Borden Ladner Gervais

# Réforme des lois québécoises en matière de protection des renseignements personnels : Guide de conformité pour les organismes publics

Juillet 2022

# Réforme des lois québécoises en matière de protection des renseignements personnels : Guide de conformité pour les organismes publics

Ce guide a pour objectif d'outiller les organismes publics en vue de l'entrée en vigueur des nouvelles exigences introduites à la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, faisant suite à l'adoption de la Loi modernisant des dispositions législatives en matière de protection des renseignements personnels (« **Loi 64** »).

Ce guide est divisé en différents thèmes qui reflètent les principaux changements apportés par la Loi 64 au régime de protection des renseignements personnels dans le secteur public.

## Pistes de conformité

Nous avons suggéré, pour chaque thème, certaines mesures que les organismes peuvent envisager afin de se préparer à l'entrée en vigueur des nouvelles dispositions et aux changements requis pour s'y conformer.

## Incertitudes

Considérant que plusieurs exigences introduites par la Loi 64 sont de droit nouveau, certaines dispositions soulèvent des défis d'interprétation. Nous avons donc identifié les éléments sur lesquels les organismes devraient porter une attention particulière à l'aide du symbole **!**.

**NB** : Ce guide reprend certains éléments mentionnés par le gouvernement du Québec sur sa page dédiée à la Protection des renseignements personnels.

# Table des matières

# Entrée en vigueur

Le tableau suivant résume les différentes périodes d'entrée en vigueur des principales modifications apportées par la Loi 64 à la *Loi sur l'accès aux documents des organismes publics et la protection des renseignements personnels* (« **Loi sur l'accès** »). Sauf exception, les modifications apportées à la Loi sur l'accès entreront en vigueur le **22 septembre 2023**, soit deux ans après la date de sanction du projet de loi n° 64. Certaines dispositions entreront toutefois en vigueur en 2022, incluant les exigences relatives au Comité sur l'accès à l'information et la protection des renseignements personnels et celles concernant la notification des incidents de confidentialité. Quant au nouveau droit à la portabilité des données, il entrera en vigueur en 2024.

| Article(s) | Exigence | Entrée en vigueur | Voir |
|---|---|---|---|
| **8** | Principe de responsabilité et rôles de responsable de l'accès aux documents et de responsable de la protection des renseignements personnels | **Septembre 2022** | Section 2.1 |
| **8.1** | Mise sur pied d'un Comité sur l'accès à l'information et la protection des renseignements personnels | **Septembre 2022** | Section 2.2 |
| **53.1** | Nouvelles exigences en matière de consentement | **Septembre 2023** | Section 3.2 |
| **55 et 65.1** | Exceptions au consentement pour l'utilisation de renseignements personnels | **Septembre 2023** | Section 3.3 |
| **63.1** | Conservation et destruction des renseignements personnels | **Septembre 2023** | Section 7.1 |
| **63.3** | Règles de gouvernance à l'égard des renseignements personnels | **Septembre 2023** | Section 2.3 |
| **63.5** | Évaluation des facteurs relatifs à la vie privée | **Septembre 2023** | Section 2.4 |
| **63.6.1** | Protection de la vie privée par défaut | **Septembre 2023** | Section 2.5 |
| **63.7 à 63.10** | Signalement des incidents de confidentialité | **Septembre 2022** | Section 7.2 |
| **65** | Obligation d'information et de transparence | **Septembre 2023** | Section 3.1 |

| Article(s) | Exigence | Entrée en vigueur | Voir |
|---|---|---|---|
| **65.0.1** | Technologies d'identification, de géolocalisation et de profilage | **Septembre 2023** | Section 3.1 |
| **65.2** | Prise de décision automatisée | **Septembre 2023** | Section 4.3 et 5.2 |
| **67.2** | Communication de renseignements personnels à un fournisseur de services | **Septembre 2023** | Section 6.1 |
| **67.2.1 à 67.2.3** | Communication de renseignements personnels à des fins de recherche | **Septembre 2022** | Section 4.1 |
| **70.1** | Communication de renseignements personnels à l'extérieur du Québec | **Septembre 2023** | Section 6.2 |
| **84** | Droit à la portabilité des données | **Septembre 2024** | Section 5.1 |
| **158 à 165** | Nouveaux mécanismes de mise en œuvre | **Septembre 2023** | Section 1 |
| **44 et 45** | Modifications aux dispositions de la LCCJTI en matière de biométrie | **Septembre 2022** | Section 7.3 |

# 1. Nouveaux mécanismes de mise en œuvre

## En vigueur le 22 septembre 2023

Le nouveau régime permettant à la Commission d'accès à l'information (« **CAI** ») d'imposer des sanctions administratives pécuniaires dans le secteur privé n'est pas introduit dans le secteur public. La Loi 64 modifie toutefois les dispositions pénales déjà prévues aux articles 158 à 165 de la Loi sur l'accès.

**Sanctions pénales** (art. 158 à 164.2). La Loi 64 crée deux catégories de sanctions qui se distinguent par leur niveau de gravité et le montant des amendes qui y sont associées (voir le tableau ci-dessous pour les infractions précises). Les infractions les moins graves sont prévues à l'article 158, qui prévoit une amende maximale de 10 000 $ dans le cas d'une personne physique et de 30 000 $ dans les autres cas. Les infractions les plus graves sont prévues à l'article 159, qui prévoit une amende maximale de 100 000 $ dans le cas d'une personne physique et de 150 000 $ dans les autres cas. La Loi 64 précise qu'en cas de récidive, les amendes seront portées au double (art. 164.1). Enfin, les poursuites pénales devront être intentées par la CAI dans un délai de cinq (5) ans suivant la perpétration de l'infraction (art. 164.2).

**Facteurs de détermination** (art. 160). Le législateur a retiré l'adverbe « sciemment » aux articles 158 et 159 de la Loi sur l'accès, ayant pour effet d'alléger le fardeau de preuve du poursuivant qui n'aura plus à démontrer l'intention coupable du contrevenant. En outre, un nouvel article 160 vient préciser les facteurs qu'un juge devra considérer lors de la détermination du montant de l'amende pénale, soit :

- la nature, la gravité, le caractère répétitif et la durée de l'infraction;
- la sensibilité des renseignements personnels concernés par l'infraction;
- le fait que le contrevenant ait agi intentionnellement ou ait fait preuve de négligence ou d'insouciance;
- le caractère prévisible de l'infraction ou le défaut d'avoir donné suite aux recommandations ou aux avertissements visant à la prévenir;
- les tentatives du contrevenant de dissimuler l'infraction ou son défaut de tenter d'en atténuer les conséquences;
- le fait que le contrevenant ait omis de prendre des mesures raisonnables pour empêcher la perpétration de l'infraction;
- le fait que le contrevenant, en commettant l'infraction ou en omettant de prendre des mesures pour empêcher sa perpétration, ait accru ses revenus ou ait réduit ses dépenses, ou avait l'intention de le faire;
- le nombre de personnes concernées par l'infraction et le risque de préjudice auquel ces personnes sont exposées.

## 1.1. Liste des infractions prévues à la Loi sur l'accès

| | Sanction pénale (art. 158) | Sanction pénale (art. 159) |
|---|---|---|
| Refuser ou entraver l'accès à un document ou à un renseignement accessible en vertu de la loi, notamment en détruisant, modifiant ou cachant le document ou en retardant indûment sa communication. | ✖ | |
| Donner accès à un document dont la loi ne permet pas l'accès ou auquel un organisme public, conformément à la loi, refuse de donner accès. | ✖ | |
| Informer une personne de l'existence d'un renseignement dont elle n'a pas le droit d'être informée en vertu de la loi. | ✖ | |
| Entraver l'exercice des fonctions du responsable de l'accès aux documents ou de la protection des renseignements personnels. | ✖ | |
| Recueillir, utiliser, conserver ou détruire des renseignements personnels en contravention à la loi. | ✖ | |
| Omettre de déclarer, s'il est tenu de le faire, un incident de confidentialité à la Commission ou aux personnes concernées. | ✖ | |
| Faire défaut de respecter les conditions prévues à une entente conclue en application de l'article 67.2.3 de la Loi sur l'accès. | ✖ | |
| Communiquer des renseignements personnels en contravention à la loi. | | ✖ |
| Entraver le déroulement d'une enquête, d'une inspection ou l'instruction d'une demande par la CAI. | | ✖ |
| Procéder ou tenter de procéder à l'identification d'une personne physique à partir de renseignements dépersonnalisés sans l'autorisation de l'organisme public qui les détient, ou à partir de renseignements anonymisés. | | ✖ |
| Refuser ou négliger de se conformer, dans le délai fixé, à une demande de production de documents émise par la CAI. | | ✖ |
| Contrevenir à une ordonnance de la CAI. | | ✖ |
| Ne pas prendre les mesures de sécurité propres à assurer la protection des renseignements personnels conformément à l'article 63.1 de la Loi sur l'accès. | | ✖ |

# 2. Responsabilité et gouvernance

La Loi 64 reconnaît formellement que tout organisme public est responsable d'assurer la protection des renseignements personnels qu'il détient (art. 52.2). Ceci implique que l'organisme doit en tout temps être en mesure de démontrer son respect des exigences législatives ainsi que les mesures prises pour assurer la protection des renseignements personnels. Le principe de responsabilité est principalement mis en œuvre par le « responsable de la protection des renseignements personnels » et le « comité sur l'accès à l'information et la protection des renseignements personnels », qui veillent au respect de la Loi sur l'accès et à l'implantation des règles de gouvernance à l'égard des renseignements personnels.

## 2.1. Responsable de l'accès aux documents et Responsable de la protection des renseignements personnels

**En vigueur le 22 septembre 2022**

**Fonctions et désignation.** Contrairement au secteur privé, la Loi sur l'accès attribuait déjà à la « personne ayant la plus haute autorité au sein d'un organisme public » les fonctions de responsable de l'accès aux documents (« **responsable de l'accès** ») et de responsable de la protection des renseignements personnels (« **responsable de la PRP** »). Avec la Loi 64, la personne ayant la plus haute autorité au sein d'un organisme public, c'est-à-dire le sous-ministre dans le cas d'un ministère ou le directeur général dans le cas d'une municipalité ou d'une commission scolaire, est désormais responsable d'assurer le respect et la mise en œuvre de la Loi sur l'accès (art. 8 al. 1). Chacune de ces fonctions peut toutefois être déléguée par écrit, en tout ou en partie, à un membre de l'organisme public, de son conseil d'administration ou à un membre du personnel de direction (art. 8 al. 2). Il importe de souligner que les rôles de responsable de l'accès et de responsable de la PRP doivent pouvoir être exercés « de manière autonome » lorsqu'ils sont délégués, ce qui indique que le ou les titulaires de ces fonctions doivent posséder les compétences requises. De plus, le troisième alinéa de l'article 8 al. 3 prévoit que la plus haute autorité au sein de l'organisme doit veiller à « faciliter l'exercice » de ces fonctions lorsqu'elle ne les exerce pas elle-même. Finalement, le quatrième alinéa de l'article 8 vient préciser les modalités de l'avis de désignation qui doit être envoyé à la CAI. Dorénavant, les organismes devront dès que possible aviser la CAI par écrit du titre, des coordonnées et de la date d'entrée en fonction de la personne ou des personnes qui exerceront les fonctions de responsable de l'accès et de responsable de la PRP (art. 8 al. 4).

**Tâches**. De nouvelles tâches sont toutefois confiées au responsable de la PRP d'un organisme public en vertu de la Loi 64, qui devra notamment :

- Participer à l'élaboration des règles de gouvernance de l'organisme à l'égard des renseignements personnels (art. 63.3). Voir la section 2.3 ci-dessous pour plus de détails sur ces règles.
- Participer aux évaluations des facteurs relatifs à la vie privée (« **EFVP** ») (art. 63.5) et suggérer des mesures afin d'assurer la protection des renseignements personnels impliqués par le projet (art. 63.6). Voir la section 2.4 ci-dessous pour plus de détails sur les EFVP.

- Consigner toute communication à une entreprise ou organisme public susceptible de diminuer le préjudice causé par un incident de confidentialité (art. 63.8) et prendre part à l'évaluation du préjudice causé par un incident de confidentialité (art. 63.10). Voir la section 7.2 pour plus de détails sur les incidents de confidentialité.

### Pistes de conformité

1. **Déterminer les qualifications requises pour exercer le rôle de responsable de la PRP et celui de responsable de l'accès.** Les organismes devraient déterminer s'ils possèdent l'expertise nécessaire à l'interne ou s'ils ont besoin de recruter une personne pour exercer ce rôle.
2. **Établir une description des rôles et responsabilités du responsable de l'accès et du responsable de la PRP.** Cette description devrait tenir compte des obligations de la Loi 64 et de la réalité de l'organisme.
3. **Désigner une personne à titre de responsable de l'accès et une personne à titre de responsable de la PRP ou attribuer les deux rôles à une même personne.** La désignation doit se faire par écrit pour être valide.
4. **Transmettre les coordonnées du responsable de l'accès et celles du responsable de la PRP à la CAI.**

## 2.2. Comité sur l'accès à l'information et la protection des renseignements personnels

**En vigueur le 22 septembre 2022**

**Mise sur pied du Comité.** La Loi 64 élargit l'obligation de mise sur pied d'un comité sur l'accès à l'information et la protection des renseignements personnels (« **Comité** ») à tous les organismes publics assujettis à la Loi sur l'accès (art. 8.1). Auparavant, cette obligation était limitée aux organismes visés par le *Règlement sur la diffusion de l'information et sur la protection des renseignements personnels*. Notons que la Loi 64 n'oblige pas la création d'un nouveau comité. Ainsi, les rôles et responsabilités que la Loi 64 confie au Comité peuvent être attribués à un comité existant au sein de l'organisme, par exemple un comité chargé de la sécurité de l'information. Néanmoins, il est prévu qu'un règlement du gouvernement puisse exclure un organisme public de l'obligation de former ce comité (art. 8.1 al. 3). Il est également possible pour un organisme public de convenir avec un autre organisme public d'une impartition des rôles et des responsabilités de ce comité (art. 172). Cette impartition s'effectue dans le cadre d'une entente approuvée par la CAI.

