. Pour les organismes publics visés, il pourrait également y avoir un suivi en lien avec le bilan inséré dans le rapport annuel de gestion ou d'activités de l'organisme public en vertu de l'article 2 du Règlement sur la diffusion. Ces suivis pourraient, par exemple, permettre de corriger des pratiques de l'organisme public non conformes à la loi, d'améliorer des processus déficients, de bonifier les mesures de protection et de sécurité, etc.

Il revient à l'organisme public de déterminer dans son processus quels éléments feront l'objet d'une reddition de comptes et de quelle façon elle sera effectuée (ex. : présentation lors d'une rencontre, production d'un rapport, etc.).

Évaluer le niveau de la protection des renseignements personnels

Un organisme public devrait se doter d'un processus pour évaluer le niveau de la protection des renseignements personnels de manière proactive. Celui-ci devrait tenir compte notamment de la taille, des activités et des ressources de l'organisme public.

Par exemple, pour un organisme public d'une certaine taille qui détient de nombreux renseignements personnels dans le cadre de ses activités, il peut s'agir de la réalisation d'un audit ou d'un processus de vérification interne ou externe qui examinera la protection des renseignements personnels au sein de l'organisme public et qui mènera à la production d'un rapport avec des recommandations. Pour un organisme public de plus petite taille, qui détient peu de renseignements personnels, il peut s'agir d'un processus de vérification plus simple effectué par le responsable de la protection des renseignements personnels.

Ce processus et, le cas échéant, les rapports et les recommandations qui en découleront permettront de planifier les ajustements à effectuer pour améliorer la protection des renseignements personnels.

CONCLUSION

La démarche en quatre étapes suggérée aidera les organismes publics à se doter de règles de gouvernance conformes à l'article 63.3 de la Loi sur l'accès et, ainsi, à bonifier la protection des renseignements personnels au sein de ces organismes publics. Cela contribue également au respect du principe de responsabilité prévu par l'article 52.2 de la Loi sur l'accès.

Par ailleurs, la démarche suggérée ne devrait pas être réalisée en vase clos par la personne responsable de la protection des renseignements personnels et son équipe. Il s'agit d'une responsabilité organisationnelle qui nécessite une approche multidisciplinaire et qui devrait nécessiter la participation de tous les intervenants qui peuvent être concernés par la protection des renseignements personnels.

Ministère
du Conseil exécutif
Québec