**Composition du Comité.** La Loi 64 prévoit que le Comité relève de la personne ayant la plus haute autorité au sein de l'organisme public (qui agit également à titre de responsable de l'accès et de responsable de la PRP à moins que ces rôles n'aient été délégués). Cette personne est responsable d'établir la composition et le mandat du Comité et de veiller à son bon fonctionnement. La Loi 64 prévoit que le Comité est minimalement composé de :

- la personne responsable de l'accès;
- la personne responsable de la PRP;
- toute autre personne dont l'expertise est requise, incluant, le cas échéant, le responsable de la sécurité de l'information et le responsable de la gestion documentaire (art. 8.1 al. 2).

**Rôle et responsabilités.** Le Comité a pour mission de soutenir l'organisme public dans l'exercice de ses responsabilités et dans l'exécution de ses obligations en vertu de la Loi sur l'accès. Ainsi, ce Comité devra, entre autres :

- Approuver les règles de gouvernance de l'organisme à l'égard des renseignements personnels (art. 63.3).
- Être consulté dès le début d'un projet d'acquisition, de développement ou de refonte d'un système d'information ou de prestation électronique de services impliquant des renseignements personnels, et suggérer des mesures de protection des renseignements personnels applicables à ce projet, notamment :
  - la nomination d'une personne chargée de la mise en œuvre des mesures de protection des renseignements personnels;
  - des mesures de protection des renseignements personnels dans les documents relatifs au projet, comme un cahier des charges ou un contrat;
  - une description des responsabilités des participants au projet en matière de protection des renseignements personnels;
  - la tenue d'activités de formation sur la protection des renseignements personnels pour les participants (art. 63.5 et 63.6).

## Pistes de conformité

1. **Déterminer si un nouveau comité doit être créé ou si un comité existant peut remplir les fonctions de Comité sur l'accès à l'information et la protection des renseignements personnels.**
2. **Élaborer (ou réviser) un document de gouvernance qui précise le mandat, les objectifs ainsi que la composition du Comité.**

## 2.3. Règles de gouvernance à l'égard des renseignements personnels

### En vigueur le 22 septembre 2023

**Contenu**. La Loi 64 reconnaît formellement le devoir des organismes d'établir des règles encadrant leur gouvernance à l'égard des renseignements personnels (art. 63.3). Celles-ci devraient notamment traiter des thèmes suivants :

- les rôles et les responsabilités des membres du personnel tout au long du cycle de vie des renseignements personnels, c'est-à-dire de leur collecte à leur destruction;
- le processus de traitement des plaintes relatives à la protection des renseignements personnels;
- les activités de formation et de sensibilisation que l'organisme offre à son personnel en matière de protection des renseignements personnels;
- les mesures de protection prises par l'organisme lorsque des renseignements personnels sont recueillis ou utilisés dans le cadre d'un sondage;
- les mesures de protection prises par l'organisme lors de l'utilisation d'une technologie de vidéosurveillance.

Notons qu'un règlement du gouvernement pourrait venir préciser le contenu et les modalités des règles de gouvernance (art. 63.3 al. 4).

**Approbation et diffusion.** La Loi 64 prévoit que les règles de gouvernance de l'organisme doivent être approuvées par son Comité avant d'être publiées sur son site Internet (art. 63.3 al. 1). Cette obligation de transparence semble plus exigeante que celle introduite dans le secteur privé. En effet, la *Loi sur la protection des renseignements personnels dans le secteur privé* (« **Loi sur le secteur privé** ») prévoit qu'une entreprise devra publier de « l'information détaillée » sur ses politiques et pratiques en matière de protection des renseignements personnels.

**Format**. L'article 63.3 al. 1 prévoit que les règles de gouvernance de l'organisme « peuvent prendre la forme d'une politique, d'une directive ou d'un guide ». Ce libellé général confère une grande latitude aux organismes publics en ce qui concerne le format de leurs règles de gouvernance. Notons que le contenu des règles de gouvernance doit rester suffisamment général de manière à ne pas divulguer de renseignements confidentiels ni stratégiques. Par exemple, un organisme devrait éviter de détailler les mesures de sécurité prises pour protéger ses systèmes informatiques dans ses règles de gouvernance afin de ne pas rendre ceux-ci vulnérables aux cyberattaques.

## Pistes de conformité

1. **Effectuer un inventaire des politiques, directives, pratiques et procédures en place relativement à la protection des renseignements personnels tout au long de leur cycle de vie.**
2. **Effectuer un exercice de cartographie afin de documenter les pratiques de l'organisme en matière de gestion des renseignements personnels.** Cet exercice sera notamment utile au développement de règles de gouvernance.
3. **Mettre à jour ou établir les politiques et procédures suivantes :**
    - Politique établissant les principes généraux relatifs à la collecte, l'utilisation et la communication de renseignements personnels
    - Politique de conservation des données et calendrier de conservation
    - Directives et procédures relatives à la réception et le traitement de plaintes et de demandes des personnes concernées souhaitant exercer leurs droits
    - Politiques et procédures relatives à la sécurité de l'information
    - Politique de gestion des incidents de confidentialité et processus de réponse aux incidents
    - Directives particulières en fonction des activités de l'organisme, par exemple : politique sur l'utilisation des caméras de surveillance, politique sur l'utilisation de systèmes biométriques, politique sur la communication de renseignements personnels dans le cadre de projets de recherche, etc.
    - Procédure relative aux méthodes de destruction des renseignements personnels et d'anonymisation, le cas échéant
4. **Développer un programme de formation et de sensibilisation en matière de protection des renseignements personnels pour les employés qui traitent ou qui ont accès à des renseignements personnels.**
5. **Faire approuver les règles de gouvernance par le Comité.**
6. **Créer une section distincte sur le site Internet de l'organisme au sujet des règles de gouvernance à l'égard des renseignements personnels.**

## 2.4. Évaluation des facteurs relatifs à la vie privée (EFVP)

**En vigueur le 22 septembre 2023**

**Obligation d'effectuer une EFVP.** Tout comme les entreprises du secteur privé, les organismes devront procéder à une EFVP pour tout projet d'acquisition, de développement ou de refonte d'un système d'information ou de prestation électronique de services impliquant la collecte, l'utilisation, la communication, la conservation ou la destruction de renseignements personnels (art. 63.5 al. 1), ou encore avant de communiquer des renseignements personnels à l'extérieur du Québec, ou de confier à une personne ou à un organisme à l'extérieur du Québec la tâche de recueillir, d'utiliser, de communiquer ou de conserver pour son compte de tels renseignements (art. 70.1).

Les organismes publics devront également procéder à une EFVP en cas de :

- Collecte de renseignements nécessaires à l'exercice de leurs attributions ou à la mise en œuvre d'un programme d'un organisme avec lequel ils collaborent pour la prestation de services ou pour la réalisation d'une mission commune (art. 64);
- Communication, sans le consentement des personnes concernées, à une personne ou à un organisme public souhaitant utiliser les renseignements à des fins d'étude, de recherche ou de production de statistiques (art. 67.2.1 à 67.2.3);
- Communication d'un renseignement personnel, sans le consentement de la personne concernée, en vertu de l'article 68 de la Loi sur l'accès.

**Exemples de projets visés par l'obligation.** Le *Guide d'accompagnement : Réaliser une évaluation des facteurs relatifs à la vie privée*, de la CAI, mis à jour en mars 2021, sera revu à la lumière de la Loi 64 et pourrait être remanié en profondeur. Dans ce guide, la CAI recommande d'effectuer une EVFP pour tout projet impliquant des renseignements personnels. Bien que cela constitue un critère beaucoup plus large que celui prévu par la Loi 64, il est tout de même intéressant de noter les types de projets identifiés par la CAI :

- Développer un nouveau système d'information ou une technique de personnalisation d'un produit ou d'un service
- Chercher une nouvelle clientèle, explorer de nouveaux marchés
- Faire appel à un système d'algorithme ou d'intelligence artificielle (« **IA** »)
- Installer un système de vidéosurveillance
- Comparer différentes versions de bases de données ou de fichiers
- Acquérir ou fusionner des organisations
- Utiliser des empreintes digitales, la géolocalisation, un système de reconnaissance faciale, des objets connectés, des capteurs pour villes intelligentes, etc.

**Pas de portée rétroactive.** L'obligation de procéder à une EFVP n'a pas de portée rétroactive. Ainsi, les organismes n'auront pas à évaluer les systèmes existants lors de l'entrée en vigueur du nouvel article 63.5. Toutefois, la mise à jour substantielle d'un système existant (par exemple, une plateforme de gestion de documents) pourrait être considérée comme une « refonte » et devra donc faire l'objet d'une EFVP.

**Forme et portée de l'EFVP**. L'EFVP doit être « proportionnée à la sensibilité des renseignements concernés, à la finalité de leur utilisation, à leur quantité, à leur répartition et à leur support » (article 63.5 al. 4). Soulignons qu'il s'agit là des mêmes critères que ceux prévus à l'article 63.1 de la Loi sur l'accès afin de qualifier les mesures de sécurité qu'un organisme doit prendre pour assurer la protection des renseignements personnels qu'elle détient. Nous comprenons que ce critère vise à ce que l'envergure de l'EFVP soit adaptée à l'impact du projet sur la vie privée des individus. Un projet impliquant peu de renseignements personnels, et qui sont peu sensibles, ne nécessitera pas le même type d'EFVP que l'implantation d'un système biométrique visant un grand nombre d'individus, par exemple. Notons que le guide sur les EFVP de la CAI fournit des outils utiles aux organismes qui veulent se familiariser avec le processus.

**Portabilité des données**. En outre, les organismes devront s'assurer que les nouveaux projets et systèmes soient en mesure d'assurer la portabilité des données, c'est-à-dire la possibilité pour les personnes concernées d'obtenir la communication de leurs renseignements personnels dans un format technologique structuré et couramment utilisé (art. 63.5 al. 3). Voir la section 5.1 du présent guide pour plus de détails sur le droit à la portabilité des données.

## Pistes de conformité

1. **Développer une procédure interne sur la réalisation d'une EFVP.** La procédure devrait notamment prévoir :
   - les critères déclenchant l'obligation d'effectuer une EFVP. Par exemple, l'organisme pourrait établir une matrice permettant d'évaluer la nécessité d'une EFVP en fonction du niveau de risque que représente le projet;
   - un processus pour s'assurer que les projets qui requièrent une EFVP soient identifiés dès le début du projet.
2. **Développer un gabarit de réalisation d'une EFVP.**
   - Le gabarit devrait être dans un format facile d'utilisation de sorte que les responsables des opérations sans connaissance de pointe en matière de protection des renseignements personnels puissent effectuer une première version.
   - Former le personnel approprié sur la façon de compléter une EFVP.
3. **Diffuser la procédure et le gabarit au sein de l'organisme.**
   - Les organismes peuvent désigner des responsables dans les départements susceptibles d'initier ces projets (services aux citoyens, bureau de projet, communications, ressources humaines, etc.)
   - Les responsables des départements devraient informer le responsable de la PRP dès le début d'un projet nécessitant une EFVP.

## 2.5. Paramètres de confidentialité et protection de la vie privée par défaut

**En vigueur le 22 septembre 2023**

**Plus haut niveau de confidentialité.** La Loi 64 prévoit qu'un organisme 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 (art. 63.6.1). Cette exigence ne s'applique toutefois pas aux témoins de connexions (*cookies*) (art. 63.6.1 al. 2). Selon le libellé de la disposition, nous comprenons qu'elle ne s'applique pas non plus à un produit ou service destiné aux employés d'un organisme (intranet, application mobile pour employés, etc.) Notons que l'article 63.6.1 ne fournit aucun qualificatif permettant de déterminer ce qui sera considéré comme étant « le plus haut niveau de confidentialité » dans un contexte donné. Cette disposition risque donc de causer des défis d'interprétation pour les organismes publics.

**Protection de la vie privée dès la conception.** Cette exigence est similaire à l'approche de « protection de la vie privée dès la conception » que l'on retrouve notamment à l'article 25 du *Règlement général sur la protection des données* (« **RGPD** »). Cette approche vise à assurer le respect du droit à la vie privée à chaque étape du processus de développement d'une initiative, et rend toutes les parties prenantes responsables de veiller à ce qu'un produit ou un service particulier protège la vie privée. L'obligation sous la Loi 64 semble toutefois avoir une portée beaucoup plus restreinte, puisqu'elle ne vise que les paramètres de confidentialité et non le cycle complet de développement d'un produit ou service.

**Témoins de connexion.** L'interaction du nouvel article 63.6.1 avec l'article 65.0.1 en matière de témoins de connexion suscite une certaine confusion. Alors que le législateur a pris soin d'exclure expressément les témoins de connexion du champ d'application de l'article 63.6.1, il ne les a pas exclus de la portée de l'article 65.0.1. L'article 65.0.1 prévoit que les organismes doivent informer les individus des moyens d'activer les technologies permettant d'effectuer un profilage, ce qui pourrait comprendre les témoins de connexion. La CAI semble interpréter cette disposition comme une obligation de désactiver les fonctions de profilage par défaut (voir la section 3.1 pour plus de détails à ce sujet).

### Pistes de conformité

1. **Effectuer un inventaire des produits ou services technologiques offerts au public qui recueillent des renseignements personnels et qui disposent de paramètres de confidentialité.**
2. **Déterminer si les paramètres de ces produits ou services technologiques sont fixés au plus haut niveau de confidentialité, sans aucune intervention de la personne concernée.**

# 3. Transparence et consentement

La Loi 64 clarifie les règles applicables en matière de transparence et de consentement dans la Loi sur l'accès.

## 3.1. Transparence et obligation d'information préalable au consentement

**En vigueur le 22 septembre 2023**

**Obligation de transparence.** La Loi 64 modifie l'article 65 de la Loi sur l'accès pour y ajouter certains éléments qui doivent être communiqués à la personne concernée lors de la collecte de ses renseignements personnels ou dans certains cas, sur demande de la personne :

- **Lors de la collecte.** L'organisme qui recueille des renseignements personnels auprès d'un individu doit, lors de la collecte et par la suite sur demande, l'informer : (i) du nom de l'organisme public au nom de qui la collecte est faite; (ii) des fins auxquelles ces renseignements sont recueillis; (iii) des moyens par lesquels les renseignements sont recueillis; (iv) du caractère obligatoire ou facultatif de la demande; (v) des conséquences pour la personne concernée ou, selon le cas, pour le tiers, d'un refus de répondre à la demande ou, le cas échéant, d'un retrait de son consentement à la communication ou à l'utilisation des renseignements recueillis suivant une demande facultative; (vi) des droits d'accès et de rectification prévus par la loi; (vii) du nom du tiers pour qui la collecte est faite; (viii) du nom des tiers ou des catégories de tiers à qui il est nécessaire de communiquer les renseignements aux fins auxquelles ces renseignements sont recueillis; (ix) de la possibilité que les renseignements soient communiqués à l'extérieur du Québec (art. 65 al. 1 et 2).
- **Sur demande.** Un organisme doit également informer, sur demande, la personne concernée : (i) des renseignements personnels recueillis auprès d'elle; (ii) des catégories de personnes qui ont accès à ces renseignements au sein de l'organisme; (iii) de la durée de conservation de ces renseignements; (iv) des coordonnées du responsable de la PRP (art. 65 al. 3).

**Technologie d'identification, de localisation et de profilage.** Un organisme qui recueille des renseignements personnels en ayant recours à une technologie permettant d'identifier, de localiser ou d'effectuer le profilage d'une personne doit préalablement l'informer du recours à une telle technologie et des moyens offerts pour l'activer (art. 65.0.1 al. 1 (1) et (2)). Notons que cette exigence touche autant les employés que les citoyens, les visiteurs de sites Internet ou tout autre individu qui interagit avec l'organisme. Cette disposition vise donc toute collecte de renseignements personnels par l'entremise de certains types de technologies :

- **Identification** : une technologie a des fonctions d'identification lorsqu'elle permet de distinguer une personne par rapport à une autre. La reconnaissance faciale (et toute autre technique de reconnaissance biométrique) est un exemple de technologie ayant des fonctions d'identification.
- **Localisation** : une technologie a des fonctions de localisation lorsqu'elle permet d'indiquer où une personne se trouve à un moment donné (par exemple, un système de positionnement GPS).

- **Profilage** : la notion de « profilage » est englobante et s'entend de la collecte et de l'utilisation de renseignements personnels afin « d'évaluer certaines caractéristiques d'une personne physique, notamment à des fins d'analyse du rendement au travail, de la situation économique, de la santé, des préférences personnelles, des intérêts ou du comportement de cette personne » (art. 65.0.1 al. 2). Le profilage concerne la situation singulière de la personne et ne vise pas la collecte et l'utilisation de données pour générer des statistiques sur un groupe.

L'interprétation de l'article 65.0.1 soulève des difficultés puisqu'il n'est pas clair si cette disposition constitue le simple prolongement de l'obligation de transparence prévue à l'article 65 de la Loi sur l'accès ou s'il s'agit d'une restriction concrète à l'utilisation de technologies de localisation, d'identification et de profilage. Notons que la CAI mentionne sur son site Web que « ces technologies ne pourront être activées par défaut, ce sera à la personne concernée de les activer si elle le souhaite ».

**Politique de confidentialité.** La Loi 64 prévoit en outre qu'un organisme qui recueille des renseignements personnels par un moyen technologique doit publier une politique de confidentialité rédigée en termes simples et clairs sur son site Internet (art. 63.4). La Loi 64 ne définit toutefois pas la notion de « moyen technologique », mais celle-ci devrait recevoir une interprétation large vu les termes utilisés. Par exemple, la collecte de renseignements personnels par l'entremise de témoins de connexion, de balises Web ou de formulaires en ligne pourrait être visée par cette disposition. Une politique de confidentialité constitue l'outil privilégié pour que l'organisme puisse remplir son obligation de transparence et informer les personnes concernées de tous les éléments que nous avons précédemment mentionnés.

**Prise de décision automatisée.** La Loi 64 introduit également des exigences de transparence pour un organisme utilisant des algorithmes (notamment l'intelligence artificielle) à des fins décisionnelles (art. 65.2). Voir les sections 4.3 et 5.2 pour les détails quant à ces exigences.

## Pistes de conformité

1. **Mettre à jour ou établir la politique de confidentialité de l'organisme.** S'assurer que les éléments suivants soient inclus en termes simples et clairs :
   - fins auxquelles et moyens par lesquels les renseignements personnels sont recueillis;
   - droits d'accès, de rectification et de retrait du consentement;
   - nom du tiers pour qui la collecte est faite (le cas échéant);
   - catégories de fournisseurs de services ou d'organismes partenaires (le cas échéant);
   - transfert des renseignements à l'extérieur du Québec (le cas échéant).

→ Suite à la page suivante

### Pistes de conformité

2. **Développer et mettre en place un processus visant à répondre aux questions et aux demandes d'information de la part de citoyens ou d'employés concernant :**
   - la nature des renseignements personnels recueillis par l'organisme;
   - les catégories d'employés qui pourraient avoir accès aux renseignements personnels au sein de l'organisme;
   - la durée de conservation des renseignements;
   - les coordonnées du responsable de la PRP;
   - la source des renseignements lorsque ceux-ci sont recueillis auprès d'un autre organisme.
3. **Faire l'inventaire des technologies qui collectent des renseignements personnels de citoyens ou d'employés afin de les identifier, de les localiser ou de les profiler.**

   Le cas échéant, pour chaque technologie :
   - Réviser la politique ou procédure applicable (ou autres documents ou formulaires de consentement) et s'assurer que ces documents : (i) informent les personnes concernées préalablement du recours à ladite technologie visée; et (ii) offrent les moyens pour l'activer.
4. **Déterminer si des renseignements personnels (de citoyens ou d'employés) sont recueillis par l'entremise de moyens technologiques. Le cas échéant :**
   - Faire l'inventaire de ces moyens technologiques.
   - Publier une politique de confidentialité (en termes simples et clairs) sur le site Internet de l'organisme.
   - Mettre en place une procédure pour s'assurer que les personnes concernées seront adéquatement informées de toute modification à la politique de confidentialité.

## 3.2. Exigences du consentement : Forme et validité

**En vigueur le 22 septembre 2023**

La Loi 64 apporte certaines précisions par rapport à la forme du consentement, aux critères de validité du consentement et aux exigences relatives à l'obtention du consentement de mineurs.

**Forme du consentement.** Pour ce qui est de la forme du consentement, la Loi 64 reconnaît la possibilité pour un organisme de s'appuyer sur un consentement implicite pour utiliser et communiquer des renseignements personnels conformément aux fins énoncées dans sa politique de confidentialité (art. 65.0.2). La Loi 64 mentionne également qu'un renseignement personnel ne peut être utilisé au sein d'un organisme qu'aux fins pour lesquelles il a été recueilli, ni communiqué à un tiers, à moins que l'individu n'y consente ou que la présente Loi ne le prévoit, lequel consentement doit être manifesté de façon

expresse dès qu'il s'agit d'un renseignement personnel sensible (art. 59 et 65.1). Un renseignement sensible est défini comme un renseignement qui, de par sa nature notamment médicale, biométrique ou autrement intime, ou en raison du contexte de son utilisation ou de sa communication, suscite un haut degré d'attente raisonnable en matière de vie privée (art. 59 al. 3).

**Validité du consentement.** La Loi 64 précise qu'un consentement valide doit être manifeste, libre, éclairé et être donné à des fins spécifiques et demandé à chacune de ces fins, en termes simples et clairs (art. 53.1 al. 1). De plus, lorsqu'une demande de consentement est effectuée par écrit, l'organisme doit s'assurer que celle-ci est présentée distinctement de toute autre information communiquée à la personne concernée. Cet accent mis sur le caractère « distinct » du consentement semble impliquer une séparation claire des informations liées à l'obtention du consentement au traitement des renseignements personnels et des informations concernant d'autres sujets, par exemple les modalités d'utilisation des services de l'organisme. Lorsqu'une personne le requiert, l'organisme doit lui prêter assistance afin de l'aider à comprendre la portée du consentement demandé.

**Consentement des mineurs.** Le consentement du mineur de moins de 14 ans est donné par le titulaire de l'autorité parentale ou par le tuteur (art. 53.1 al. 2 et 64.1) et le consentement du mineur de 14 ans et plus peut être donné par le mineur, par le titulaire de l'autorité parentale ou alors par le tuteur.

## Pistes de conformité

1. **Faire l'inventaire des renseignements personnels recueillis, utilisés et communiqués par l'organisme** (citoyens et employés) afin de déterminer :
   - ceux qui sont de nature sensible;
   - ceux appartenant à des mineurs;
   - ceux qui sont exclus du champ d'application de la Loi (c.-à-d. coordonnées d'affaires).
2. **Faire l'inventaire des formulaires de consentement** ou autres documents utilisés pour obtenir le consentement des individus concernés (citoyens ou employés) et les réviser afin de s'assurer que :
   - Tout consentement obtenu est manifeste, libre, et éclairé.
   - Tout consentement est donné à des fins spécifiques en termes simples et clairs.
   - Lorsque la demande de consentement est faite par écrit, elle est présentée distinctement de toute autre information communiquée à la personne concernée.
   - Le consentement du mineur de moins de 14 ans est obtenu par le titulaire de l'autorité parentale ou par le tuteur.
   - Le consentement du mineur de 14 ans et plus est obtenu par le mineur, le titulaire de l'autorité parentale ou alors par le tuteur.
3. **Mettre en place une procédure pour répondre à une demande d'assistance de la part d'une personne concernée (citoyen ou employé) afin de l'aider à comprendre la portée du consentement qu'elle s'apprête à donner.**

## 3.3. Exceptions à l'exigence du consentement

**En vigueur le 22 septembre 2023**

**Sauf en ce qui concerne la communication à des fins d'étude, de recherche ou deproduction de statistiques (22 septembre 2022)**

La Loi 64 exclut certaines informations du champ d'application de la Loi sur l'accès et introduit également des exceptions au consentement quant à certaines utilisations ou communications de renseignements personnels.

**Cordonnées d'affaires.** La Loi 64 exclut les coordonnées d'affaires du champ d'application de la Loi sur l'accès, soit les « renseignements personnels concernant l'exercice par la personne concernée d'une fonction au sein d'une entreprise, tels que son nom, son titre et sa fonction, de même que l'adresse, l'adresse de courrier électronique et le numéro de téléphone de son lieu de travail » (art. 55 al. 1).

**Utilisation sans consentement.** La Loi 64 introduit une nouvelle exception au consentement à l'article 65.1 de la Loi sur l'accès soit celle concernant l'utilisation d'un renseignement personnel dépersonnalisé à des fins d'étude, de recherche ou de production de statistiques. Ainsi, un organisme public peut utiliser des renseignements personnels à d'autres fins que celles pour lesquelles il a été initialement recueilli, sans le consentement de la personne concernée, dans les situations suivantes :

- **Fins compatibles** : lorsque son utilisation est à des fins compatibles avec celles pour lesquelles il a été recueilli (art. 65.1 al. 2 (1)).
- **Intérêt de l'individu** : lorsque son utilisation est manifestement au bénéfice de la personne concernée (art. 65.1 al. 2 (2)).
- **Application d'une loi** : lorsque son utilisation est nécessaire à l'application d'une loi au Québec ((art. 65.1 al. 2 (3)).
- **Recherche** : lorsque l'utilisation est nécessaire à des fins d'étude, de recherche ou de production de statistiques et qu'il est dépersonnalisé (art. 65.1 al. 2 (4)). Voir la section 4.2 pour des détails au sujet de la définition de renseignement « dépersonnalisé ».

**Communication sans consentement.** En vertu de la Loi 64, un renseignement personnel pourra être communiqué sans le consentement de la personne concernée, dans les situations suivantes :

- **Contexte d'impartition** : lorsque la communication est nécessaire à l'exercice d'un mandat ou à l'exécution d'un contrat de service et que des mesures de protection des renseignements personnels sont prévues (art. 67.2). Voir la section 6.1 pour plus de détails sur cette exception.
- **Recherche** : lorsque la communication s'effectue à une personne ou à un organisme qui souhaite utiliser les renseignements à des fins d'étude, de recherche ou de production de statistiques et que les mesures de protection des renseignements personnels prévues à la Loi sont mises en place (art. 67.2.1 à 67.2.3). Nous notons que cette exception n'est pas assujettie à l'exigence que les renseignements soient dépersonnalisés (comme c'est le cas pour l'exception en matière d'utilisation à des fins d'étude, de recherche ou de production de statistiques internes à l'organisation) bien qu'un cadre spécifique s'applique à ces types de projets de recherche. Voir la section 4 pour des détails sur ce nouveau régime.

- **Situation d'urgence** : lorsque la communication est nécessaire en raison d'une situation d'urgence mettant en danger la vie, la santé ou la sécurité de la personne concernée (art. 59 al. 2 (4)).
- **Infraction** : lorsque la communication s'effectue à une personne ou à un organisme qui, en vertu de la loi, est chargé de prévenir, détecter ou réprimer le crime ou les infractions aux lois, si le renseignement est nécessaire aux fins d'une poursuite pour une infraction à une loi applicable au Québec (art. 59 al. 2 (3)).

**Registre des communications.** Notons que l'article 67.3 de la Loi sur l'accès prévoit en outre qu'un organisme public doit inscrire dans un registre toute communication de renseignements personnels effectuée sans le consentement de la personne concernée conformément aux articles 66, 67, 67.1, 67.2, 67.2.1 et 68 de la loi. Ce registre doit comprendre les éléments suivants :

- la nature ou le type de renseignement communiqué;
- la personne ou l'organisme qui reçoit cette communication;
- la fin pour laquelle ce renseignement est communiqué et une indication, le cas échéant, qu'il s'agit d'une communication de renseignements personnels à l'extérieur du Québec effectuée conformément l'article 70.1;
- la raison justifiant cette communication.

## Pistes de conformité

1. **Faire l'inventaire des utilisations pouvant faire l'objet d'une exception à l'exigence du consentement,** c'est-à-dire :
   - utilisation manifestement au bénéfice de la personne concernée;
   - utilisation à des fins compatibles avec celles pour lesquelles le renseignement a été recueilli;
   - utilisation nécessaire à l'application d'une loi au Québec;
   - utilisation nécessaire à des fins d'étude, de recherche ou de production de statistiques (et les renseignements sont dépersonnalisés).
2. **Faire l'inventaire des communications pouvant faire l'objet d'une exception à l'exigence du consentement,** c'est-à-dire :
   - communication nécessaire à l'exercice d'un mandat ou à l'exécution d'un contrat de service;
   - communication à une personne ou à un organisme qui souhaite utiliser les renseignements à des fins d'étude, de recherche ou de production de statistiques;
   - communication nécessaire en raison d'une situation d'urgence mettant en danger la vie, la santé ou la sécurité de la personne concernée;

→ Suite à la page suivante

## Pistes de conformité

- communication à une personne ou à un organisme qui est chargé de prévenir, détecter ou réprimer le crime ou les infractions aux lois et les renseignements sont nécessaires à la poursuite d'une infraction à une loi applicable au Québec.

3. **Inscrire dans un registre toute communication de renseignements personnels effectuée en vertu des articles 66, 67, 67.1, 67.2, 67.2.1 et 68 de la Loi sur l'accès.**

4. **Réviser la politique de confidentialité et les formulaires de consentement afin de :**

- Refléter les exceptions à l'exigence de consentement et structurer ces documents de telle sorte que les utilisations ou communications exemptes de consentement soient mieux reflétées.

# 4. Recherche et prise de décision automatisée

La Loi 64 introduit des modifications importantes à la Loi sur l'accès afin d'assouplir le régime applicable en matière de recherche. Des obligations importantes sont également introduites en ce qui concerne les décisions prises au moyen de technologies qui effectuent un « traitement automatisé » de renseignements personnels. Bien que non définie par la Loi 64, cette notion semble clairement viser les algorithmes d'apprentissage automatique et les autres technologies associées au domaine de l'intelligence artificielle qui sont en mesure de prendre des décisions sophistiquées sans supervision humaine.

## 4.1. Exception au consentement pour la communication à des fins de recherche

**En vigueur le 22 septembre 2022**

La Loi 64 abroge la procédure d'autorisation prévue à l'article 125 de la Loi sur l'accès, longtemps critiquée pour ses difficultés pratiques et pour l'incertitude engendrée par le pouvoir discrétionnaire de la CAI en matière d'évaluation des demandes d'autorisation des communications de renseignements personnels à des fins de recherche et son pouvoir de révocation.

Le régime introduit par les nouveaux articles 67.2.1 à 67.2.3 de la Loi sur l'accès permet aux parties souhaitant partager des renseignements personnels à des fins de recherche de procéder elles-mêmes à l'évaluation de la demande de communication. Le nouveau régime met l'accent sur la vérification diligente et la transparence, et exige seulement d'informer la CAI de l'entente intervenue entre l'organisme divulgateur et la personne requérante (entreprise, organisme public ou chercheur individuel), ainsi que des violations de l'entente ou des événements susceptibles de porter atteinte à la confidentialité des renseignements personnels.

**Évaluations des facteurs relatifs à la vie privée (EFVP)**. Le nouvel article 67.2.1 prévoit que les renseignements personnels peuvent être communiqués une personne ou à un organisme qui souhaite utiliser ces renseignements à des fins d'étude, de recherche ou de production de statistiques si une EFVP arrive aux conclusions suivantes :

- Les renseignements personnels sont nécessaires pour atteindre l'objectif de la recherche;
  - En d'autres termes, si l'objectif de la recherche peut être atteint au moyen de renseignements anonymisés, l'organisme public ne doit pas communiquer de renseignements personnels. Les articles 67.2.1 et les suivants ne s'appliquent pas, car les renseignements dûment anonymisés ne constituent pas des renseignements personnels. Par ailleurs, si l'objectif peut être atteint avec des renseignements dépersonnalisés, l'organisme public doit privilégier la communication de tels renseignements et respecter l'ensemble des conditions prévues aux articles 67.2.1 à 67.2.3. Voir la section 4.2 pour la distinction entre les renseignements anonymisés et les renseignements dépersonnalisés.

- Il est déraisonnable d'exiger de la personne requérante qu'elle obtienne le consentement;
  - Pour ce critère, on peut tenir compte, par exemple, de la difficulté de joindre les personnes ou de leur nombre important. Si l'organisme public juge que le demandeur peut raisonnablement obtenir le consentement des personnes concernées à la communication de leurs renseignements personnels, il doit refuser de communiquer ces renseignements sans leur consentement.
- L'objectif de la recherche l'emporte, eu égard à l'intérêt public, sur l'impact de la communication sur le droit à la vie privée des personnes concernées;
  - Ce critère de proportionnalité implique d'évaluer les bienfaits appréhendés du projet par rapport au niveau de risque qu'il pourrait engendrer sur la vie privée des personnes concernées. Les risques sur la vie privée des personnes concernées dépendent notamment de la sensibilité des renseignements personnels, de leur quantité et de leur utilisation. L'organisme public peut s'appuyer, si le cas le permet, sur la décision documentée d'un comité d'éthique de la recherche afin de déterminer si le critère de proportionnalité milite en faveur de la communication des renseignements personnels ou non. Ce document doit être transmis par la personne requérante en soutien à sa demande.
- Les renseignements sont utilisés de manière à en assurer la confidentialité;
  - Un organisme public doit refuser la communication si le projet implique une diffusion de renseignements personnels au grand public ou si l'utilisation prévue de ces renseignements ne garantit pas le maintien de leur caractère confidentiel. En vertu de l'article 67.2.2, la personne requérante doit notamment exposer les motifs pouvant soutenir que les renseignements personnels sont utilisés de manière à en assurer la confidentialité. Un tel exposé doit minimalement comprendre les mesures de protection que le demandeur met en place pour en assurer la confidentialité.
- Seuls les renseignements nécessaires sont communiqués.
  - L'EFVP doit comprendre une analyse de la nécessité de communiquer chaque type de renseignement demandé afin que l'organisme public ne communique que les renseignements qui sont réellement nécessaires à l'étude, à la recherche ou à la production de statistiques.

Soulignons que l'article 67.2.1 al. 2 de la Loi sur l'accès ne précise pas quelle partie doit entreprendre l'EFVP. En général, cette tâche revient à l'organisme qui est en contrôle des renseignements personnels. En l'occurrence, il s'agit vraisemblablement de l'organisme à qui la demande de communication est adressée qui devra donc procéder à une EFVP préalable à la communication. D'ailleurs, l'organisme divulgateur prendrait un risque important en se fiant à une EFVP réalisée par la personne requérante, car celle-ci pourrait, dans son propre intérêt, ne pas avoir identifié tous les risques pertinents du point de vue de l'organisme divulgateur. La personne requérante deviendrait de facto responsable des renseignements personnels dès leur réception, considérant qu'il n'y a pas de relation de fournisseur de services dans ce contexte. Ainsi, en l'absence de lignes directrices de la CAI à ce sujet, les organismes devraient faire preuve de prudence et supposer que l'article 67.2.1 de la Loi sur l'accès sera interprété comme exigeant de chaque partie à la communication qu'elle procède à sa propre EVFP, ou à tout le moins qu'elle participe activement à une EVFP conjointe, dans le cadre de son obligation de diligence raisonnable préalable à la communication.

**Ressources.** Les organismes qui communiquent des renseignements personnels à des fins de recherche doivent être prêts à estimer le coût d'une telle évaluation, qui nécessitera généralement la contribution du service juridique de l'organisme ou d'un conseiller juridique externe. Le coût de réalisation d'une EFVP (réalisée par l'organisme divulgateur ou en collaboration avec la personne requérante) peut être important et, quelle que soit la structure de l'entente avec la personne requérante, les coûts associés à cet exercice pour l'organisme divulgateur doivent y être comptabilisés.

**Obligations des personnes requérantes.** Pour sa part, la personne requérante doit formuler sa demande par écrit et fournir à l'organisme toute l'information utile au soutien de sa demande, à savoir une présentation détaillée des activités de recherche, les arguments à l'effet que les critères de l'EFVP requis par l'article 67.2.1 sont remplis, la liste des personnes et organismes à qui des demandes similaires sont faites ainsi que, le cas échéant, la description des technologies qui seront utilisées pour le traitement des renseignements, et la décision documentée d'un comité d'éthique de la recherche relative à cette recherche (article 67.2.2). Dans le cadre de ses efforts de vérification diligente préalable à la communication des renseignements, l'organisme divulgateur doit s'assurer que la personne requérante lui a fourni toute l'information et la documentation énoncées à l'article 67.2.2.

**Dispositions obligatoires de l'entente.** Le nouvel article 67.2.3 prévoit que les deux parties à la communication de renseignements personnels à des fins de recherche doivent conclure une entente stipulant notamment que les renseignements :

- ne peuvent être rendus accessibles qu'aux personnes qui ont besoin d'y avoir accès dans le cadre de leurs fonctions et seulement s'ils ont signé un engagement de confidentialité;
- ne peuvent être utilisés à des fins différentes de celles prévues à la présentation détaillée des activités de recherche;
- ne peuvent être appariés avec tout autre fichier de renseignements non prévu dans la présentation détaillée des activités de recherche;
- ne peuvent être communiqués, publiés ou autrement diffusés sous une forme permettant d'identifier les personnes concernées.

Cette entente doit également prévoir :

- les informations devant être communiquées aux personnes concernées lorsque des renseignements personnels les concernant sont utilisés pour les joindre en vue de leur participation à l'étude ou à la recherche;
- des mesures pour assurer la protection des renseignements;
- un délai de conservation des renseignements;
- l'obligation d'aviser l'organisme qui communique les renseignements de la destruction de ceux-ci;
- que l'organisme qui communique les renseignements et la CAI doivent être avisés sans délai : (i) du non-respect de toute condition prévue à l'entente; (ii) de tout manquement aux mesures de protection prévues à l'entente; (iii) de tout événement susceptible de porter atteinte à la confidentialité des renseignements.

**Présentation de l'entente à la CAI.** L'entente devra être transmise à la CAI et entrera en vigueur 30 jours après sa réception par celle-ci. Bien que les dispositions de l'article 67.2.3 n'accordent pas à la CAI le pouvoir de résilier l'entente si celle-ci ne remplit pas toutes les exigences, la CAI pourrait ordonner à l'organisme divulgateur de ne pas communiquer les renseignements jusqu'à ce que l'entente soit révisée pour inclure les éléments requis. Cela dit, faute de lignes directrices à ce sujet, on peut considérer qu'à l'expiration du délai de 30 jours, la CAI aura moins d'autorité pour se prononcer sur une entente exécutoire.

**Registre des communications.** Une communication de renseignements personnels à un fournisseur de services sans le consentement de la personne concernée doit être inscrite dans un registre conformément à l'article 67.3 de la Loi sur l'accès (voir la section 3.3 à ce sujet).

### Pistes de conformité

1. **Mettre en place une procédure pour traiter les demandes de communication de renseignements personnels à des fins d'étude, de recherche ou de production de statistiques.** Celle-ci devrait notamment prévoir :
   - que l'organisme doit recevoir toute la documentation énoncée à l'article 67.2.2 avant de procéder à la communication;
   - que l'organisme doit réaliser une EFVP avant de procéder à la communication;
   - que l'organisme doit conclure une entente qui répond aux exigences de l'article 67.2.3 avant de procéder à la communication.
2. **Remettre une copie de cette entente à la CAI au moins 30 jours avant la communication des renseignements.**

## 4.2. Exception au consentement pour la recherche et les analyses internes

**En vigueur le 22 septembre 2023**

La Loi 64 modifie l'article 65.1 de la Loi sur l'accès afin d'autoriser les organismes à utiliser, sans le consentement des personnes concernées, les renseignements personnels à des fins d'analyses internes.

**Étude ou recherche à partir de renseignements dépersonnalisés.** L'article 65.1 al. 2(4) prévoit que l'utilisation d'un renseignement personnel sans consentement sera permise lorsque son utilisation est « nécessaire à des fins d'étude, de recherche ou de production de statistiques et qu'il est dépersonnalisé ». Étant donné que l'exception au consentement prévue à l'article 65.1 s'applique à

l'utilisation des renseignements personnels au sein de l'organisme, il est tout naturel d'interpréter les termes « étude » ou « recherche » comme termes l'analyse de données afin d'acquérir des connaissances permettant à l'organisme d'orienter sa prise de décision et d'influencer ses actions. Toutefois, l'exception s'étend également à d'autres formes d'activités de recherche internes, notamment celles qui font appel à l'apprentissage automatique ou à d'autres techniques avancées d'analyse des données susceptibles d'être impliquées dans le développement de systèmes décisionnels automatisés (examinés plus en détail dans la section 4.3).

**Dépersonnalisation ou anonymisation.** Le nouvel article 65.1 prévoit qu'un renseignement personnel est « dépersonnalisé lorsqu'il ne permet plus d'identifier directement la personne concernée » (art. 65.1 al. 5). Cette définition correspond essentiellement à la notion de « pseudonymisation » des données, telle qu'elle est généralement comprise (notamment dans le RGPD). À titre comparatif, la Loi 64 prévoit également des critères pour l'anonymisation des renseignements personnels en précisant que « [p]our l'application de la présente loi, un renseignement concernant une personne physique est anonymisé lorsqu'il ne permet plus, de façon irréversible, d'identifier directement ou indirectement cette personne » (art. 73 [notre emphase]). Il est intéressant de noter que le libellé du nouvel article 65.1 prévoit aussi clairement qu'aucun consentement n'est nécessaire même lorsque ces renseignements sont sensibles préalablement à leur anonymisation (art. 65.1 al. 1 et 2).

**Diligence dans l'utilisation de renseignements dépersonnalisés.** Le nouvel article 65.1 reconnaît également le risque de réidentification lié aux renseignements dépersonnalisés en obligeant les organismes qui les utilisent à prendre « les mesures raisonnables afin de limiter les risques que quiconque procède à l'identification d'une personne physique à partir de renseignements dépersonnalisés » (art. 65.1 al. 6). D'ailleurs, bien que cela ne soit pas expressément indiqué, il serait conforme à la définition des renseignements personnels sensibles prévue à l'article 65.1 al. 5 (ainsi qu'aux orientations de la CAI et des autres commissaires canadiens à la protection de la vie privée) d'interpréter les « mesures raisonnables » comme nécessitant l'adoption de mesures supplémentaires ou plus rigoureuses lorsque les renseignements personnels sous-jacents aux renseignements dépersonnalisés sont sensibles.

**Évaluation des facteurs relatifs à la vie privée.** La recherche interne menée en vertu de l'art. 65.1 al. 2 (1) ou (4) nécessite la réalisation d'une EFVP lorsqu'elle s'inscrit dans le cadre d'un projet d'acquisition, de développement ou de refonte d'un système d'information ou de prestation électronique de services (art. 63.5 al. 1) (voir la section 2.4).

### Pistes de conformité

1. **Mettre en place une procédure pour s'assurer qu'avant d'utiliser des renseignements personnels à des fins d'analyses internes, l'organisme a :**
   - obtenu le consentement pour cette utilisation;
   - déterminé que la finalité de la recherche est compatible avec la finalité pour laquelle les renseignements ont été recueillis;
   - dépersonnalisé (c'est-à-dire, au minimum, pseudonymisé) les renseignements personnels.
2. **Prendre les mesures nécessaires pour réduire le risque de réidentification,** lorsque l'organisme utilise des renseignements dépersonnalisés.
3. **Adopter des mesures encore plus rigoureuses pour éviter la réidentification** lorsque les renseignements personnels sous-jacents aux renseignements dépersonnalisés sont sensibles.
4. **Mettre en place une procédure visant à effectuer une EFVP** si la recherche interne (en vertu de l'une ou l'autre des exceptions discutées) s'inscrit dans le cadre d'un « projet d'acquisition, de développement et de refonte d'un système d'information ou de prestation électronique ».

## 4.3. Prise de décision automatisée

**En vigueur le 22 septembre 2023**

Le nouvel article 65.2 introduit une obligation de transparence pour les organismes qui prennent une décision concernant une personne qui est fondée exclusivement sur un traitement automatisé de ses renseignements personnels. Il pourrait s'agir, par exemple, de situations où un organisme décide d'accorder ou de refuser l'accès à un produit ou à un service en se basant sur l'évaluation de la situation financière ou médicale d'un citoyen.

**Définition.** Afin de déterminer l'application de l'article 65.2, il convient de :

- **Identifier la présence d'une « décision » prise à partir de renseignements personnels**
  On entend, par décision, « l'action de décider, de prendre position à l'égard d'une situation précise suivant un processus qui peut être plus ou moins élaboré. Par extension, son résultat. » Une décision doit donc permettre à l'organisme de prendre une position précise sur une personne et d'avoir un effet sur celle-ci (par exemple, des conséquences juridiques).

- **Conclure que la décision est fondée exclusivement sur un traitement automatisé des renseignements personnels**
  Une décision fondée exclusivement sur un traitement automatisé est celle qui a été prise sans aucune intervention humaine (par exemple, par l'entremise d'un algorithme). Cela signifie qu'aucune personne physique n'a exercé un contrôle important dans la décision. Il faut donc comprendre, par exemple, qu'une intervention humaine mineure, c'est-à-dire qui n'a pas de répercussion réelle sur la décision, n'a pas pour effet d'écarter l'application de l'article 65.2 de la Loi sur l'accès.

**Exigences en matière de notification et d'information.** L'article 65.2 exige que les organismes informent les personnes concernées du fait que leurs renseignements personnels sont utilisés pour prendre une décision fondée exclusivement sur un traitement automatisé, au plus tard au moment où la personne est informée de la décision elle-même. D'un point de vue pratique, on peut penser que des avis distincts ou « juste à temps » pourraient être exigés en vertu des futures lignes directrices de la CAI. Les organismes utilisant des technologies pour prendre des décisions basées exclusivement sur le traitement automatisé de renseignements personnels devraient en outre mentionner cette utilisation dans leur politique de confidentialité.

L'article 65.2 oblige également les organismes à informer, sur demande, la personne visée par une décision automatisée :

- des renseignements personnels utilisés pour rendre la décision;
- des raisons ainsi que des principaux facteurs et paramètres ayant mené à la décision;
- du droit de faire rectifier les renseignements personnels utilisés pour rendre la décision.

Notons que la formulation utilisée ne limite pas l'obligation d'information aux renseignements personnels qui concernent la personne visée par la décision. Bien qu'aucune interprétation de la loi n'exige que les renseignements personnels de tiers soient divulgués à la personne visée par une décision automatisée, il se pourrait que les organismes soient tenus de divulguer la nature de tous les renseignements personnels utilisés dans le cadre du processus décisionnel (par exemple, le fait que lors de la phase d'entraînement de l'algorithme on ait utilisé les noms de criminels reconnus coupables et les codes postaux de leur lieu de résidence). À cet égard, il importe de préciser que les technologies d'apprentissage automatique (*machine learning*) qui prennent des décisions concernant des individus peuvent avoir besoin d'ingérer une multitude de renseignements personnels provenant de différentes personnes afin de produire un modèle capable de prendre des décisions précises. Les lignes directrices de la CAI seront d'une importance capitale pour comprendre comment cette obligation de transparence devra être appliquée en pratique.

**Intervention humaine.** L'article 65.2 ne fournit pas d'indication à savoir ce qui constitue une « décision fondée exclusivement sur un traitement automatisé de renseignements personnels ». Cela dit, il nous semble clair qu'une intervention significative d'une personne physique dans le processus décisionnel aura pour effet de rendre inapplicable cette nouvelle exigence.

Influence européenne. La CAI a fait du traitement automatisé l'un des thèmes de son « Espace évolutif » sur le projet de loi n° 64, ce qui illustre son intention d'émettre certaines lignes directrices à ce sujet. Il est donc raisonnable pour les organismes de s'attendre à la publication de telles orientations d'ici

l'entrée en vigueur de l'article 65.2. Il convient de mentionner que le terme « traitement automatisé » semble être repris du RGPD de l'UE et pourrait donc être interprété de manière similaire. En Europe, le Groupe de travail « Article 29 » sur la protection des données a émis, avant l'entrée en vigueur de la loi, des lignes directrices sur l'interprétation des dispositions du RGPD régissant le traitement automatisé (voir Groupe de travail « Article 29 » sur la protection des données, *Lignes directrices relatives à la prise de décision individuelle automatisée et au profilage aux fins du règlement 2016/679*). Notons que l'interprétation formulée par le Groupe de travail a été facilitée par le libellé restrictif des dispositions du RGPD qui visent un traitement automatisé « produisant des effets juridiques à l'égard d'une personne physique » ou « l'affectant de manière significative ». Le nouvel article 65.2 ne comporte pas de telles restrictions, ce qui compliquera sans doute le travail d'interprétation de la CAI. En l'absence de lignes directrices, les organismes peuvent toutefois se préparer aux nouvelles obligations de notification et d'information prévues par la Loi en envisageant de suivre avec prudence l'interprétation retenue dans le contexte européen pour déterminer si et dans quelles circonstances une technologie sera considérée comme un « traitement automatisé ».

**Explicabilité des algorithmes.** L'obligation d'informer la personne visée par une décision automatisée « des raisons et des principaux facteurs et paramètres » qui ont mené à la décision constitue une forme d'explication de la décision automatisée. Comme cela a été abondamment discuté dans la littérature au sujet de l'IA, les processus utilisés par les modèles d'apprentissage automatique pour parvenir à leurs résultats sont reconnus pour leur opacité. Dans de nombreux cas, l'explication fournie est soit superficielle au point d'être vide de sens ou bien si technique qu'elle est incompréhensible pour l'individu moyen. Bien que le terme « principaux » donne une indication quant au niveau de détail requis, les organismes doivent, en l'absence de lignes directrices, faire preuve de prudence afin d'éviter de communiquer des renseignements qui pourraient (i) révéler des secrets commerciaux ou violer le droit de propriété intellectuelle du concepteur du système automatisé ou (ii) permettre à des tiers mal intentionnés de s'infiltrer dans leurs systèmes.

**Droit de présenter des observations.** En outre, la personne qui fait l'objet de la décision automatisée doit avoir « l'occasion de présenter ses observations à un membre du personnel de l'organisme public en mesure de réviser la décision » (art. 65.2 al. 3). Les activités de traitement automatisé doivent donc, sur demande, être examinées par du personnel ayant le pouvoir (et, vraisemblablement, les connaissances suffisantes) de réévaluer les décisions prises par le système. Il est intéressant de noter que l'article 65.2 n'accorde pas aux personnes visées un droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé (comme celui prévu à l'article 22 du RGPD), mais uniquement un droit de « présenter ses observations ». Ceci semble accorder au personnel chargé de la révision une grande latitude dans son évaluation de la décision automatisée après réception des observations de la personne concernée. En d'autres termes, l'organisme ne semble pas avoir d'obligation distincte de délibérer et de parvenir à une conclusion indépendante ou de fournir une justification quant à son choix de réviser ou non la décision. Les organismes seront donc en mesure de trier les demandes non fondées et ainsi éviter les frais administratifs importants liés à la gestion de telles demandes. Néanmoins, ils doivent être prêts à évaluer les observations soumises par les personnes concernées et à agir de manière appropriée lorsque l'examen de la décision et des observations révèle clairement un problème dans le processus de traitement automatisé ou la manière dont les renseignements personnels sont utilisés.

## Pistes de conformité

1. **Se préparer à agir en fonction des orientations qui seront publiées par la CAI concernant l'interprétation de la notion de « traitement automatisé ».** En l'absence de telles orientations, les organismes peuvent considérer l'interprétation donnée au « traitement automatisé » en vertu du RGPD de l'UE, en faisant preuve toutefois d'une certaine prudence.

2. **Mettre en place une procédure pour s'assurer que lorsqu'un organisme prend des décisions fondées exclusivement sur le traitement automatisé de renseignements personnels, il verra à :**
   - En informer les individus par l'entremise de sa politique de confidentialité;
   - Mettre en place une procédure conformément aux pistes de conformité prévues dans la section 5.

3. **Faire preuve de prudence dans la communication des raisons ayant mené à la décision, qui pourraient :**
   - Révéler des secrets commerciaux ou violer le droit de propriété intellectuelle du concepteur du système automatisé;
   - Permettre à des tiers mal intentionnés d'infiltrer le système.

4. **Se préparer à évaluer les observations des personnes concernées relatives à une décision prise par traitement automatisé** et à agir de manière appropriée lorsque l'examen de la décision et des observations révèle clairement un problème dans le processus de traitement automatisé ou la manière dont les renseignements personnels sont utilisés.

# 5. Nouveaux droits individuels

La Loi 64 introduit de nouveaux droits individuels dans la Loi sur l'accès, notamment un droit à la portabilité des données et un droit d'être informé d'une prise de décision automatisée et de s'y opposer. En outre, la Loi 64 renforce le contrôle individuel et les droits existants en matière de protection des renseignements personnels en permettant aux personnes concernées de demander aux organismes des informations supplémentaires sur le traitement de leurs données.

## 5.1. Droit à la portabilité des données

**En vigueur le 22 septembre 2024**

Considéré comme une extension au droit d'accès, le droit à la portabilité des données accorde aux personnes concernées la possibilité de recevoir les renseignements personnels informatisés qu'un organisme a recueillis à leur sujet dans un **format technologique structuré et couramment utilisé**, et de voir ces renseignements transférés directement à « toute personne ou à tout organisme autorisé par la Loi à recueillir un tel renseignement » (art. 84 al. 3). Ces renseignements doivent également être communiqués sous la forme d'une **transcription écrite et intelligible** (art. 84 al. 2). Ainsi, l'objectif du droit à la portabilité des données semble être de faciliter la réutilisation des données et d'améliorer la capacité des citoyens à transférer leurs renseignements d'un organisme vers un autre. Bien que le droit à la portabilité des données ne vise pas nécessairement l'interopérabilité entre les systèmes, celle-ci est souvent présentée comme l'un de ses objectifs sous-jacents.

⚠ **Signification d'un « format technologique structuré et couramment utilisé ».** Les termes « structuré », « couramment utilisé » et « technologique » ne sont pas explicitement définis dans la Loi, et leur signification est susceptible de varier selon l'industrie ou le secteur concerné. Dans l'UE, l'ancien Groupe de travail Article 29 a publié des directives dans lesquelles il a estimé que les formats ouverts tels que CSV, XML et JSON, accompagnés de métadonnées utiles à la compréhension de leur signification, étaient conformes au droit de portabilité des données du RGDP lorsqu'aucun format communément utilisé n'était disponible. Cela dit, des lignes directrices seront nécessaires pour confirmer quels formats peuvent être considérés conformes aux exigences de la Loi 64.

**Portée du droit à la portabilité des données.** Le droit à la portabilité des données ne s'applique qu'aux renseignements personnels informatisés qui ont été recueillis auprès de la personne concernée. En d'autres termes, il ne s'applique pas aux renseignements détenus dans un format non informatisé, comme des documents papier, ou recueillis auprès d'un tiers. Le droit à la portabilité des données exclut également de son champ d'application les renseignements personnels qui ont été créés ou inférés à partir des renseignements recueillis auprès de la personne concernée. Les données inférées peuvent par exemple prendre la forme de déductions sur la probabilité qu'un citoyen sollicite

un service en particulier ou sur la probabilité qu'il soit intéressé à recevoir du contenu publicitaire particulier. Il convient de noter que la mise en œuvre de ce droit doit également être prise en compte lors de l'acquisition, du développement ou de la refonte d'un système d'information ou de prestation électronique de services impliquant la collecte, l'utilisation, la communication ou la destruction de renseignements personnels (art. 65.5 al. 1) (voir section 2.4). Bien qu'une plus grande clarté soit nécessaire en ce qui concerne certains aspects procéduraux associés au droit à la portabilité des données, son inclusion sous la section de la Loi sur l'accès portant sur le droit d'accès suggère que les organismes devraient traiter les demandes de portabilité des données conformément au régime actuel applicable aux demandes d'accès aux renseignements personnels.

**Exemptions à la portabilité des données.** Lorsque la fourniture des renseignements dans un format technologique structuré et couramment utilisé « soulève des difficultés pratiques sérieuses » pour l'organisme qui reçoit la demande, ce dernier peut être exempté de l'obligation de se conformer à cette exigence (art. 84 al. 3). En outre, le droit à la portabilité des données ne saurait s'appliquer aux renseignements qui sont autrement exemptés du droit d'accès, car la portabilité des données est considérée comme une extension de ce dernier (voir les articles 86 à 88.1). En ce sens, les renseignements personnels informatisés dont la divulgation risque de révéler des renseignements personnels sur un tiers sont susceptibles d'être exclus des exigences d'accès et de portabilité en vertu de l'article 88 de la Loi sur l'accès.

Enfin, il est important de noter que le droit à la portabilité des données est la seule disposition de la Loi 64 à entrer en vigueur le 22 septembre 2024, soit trois ans après la sanction de la loi.

## 5.2. Droit d'être informé d'une décision automatisée et de s'y opposer

**En vigueur le 22 septembre 2023**

La Loi 64 accorde aux personnes concernées trois nouveaux droits en ce qui concerne la prise de décision automatisée impliquant des renseignements personnels, à savoir (i) le droit d'en être informé, (ii) le droit de demander des informations supplémentaires sur la prise de décision automatisée, et (iii) le droit de soumettre des observations à une personne désignée au sein de l'organisme. Il convient de souligner que ces droits sont limités aux décisions basées « exclusivement » sur un traitement automatisé des renseignements personnels d'un individu, excluant ainsi les décisions basées sur une combinaison de traitement automatisé et d'intervention humaine significative.

**Droit d'être informé de la prise de décision automatisée.** Les personnes concernées ont le droit d'être informées du fait que leurs renseignements personnels sont utilisés pour prendre une décision fondée exclusivement sur un traitement automatisé. Voir la section 4.3 pour plus de détails sur cette nouvelle exigence.

**Droit de demander de l'information supplémentaire sur la prise de décision automatisée.**
Les personnes concernées peuvent également demander des informations supplémentaires concernant la prise de décision automatisée. Ils sont notamment en droit de connaître les renseignements personnels qui ont été utilisés pour rendre la décision, les raisons et les principaux facteurs et paramètres ayant mené à la décision et leur droit de faire rectifier les renseignements personnels utilisés pour rendre la décision. Voir la section 4.3 pour plus de détails sur cette nouvelle exigence. Étant donné qu'aucune modalité n'est imposée à l'exercice du droit de demander de l'information supplémentaire, un individu peut être autorisé à soumettre une demande verbalement ou par écrit. L'organisme doit néanmoins agir avec diligence et conserver une trace de ce type de demande, y compris la réponse de l'organisme à celle-ci, car le non-respect de cette exigence – ou de tout autre droit accordé en vertu de l'article 65.2 – peut donner lieu à l'imposition de sanctions (voir la section 1).

**Droit de présenter des observations à une personne désignée au sein de l'organisme.**
Les personnes concernées doivent avoir la possibilité de présenter leurs observations à un membre du personnel de l'organisme public et cette personne désignée doit être en mesure de réviser la décision. Voir la section 4.3 pour plus de détails sur cette nouvelle exigence.

## 5.3. Droit d'obtenir des renseignements sur le traitement des renseignements personnels

**En vigueur le 22 septembre 2023**

La Loi 64 permet aux personnes concernées de demander de l'information sur le traitement de leurs renseignements personnels, à savoir quels renseignements personnels ont été recueillis auprès d'eux et comment ils sont traités par l'organisme. En particulier, une personne pourrait demander de recevoir non seulement les informations qui lui ont été fournies au moment de la collecte, mais aussi des informations supplémentaires, comme les catégories de personnes qui ont accès à ses renseignements personnels au sein de l'organisme, la période de conservation applicable et les coordonnées du responsable de la PRP (art. 65 al. 3). Si des renseignements personnels ont été recueillis auprès d'un tiers, la personne concernée peut également demander à être informé de la source des renseignements, sauf si les renseignements ont été recueillis dans le cadre d'une enquête visant à prévenir, à détecter ou à réprimer un crime ou une infraction à la Loi (art. 65 al. 6). Pour plus de détails sur les exigences de transparence, voir la section 3.1. Notons que ce droit s'inscrit dans le cadre du droit d'accès, ce qui signifie qu'un organisme qui reçoit ce type de demande doit la traiter conformément à la procédure et aux délais applicables à une demande d'accès. En revanche, la Loi 64 sépare ces deux droits, créant ainsi un régime plus souple pour les demandes faites en vertu de l'article 65.

## Pistes de conformité

1. **Effectuer un inventaire des pratiques susceptibles de faire intervenir les nouveaux droits individuels** afin de déterminer si ces pratiques relèvent de l'une des situations suivantes:
   - L'organisme rend des décisions fondées exclusivement sur un traitement automatisé de renseignements personnels.
   - L'organisme collecte des renseignements personnels informatisés.
2. **Effectuer un inventaire des politiques et procédures existantes relatives au traitement des droits individuels et les examiner pour s'assurer que :**
   - L'organisme est capable de reconnaître et de répondre à une demande (verbale ou écrite) d'information sur le traitement des données.
   - L'organisme est en mesure de communiquer, sur demande, des renseignements personnels informatisés à la personne concernée, ou à une personne ou un organisme autorisé par la Loi à recueillir de tels renseignements, dans un format technologique structuré et couramment utilisé.
3. **Si l'organisme rend des décisions fondées exclusivement sur un traitement automatisé, mettre en place une procédure pour s'assurer que:**
   - L'organisme est en mesure d'informer les personnes concernées de ce fait au plus tard au moment où il les informe de la décision.
   - L'organisme est capable de reconnaître et de répondre à une demande (verbale ou écrite) d'information sur la prise de décision automatisée.
   - L'organisme a désigné un membre de son personnel qui est en mesure de réviser ces décisions et qui est chargé de recevoir les observations des personnes concernées.

# 6. Impartition et transfert de renseignements personnels à l'extérieur du Québec

La Loi 64 introduit de nouvelles exigences en matière d'impartition et de communication de renseignements à l'extérieur du Québec.

## 6.1. Impartition

**En vigueur le 22 septembre 2023**

**Transparence.** Comme l'indique la section 3.1, la Loi 64 requiert que l'organisme indique à la personne concernée, au moment de la collecte et par la suite sur demande, le nom des tiers ou des catégories de tiers à qui il est nécessaire de communiquer les renseignements pour accomplir les fins pour lesquelles les renseignements sont recueillis (art. 65 al. 2). Ceci implique que, désormais, la politique de confidentialité de l'organisme devra indiquer que les renseignements personnels pourront être transmis à ses fournisseurs de service (catégorie de tiers) ou nommer ceux-ci individuellement.

**Exception au consentement.** Notons que contrairement à la Loi sur le secteur privé, la Loi sur l'accès autorisait déjà les organismes publics à communiquer des renseignements personnels à un tiers sans le consentement de la personne concernée, lorsque cette communication est nécessaire à l'exercice d'un mandat ou à l'exécution d'un contrat de services ou d'entreprise (art. 67.2). Cette exception permet donc à l'organisme de transmettre des renseignements personnels à des mandataires et fournisseurs de services (« **fournisseur de services** ») sans devoir obtenir un consentement spécifique à cet effet.

**Entente écrite.** La Loi sur l'accès requiert en outre que le traitement de renseignements personnels par un fournisseur de services soit sujet à un contrat écrit devant comprendre :

- Une liste des dispositions de la Loi sur l'accès que le fournisseur de services s'engage à respecter.
- Des mesures permettant d'assurer la protection du caractère confidentiel des renseignements personnels communiqués. Le contrat devrait donc prévoir les mesures physiques, organisationnelles et techniques devant être mises en place par le fournisseur de service traitant les renseignements, que ceux-ci soient en transit ou stockés.
- Une disposition prévoyant que le fournisseur ne peut utiliser les renseignements que dans le cadre de l'exécution du contrat. Le contrat devrait donc prohiber l'utilisation des renseignements personnels par le fournisseur pour ses fins propres ou pour les fins d'un tiers. Il serait utile de clarifier si les nouvelles exceptions au consentement prévues à l'article 65.1 permettraient néanmoins au fournisseur de services d'utiliser les renseignements pour les fins qui y sont prévues (par exemple, dépersonnaliser les renseignements pour les utiliser à des fins internes de recherche ou de production de statistiques).

- Une disposition prévoyant que le fournisseur ne peut conserver les renseignements après l'expiration du contrat. La Loi 64 ne précise pas si l'anonymisation de ces renseignements par les fournisseurs de services afin de les utiliser pour poursuivre leurs fins sérieuses et légitimes (art. 73) permettrait de satisfaire cette exigence.

**Engagement de confidentialité.** L'article 67.2 al. 2 (2) requiert en outre que l'organisme public obtienne, de la part du fournisseur de services, un engagement de confidentialité signé par toute personne à qui les renseignements pourraient être communiqués, à moins que le responsable de la PRP estime que cela n'est pas nécessaire.

**Obligation de notification.** L'article 67.2 al. 2 (2) requiert également que le fournisseur de service avise sans délai le responsable PRP de l'organisme de « toute violation ou tentative de violation par toute personne de l'une ou l'autre des obligations relatives à la confidentialité du renseignement communiqué », et non simplement des incidents de confidentialité. Il n'est pas clair si les parties peuvent aménager, dans le cadre de leur entente écrite, les conditions auxquelles cette obligation sera soumise le cas échéant, par exemple pour limiter l'obligation de notification aux seuls « incidents de confidentialité ».

**Autoriser les vérifications par l'organisme.** Le fournisseur de services doit permettre au responsable de la PRP d'effectuer toute vérification relative aux obligations de confidentialité du fournisseur, c'est-à-dire de demander tout document et effectuer toute vérification additionnelle. Il n'est pas clair si les parties peuvent aménager les conditions auxquelles ces obligations seront soumises le cas échéant, par exemple en exigeant que les vérifications soient faites à certains moments ou soumises à certaines conditions.

**Exceptions.** Ces deux obligations (entente écrite et obligation de notification) ne s'appliquent pas lorsque le fournisseur de services est un autre organisme public au sens de la Loi sur l'accès ou un membre d'un ordre professionnel (art. 67.2 al. 3).

**Registre des communications.** La communication de renseignements personnels à un fournisseur de services sans le consentement de la personne concernée doit être inscrite dans un registre conformément à l'article 67.3 de la Loi sur l'accès (voir la section 3.3 à ce sujet).

**Obligation d'effectuer une EFVP.** Finalement, notons que lorsqu'un projet d'impartition comprend l'acquisition, le développement ou la refonte d'un système d'information ou d'une prestation électronique de services impliquant la collecte, l'utilisation, la communication, la conservation ou la destruction de renseignements personnels par un fournisseur de services pour le compte de l'organisme, ce dernier devra procéder à une EFVP (art. 63.5 al. 1). Bien que cette responsabilité incombe à l'organisme, le fournisseur de services devrait collaborer à cet exercice. Nous référons à la section 2.4 pour les exigences relatives aux EFVP.

## Pistes de conformité

1. **Politique de confidentialité.** Réviser la politique de confidentialité de l'organisme pour s'assurer qu'elle indique que les renseignements personnels pourront être transmis à ses fournisseurs de service. La politique devrait également mentionner le type de fournisseurs ou les nommer individuellement.

2. **Développer une procédure d'impartition** qui régit les employés susceptibles de sous-traiter le traitement de renseignements personnels (par exemple, l'équipe chargée de l'approvisionnement).

3. **Préparer un modèle de contrat (ou de clauses) de traitement des renseignements personnels.** Ce contrat devra prévoir :

   - les dispositions de la Loi sur l'accès auxquelles le fournisseur de services doit se conformer;
   - la protection des renseignements personnels;
   - l'utilisation des renseignements personnels aux fins de l'exécution du contrat;
   - la destruction des renseignements à l'issue du contrat;
   - l'obligation pour le fournisseur de services de notifier sans délai l'organisme en cas de violation ou tentative de violation des obligations de confidentialité;
   - la possibilité pour l'organisme de demander tout document et d'effectuer toute vérification relative à la confidentialité des renseignements.

4. **Préparer un modèle d'engagement de confidentialité à faire signer par le personnel du fournisseur qui pourrait avoir accès aux renseignements personnels.**

5. **Recenser les fournisseurs de services traitant des renseignements personnels pour l'organisme.** L'organisme devra alors :

   - Déterminer si un contrat écrit conforme aux exigences légales a bien été conclu avec chaque fournisseur de service.
   - Dans la négative, transmettre le modèle de contrat de traitement des renseignements personnels décrit à la piste 3 ci-dessus aux fournisseurs de services concernés.

6. **Communiquer avec les fournisseurs de service existants dont les systèmes/ prestations requièrent que l'organisme mène une EFVP.** Sur la base de la liste mentionnée à la piste 5 ci-dessus, l'organisme devrait prévoir de:

   - Communiquer avec chaque fournisseur de services existant que l'organisme souhaite impliquer dans le développement l'acquisition, le développement ou la refonte de systèmes ou prestations de services impliquant la collecte, l'utilisation, la communication, la conservation ou la destruction de renseignements personnels, pour leur indiquer que l'organisme va mener une EFVP pour laquelle il aura besoin de sa collaboration.

→ Suite à la page suivante

### Pistes de conformité

7. **Effectuer les EFVP.** Une EFVP devra être menée par l'organisme pour chaque projet d'impartition impliquant l'acquisition, le développement ou la refonte d'un système d'information ou d'une prestation électronique de services impliquant le traitement de renseignements personnels.

## 6.2. Transferts hors Québec

**En vigueur le 22 septembre 2023**

**Transparence.** Comme l'indique la section 3.1, l'organisme qui collecte des renseignements personnels auprès de personnes concernées doit les informer de la possibilité que ces renseignements soient communiqués à l'extérieur du Québec (et non simplement du Canada). Cette information devra être fournie au moment de la collecte et sur demande (art. 65 al. 2).

**Évaluation des facteurs relatifs à la vie privée.** Les transferts de renseignements personnels à l'extérieur du Québec sont une préoccupation majeure de la Loi 64, qui effectue une refonte de l'article 70.1 de la Loi sur l'accès. Ainsi, un organisme qui (1) souhaite communiquer des renseignements personnels à l'extérieur du Québec ou (2) confie à un tiers situé à l'extérieur du Québec la tâche de recueillir, d'utiliser, de communiquer ou de conserver pour son compte des renseignements personnels, doit effectuer une EFVP qui tient compte des facteurs suivants :

- la sensibilité des renseignements (un renseignement considéré comme sensible doit faire l'objet d'une protection accrue par rapport à un autre qui ne l'est pas, comme prévu à l'article 63.1 de la Loi sur l'accès);
- la finalité de leur utilisation;
- les mesures de protection, y compris celles qui sont contractuelles, qui s'y appliqueront;
- le régime juridique applicable dans l'État où les renseignements seraient communiqués, notamment les principes de protection des renseignements personnels qui y sont applicables. Il est à noter que la Loi 64 fait référence à des « principes », et non à une « Loi ».

Si l'EFVP « démontre que le renseignement bénéficierait d'une protection adéquate, notamment au regard des principes de protection des renseignements personnels généralement reconnus » alors la communication sera autorisée. Notons que la Loi ne précise pas en quoi consistent les « principes de protection des renseignements personnels généralement reconnus ». On peut se demander si cette notion est identique aux principes de protection personnels énumérés par la CAI dans son Guide d'accompagnement pour réaliser une EFVP, soit:

- Déterminer les fins de la collecte
- Limiter la collecte de renseignements personnels
- Informer la personne concernée
- Mettre en place des mesures de sécurité appropriées
- Limiter l'accès aux renseignements personnels
- Limiter l'utilisation de renseignements personnels
- Obtenir le consentement à communiquer des renseignements personnels
- Requérir le consentement des personnes concernées
- Assurer la qualité des renseignements personnels
- Permettre l'exercice des droits d'accès et de rectification
- Répondre avec diligence

**Influence européenne.** Cette nouvelle approche ressemble aux exigences du RGPD, qui exigences qu'une organisation transférant des données à caractère personnel hors de l'Espace économique européen vers une juridiction n'ayant pas été reconnue adéquate par la Commission européenne effectue une évaluation des risques de transfert avant de transférer ces données à l'étranger (voir sur ce point les recommandations 01/2020 et 02/2020 du *European Data Protection Board*).

**Entente écrite.** Si l'EFVP démontre que les renseignements traités à l'étranger feront l'objet d'une protection adéquate, l'organisme doit conclure avec le tiers une entente écrite qui tient compte, notamment :

- des résultats de l'EFVP;
- le cas échéant, des modalités convenues dans le but d'atténuer les risques identifiés dans le cadre de cette évaluation (art. 70.1 al. 2).

En outre, l'entente peut notamment inclure :

- l'interdiction d'utiliser à d'autres fins ou de communiquer les renseignements personnels;
- des mesures de sécurité précises;
- des règles relatives à l'accès aux renseignements personnels par les membres du personnel de l'organisme d'un autre gouvernement qui reçoit les renseignements personnels;
- l'obligation d'aviser l'organisme en cas d'incident de confidentialité ou de toute autre violation ou tentative de violation de l'une ou l'autre des obligations relatives à la confidentialité des renseignements personnels communiqués;
- des règles relatives à la conservation et à la destruction des renseignements personnels au terme de l'entente ou en cas de résiliation.

**Mesures contractuelles.** Ainsi, si l'EFVP conclut que les renseignements traités à l'étranger par un fournisseur de services seront suffisamment protégés avec un contrat reprenant les exigences de l'article 67.2, aucune autre mesure ne sera nécessaire. Si en revanche l'évaluation conclut que le traitement à l'étranger crée un risque pour leur protection, alors les parties devront convenir de mesures permettant de réduire ce risque à un niveau adéquat. La Loi ne précise pas en quoi consisterait ce type de mesures, mais on peut imaginer que des mesures techniques (par exemple le cryptage ou la dépersonnalisation), organisationnelles et contractuelles (par exemple des restrictions au partage des renseignements avec des autorités gouvernementales étrangères) pourraient être de nature à atténuer le niveau de risque.

## Pistes de conformité

1. **Réviser la politique de confidentialité de l'organisme afin de préciser si des renseignements personnels pourraient être communiqués à l'extérieur du Québec.**
2. **Effectuer une cartographie des renseignements communiqués en dehors du Québec.** Cet exercice permettra d'obtenir une description des flux de renseignements. L'organisme devra notamment vérifier :
   - l'adresse de l'entité impliquée dans la communication;
   - les modalités selon lesquelles les affiliés et/ou sous-traitants de l'entité qui sont situés dans d'autres juridictions pourront avoir accès aux renseignements;
   - la nature et le volume de renseignements personnels traités en dehors du Québec.
3. **Compléter le modèle d'EFVP pour évaluer les risques associés à la communication de renseignements personnels hors du Québec.** Ce modèle devra prendre en compte:
   - la sensibilité des renseignements communiqués;
   - la finalité de leur utilisation;
   - les mesures de protection, y compris contractuelles, qui s'y appliqueront;
   - le régime juridique applicable dans l'État de destination.
4. **Mener une EFVP pour les activités de traitement impliquant la communication de renseignements personnels en dehors du Québec.** Cet exercice devra notamment évaluer si le cadre juridique de chacune des juridictions dans lesquelles les renseignements seront traités dispose de principes de protection des renseignements personnels conformes aux « principes de protection des renseignements personnels généralement reconnus ».
5. **Adapter son modèle de contrat (ou de clauses) relatif au traitement des renseignements personnels pour prendre en compte les exigences liées aux fournisseurs de services situés hors du Québec.** Ce modèle devra :
   - Refléter les exigences de l'article 67.2 décrites à la section 6.1.
   - Prévoir des mesures de protection modulables en fonction des résultats de l'EFVP.
6. **Compléter la procédure d'impartition décrite à la section 6.1** pour refléter les exigences liées à la communication de données en dehors du Québec.

# 7. Cybersécurité, gestion des incidents de confidentialité et biométrie

La Loi 64 renforce l'obligation des organismes d'assurer la protection des renseignements personnels à l'aide de nouvelles mesures de protection en plus d'introduire un nouveau régime de notification des incidents de confidentialité.

## 7.1. Cybersécurité

**En vigueur le 22 septembre 2023**

**Mesures de sécurité.** L'obligation relative aux mesures de sécurité prévue à l'article 63.1 de la Loi sur l'accès demeure inchangée par la Loi 64. À titre de rappel, les organismes doivent prendre les mesures de sécurité appropriées et raisonnables pour protéger les renseignements personnels en tenant compte, notamment, de leur sensibilité, de la finalité de leur utilisation, de leur quantité, de leur répartition et de leur support. Ainsi, plus un renseignement sera sensible, plus les mesures de sécurité devront être robustes. Les mesures de sécurité visent entre autres les contrôles techniques, physiques et organisationnels et devraient toujours être évaluées et prédéfinies selon les circonstances propres à chaque projet, en procédant à une analyse technique des risques de sécurité en parallèle à l'EFVP. De cette manière, les organismes peuvent mettre en place les arrangements requis avant la signature du contrat en tenant compte des résultats de ces deux évaluations, lesquelles influenceront grandement les recommandations juridiques et la négociation des clauses contractuelles. L'analyse des risques de sécurité devrait toujours comprendre une vérification diligente du niveau de sécurité offert par un fournisseur et par la solution ou le service offert, le cas échéant.

**Mesures de protection.** Dans le cadre des nouvelles obligations apportées par la Loi 64 en matière d'EFVP, il est prévu que le comité puisse suggérer, à toute étape d'un projet, des « mesures de protection des renseignements personnels » (art. 63.6 (2)) applicables au projet (voir la section 2.4). Ces « mesures de protection » décrites à l'article 63.6 s'ajoutent aux mesures de sécurité mises en place en vertu l'article 63.1 de la Loi sur l'accès. À tout événement, le responsable de la PRP devrait collaborer en continu avec un expert en sécurité pour assurer une cohérence dans la mise en place des contrôles requis.

### Pistes de conformité

1. **Catégoriser (ou classifier) les actifs informationnels de manière à leur attribuer des mesures de sécurité correspondant au niveau de catégorisation.**
   - Les niveaux de catégorisation devraient notamment tenir compte des besoins en termes de confidentialité, d'intégrité et de disponibilité de l'information.
2. **Assurer une forte cohésion entre le responsable de la PRP, le Comité et le département de sécurité, de manière à ce que les mesures de protection soient effectives et cohérentes d'un projet à l'autre.**

## 7.2. Incidents de confidentialité

**En vigueur le 22 septembre 2022**

La Loi 64 introduit dans le secteur public un régime de notification obligatoire des incidents de confidentialité similaire à celui introduit dans le secteur privé.

**Définition.** Le nouvel article 63.8 définit la notion d'incident de confidentialité comme étant l'accès, l'utilisation ou la communication non autorisée de renseignements personnels, la perte de renseignements personnels ou tout autre atteinte à la protection d'un tel renseignement. Ainsi, toute atteinte, brèche ou incident de sécurité touchant les renseignements personnels tombera vraisemblablement sous l'application de l'article 63.8. Parmi les différents types d'incidents de confidentialité, on retrouve l'hameçonnage, le déploiement de logiciels malveillants, les attaques par rançongiciel, les botnets, les attaques par force brute, l'envoi de renseignements personnels à une mauvaise adresse courriel, etc.

⚠ Il est intéressant de souligner que le Québec intègre l'utilisation non autorisée de renseignements personnels dans sa définition d'incident de confidentialité. Cette particularité pourrait engendrer certaines difficultés d'interprétation, à savoir si une utilisation sans consentement à des fins de marketing, par exemple, peut être considérée comme un « incident de confidentialité ». Bien qu'une telle interprétation puisse conduire à une surabondance de notifications des incidents à la CAI et aux personnes concernées, les organismes devront faire preuve de jugement dans leur évaluation du risque de préjudice.

**Exemples.** Voici quelques exemples de situations susceptibles d'être considérées comme un incident de confidentialité :

- Un membre du personnel consulte des renseignements personnels non nécessaires à l'exercice de ses fonctions en outrepassant les autorisations d'accès qui lui ont été consenties.
- Un membre du personnel utilise des renseignements personnels d'une base de données à laquelle il a accès dans le cadre de ses fonctions dans le but d'usurper l'identité d'une personne.
- Un courriel contenant des renseignements personnels est envoyé au mauvais destinataire.
- Une personne perd ou se fait voler des documents contenant des renseignements personnels.
- Un pirate informatique s'infiltre dans les systèmes de l'organisme afin d'extraire ou d'altérer des fichiers contenant des renseignements personnels.

**Mitigation des risques.** L'article 63.7 al. 1 oblige les organismes ayant des « motifs de croire » qu'un incident de confidentialité a eu lieu à prendre des « mesures raisonnables pour diminuer les risques qu'un préjudice soit causé et éviter que de nouveaux incidents de même nature ne se produisent ». Cette exigence s'applique à toute entité ou tout tiers assurant la garde ou l'hébergement des renseignements personnels, tel qu'un fournisseur de service ou un sous-traitant. En pratique, cela signifie que les organismes devront prendre toutes les mesures appropriées et raisonnables afin de prévenir le préjudice pouvant être causé aux personnes touchées par un incident, et ce, sans égard au niveau de gravité du risque. Les mesures à prendre seront déterminées en fonction du type d'incident et du contexte applicable, mais pourraient inclure par exemple des enquêtes approfondies et toute mesure de sécurité visant à contenir et à éradiquer l'incident. Une bonne façon de prévenir les incidents et les risques de préjudice consiste à se doter d'un programme de sécurité robuste basé sur les bonnes pratiques de l'industrie, et de faire tester son plan de réponse aux incidents par des experts en réponse aux incidents.

**Évaluation du risque de préjudice sérieux.** Tous les incidents de confidentialité devront faire l'objet d'un processus d'évaluation du « risque de préjudice sérieux », afin de déterminer si l'incident en question devra être notifié à la CAI et aux personnes concernées. La Loi 64 ne fournit pas de définition ou d'exemples de préjudice sérieux, mais énonce néanmoins les principaux facteurs à considérer pour évaluer le niveau de gravité du risque de préjudice :

- **La sensibilité des renseignements en cause.** Les renseignements qui, en raison de leur nature (par exemple médicale, biométrique ou autrement intime) ou du contexte de leur utilisation, feront croître le risque de préjudice.
- **Les conséquences appréhendées de leur utilisation.** Par exemple, si les renseignements compromis sont susceptibles d'être utilisés pour commettre une fraude ou un vol d'identité.
- **La probabilité qu'ils soient utilisés à des fins préjudiciables.** Si, par exemple, les renseignements ont été exfiltrés sur des serveurs de l'organisme ou publiés sur le Dark Web, ils risquent d'être utilisés à de mauvaises fins (art. 63.10).

**Notification des incidents.** Si l'organisme détermine que l'incident présente un risque de préjudice sérieux pour les personnes concernées, il devra aviser la CAI ainsi que toute personne dont les

renseignements ont été compromis par l'incident, à défaut de quoi la CAI pourra lui ordonner de le faire (art. 63.8 al. 2). Il est également prévu que l'organisme peut, à sa discrétion, aviser toute personne ou organisme susceptible de réduire le risque de préjudice, mais en ne lui communiquant que les renseignements personnels nécessaires à cette fin (sans le consentement de la personne concernée). Dans ce dernier cas, le responsable de la PRP devra enregistrer la communication (art. 63.7 al. 2). Aucun délai n'est prévu pour la notification des incidents, mais celle-ci devra se faire avec « diligence », selon l'article 63.8. À titre comparatif, la *Loi sur la protection des renseignements personnels et les documents électroniques* exige la notification dès que possible au Commissaire à la protection de la vie privée du Canada dans le cas où une atteinte aux mesures de sécurité présente un « risque réel de préjudice grave ». En Europe, le RGPD exige la divulgation d'une atteinte à l'autorité de surveillance du pays au plus tard 72 heures après la violation lorsqu'elle entraîne un risque de préjudice.

**Relation avec les fournisseurs.** Si un incident de confidentialité se produit chez un fournisseur de services en possession de renseignements personnels externalisés, certaines conditions relatives à la notification des incidents pourront être prévues contractuellement. Toutefois, puisque les obligations de notification de la Loi 64 s'appliquent tant aux organismes publics, assujettis à la Loi sur l'accès, qu'aux entreprises, soumises à la Loi sur le secteur privé, un fournisseur de services pourrait être lui-même tenu de notifier l'incident à la CAI et aux personnes concernées en vertu de l'obligation de notification.

⚠ Il n'est pas clair si le législateur québécois a volontairement omis de mentionner que l'obligation de notification s'applique à l'entité qui a le contrôle des renseignements et si la CAI s'attend à ce que tant l'organisation agissant en tant que responsable du traitement des données que son fournisseur de services (et sous-traitant) signalent l'incident, ce qui pourrait nécessiter une certaine coordination entre l'organisation et son fournisseur de services.

**Exception.** Malgré ce qui précède, soulignons qu'une personne dont un renseignement personnel est concerné par un incident de confidentialité n'aura pas à être avisée si un tel avis était susceptible d'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, selon l'article 63.7 al. 3.

**Formalités**. La Loi 64 n'impose pas de forme particulière au regard des avis que les organismes devront faire parvenir à la CAI et aux individus concernés pour remplir leurs obligations de notification. Toutefois, l'article 63.7 al. 4 reconnaît au gouvernement le pouvoir de déterminer, par règlement, le contenu et les modalités de ces avis. D'ici l'adoption d'un tel règlement, les organismes peuvent utiliser le formulaire de déclaration d'un incident de sécurité accessible sur le site Internet de la CAI, énonçant les différentes informations à divulguer sur le contexte de l'incident et les étapes à franchir.

**Registre des incidents.** Finalement, les organismes devront tenir un registre des incidents de confidentialité dont une copie devra être transmise à la CAI sur demande, en vertu de l'article 63.11. Un règlement du gouvernement pourra déterminer la teneur de ce registre ainsi que les délais de rétention d'un tel registre. À titre de comparaison, le *Règlement fédéral sur les atteintes aux mesures de sécurité* prévoit que les organisations doivent conserver le registre de toutes les atteintes aux mesures de sécurité pendant vingt-quatre mois après la date à laquelle elle conclut qu'il y a eu atteinte et ce, sans égard au risque de préjudice.

## Pistes de conformité

1. **Définir une structure organisationnelle prévoyant des rôles et responsabilités en matière de prévention, de gestion et de réponse aux incidents.**
2. **Mettre à jour ou élaborer la politique de gestion des incidents de l'organisme de manière à y inclure les nouvelles obligations,**
   - Élaborer un plan de réponse aux incidents détaillé et basé sur les standards de l'industrie.
   - Faire tester et approuver ce plan par des experts en réponse aux incidents.
3. **Réviser les contrats avec des fournisseurs de service afin d'y inclure les nouvelles obligations de notification des incidents de manière à s'assurer que :**
   - Tous les incidents impliquant des renseignements personnels sont communiqués à l'organisme rapidement.
   - Les clauses reflètent la nouvelle définition d'« incident de confidentialité ».
   - Le fournisseur est en mesure de communiquer à l'organisme toutes les informations requises pour lui permettre d'évaluer le risque de préjudice sérieux.
4. **Établir un programme de formation en matière de prévention et de gestion des incidents.**
5. **Tenir un registre au sein de l'organisme de tous les incidents de confidentialité et ce, même s'ils ne comportent pas de risque de préjudice sérieux.** Ce registre devrait comprendre au minimum :
   - le responsable de l'enquête;
   - les circonstances de l'incident;
   - la date ou la période où il y a eu un incident;
   - la nature des renseignements personnels visés par l'incident, pour autant qu'elle soit connue;
   - la raison pour laquelle l'organisme juge que l'incident ne comporte pas de préjudice sérieux pour les personnes concernées.

## 7.3. Biométrie

**En vigueur le 22 septembre 2022**

**Déclaration à la CAI.** Le législateur québécois avait prévu, depuis 2001 avec la *Loi concernant le cadre juridique des technologies de l'information* (« **LCCJTI** ») certaines dispositions visant à encadrer l'utilisation des banques de données biométriques afin d'en assurer une certaine sécurité. La Loi 64 apporte des changements aux articles 44 et 45 de la LCCJTI, plus particulièrement concernant l'obligation de déclarer l'utilisation des technologies biométriques. Jusqu'à présent, l'obligation de divulgation à la CAI se limitait aux « banques de caractéristiques ou de mesures biométriques » (en d'autres mots, aux bases de données biométriques). Maintenant, à l'obligation d'obtenir le consentement exprès des individus pour la collecte de leurs données biométriques prévue à l'article 44 s'ajoute celle d'avoir préalablement divulgué à la CAI l'utilisation de procédés biométriques destinés à la vérification ou la confirmation de l'identité, et ce, sans égard à l'existence d'une base de données biométriques. Ainsi, sans une telle déclaration à la CAI et le consentement exprès, nul ne pourra faire usage de technologies biométriques pour les fins ci-haut mentionnées.

**Délai.** Par ailleurs, il est à noter que l'article 45 de la LCCJTI a été modifié de manière à obliger les organisations à déclarer à la CAI toute création de banques de données biométriques au plus tard 60 jours avant sa mise en service. La Loi 64 est ainsi venue préciser un délai maximal pour cette divulgation préalable.

### Pistes de conformité

1. **Mettre en place une directive sur l'utilisation de systèmes biométriques** de manière à y prévoir les obligations ci-haut mentionnées et celles sur la protection des données biométriques.
2. **Faire une évaluation des facteurs relatifs à la vie privée** préalablement à tout projet impliquant des données biométriques.

Le présent guide sera mis à jour régulièrement par l'équipe Respect de la vie privée et protection des renseignements personnels de BLG (Montréal) afin de refléter les développements réglementaires et les lignes directrices publiées par la CAI et les autres intervenants.

# Principaux contacts

Pour toute question sur les récents développements concernant le cadre juridique régissant la protection des renseignements personnels au Québec, veuillez communiquer avec l'un des membres de l'équipe Respect de la vie privée et protection des renseignements personnels de BLG :


**Éloïse Gratton**
Associée
T 514.954.3106
egratton@blg.com

**Elisa Henry**
Associée
T 514.954.3113
ehenry@blg.com

**François Joli-Coeur**
Associé
T 416.367.6178
fjolicoeur@blg.com

**Simon Du Perron**
Avocat
T 514.954.2542
sduperron@blg.com

**Max Jarvie**
Avocat principal
T 514.954.2628
mjarvie@blg.com

**Julie M. Gauthier**
Avocate-conseil
T 514.954.3198
jugauthier@blg.com

**Andy Nagy**
Avocat
T 514.395.2714
anagy@blg.com

**Anthony Hémond**
Avocat-conseil
T 514.395.3899
AHemond@blg.com

**Daniel-Nicolas El Khoury**
Avocat
T 514.395.3882
DElKhoury@blg.com

**Catherine Labasi-Sammartino**
Avocate
T 514.954.2537
CLabasiSammartino@blg.com