Borden Ladner Gervais

Loi sur la protection des renseignements personnels dans le secteur privé :

Guide de conformité pour les entreprises

Février 2026

Loi sur la protection des renseignements personnels dans le secteur privé :

Guide de conformité pour les entreprises

Ce Guide vise à outiller les entreprises face aux exigences de la Loi sur la protection des renseignements personnels dans le secteur privé (« LPRPSP »).

Ce Guide est divisé en différents thèmes qui reflètent les principales obligations de la LPRPSP – le régime de protection des renseignements personnels dans le secteur privé. Ainsi, ce document est destiné à toute personne qui recueille, utilise, communique ou détient des renseignements personnels à l'occasion de l'exploitation d'une entreprise.

Meilleures pratiques

Nous suggérons des mesures que les entreprises peuvent adopter pour chaque thème afin de renforcer leur conformité et faire preuve de proactivité en matière de protection des renseignements personnels.

Table des matières

1. Mécanismes de mise en œuvre

La LPRPSP établit trois types de mécanismes afin d'assurer la conformité des entreprises aux exigences en matière de traitement des renseignements personnels, soit (1) des sanctions administratives pécuniaires (2) des sanctions pénales et (3) un droit privé d'action.

Sanctions administratives pécuniaires. La LPRPSP prévoit un régime de sanctions administratives pécuniaires (« **SAP** ») administré par la Commission d'accès à l'information (« **CAI** »). En vertu de ses dispositions, une « personne désignée par la Commission, mais qui n'est pas membre de l'une de ses sections » peut imposer des SAPs aux entreprises qui contreviennent à la loi (voir le tableau 1.1 pour les infractions précises) pouvant aller jusqu'à 10 000 000 $ ou 2 % du chiffre d'affaires mondial.

Selon le Cadre général d'application des sanctions administratives pécuniaires de la CAI (« **Cadre d'application des SAPs** »), la personne chargée de l'imposition des SAPs a été désignée par la CAI comme étant le directeur ou la directrice de la Direction de la surveillance ou, en son absence, la personne chargée de l'intérim. Cette personne dispose d'un pouvoir discrétionnaire pour évaluer l'opportunité d'imposer une sanction, en tenant compte de l'ensemble des circonstances propres à chaque dossier. Une sanction est généralement imposée lorsqu'un manquement prévu à l'article 90.1 de la LPRPSP est constaté et que les critères énoncés dans le Cadre d'application des SAPs sont remplis (voir le tableau 1.3 pour une énumération des critères).

Avant d'imposer une SAP, la CAI transmet un avis de non-conformité, invitant l'entreprise à corriger la situation. En l'absence de correction, la sanction est ensuite officialisée par un avis de réclamation précisant le montant dû, les motifs, les délais applicables et les recours possibles – notamment, une demande de réexamen ou un recours devant la Cour du Québec. Il est également possible de conclure un engagement formel avec la CAI afin de corriger le manquement et éviter une sanction.

Sanctions pénales. La LPRPSP prévoit plusieurs infractions (voir le tableau 1.1 pour les infractions précises) en vertu desquelles la CAI peut intenter des poursuites pénales. Celles-ci peuvent être sanctionnées par l'imposition, par la Cour du Québec, d'une amende pouvant aller jusqu'à 25 000 000 $ ou 4 % du chiffre d'affaires mondial.

Selon le Cadre d'application des SAPs, la CAI priorise généralement une poursuite pénale lorsque cette voie est jugée la plus appropriée compte tenu des objectifs poursuivis et des circonstances propres à chaque dossier. Une poursuite pénale est notamment envisagée dans les cas suivants :

- Les conséquences de l'infraction sont graves, notamment en cas d'atteinte à la vie privée, à une clientèle vulnérable ou à des renseignements sensibles;
- Le non-respect d'une ordonnance de la CAI;
- Les mesures adéquates n'ont pas été prises par la personne en défaut pour remédier à l'infraction, malgré l'imposition de SAPs ou l'exercice d'autres mesures administratives;

- La personne en défaut a agi intentionnellement ou a fait preuve de négligence ou d'insouciance;
- Une entrave au déroulement d'une enquête ou d'une inspection de la CAI a été constatée;
- Une entrave à l'instruction d'une demande de la CAI a été constatée, notamment par la communication de renseignements faux ou inexacts ou l'omission de renseignements requis;
- Plusieurs manquements ou infractions à la LPRPSP ont été commis par la même personne en défaut ou sont récurrents dans le temps.

La décision d'intenter une poursuite pénale est prise par un membre de la section de surveillance de la CAI et est amorcée par la signification d'un constat d'infraction.

Dommages punitifs. La LPRPSP reconnaît la possibilité pour les personnes de réclamer des dommages-intérêts punitifs d'au moins 1 000 $ lorsqu'une atteinte illicite à un droit conféré par la LPRPSP ou par les articles 35 à 40 du Code civil du Québec (« **CCQ** ») cause un préjudice et que cette atteinte est intentionnelle ou résulte d'une faute lourde. L'article 93.1 de la LPRPSP constitue une disposition d'attribution de dommages-intérêts punitifs au sens de l'article 1621 du CCQ.

Il convient de noter qu'en date du 1 janvier 2026, aucune SAPs ou sanctions pénales n'ont été imposées. Ceci dit, on peut voir une augmentation du nombre de demandes déposées dans lesquelles les demandeurs réclament des dommages punitifs, notamment *Synotte c. TiktTok Technology Canada Inc.* (2025) et S.C. c. *Gameloft et autres* (2025). Il sera pertinent de suivre ces dossiers de près pour voir si de tels dommages seront attribués.

Les tableaux suivants proposent une synthèse des mécanismes de mise en œuvre prévus par la LPRPSP.

1.1. Infractions

	Sanction pénale	SAP	Dommages punitifs
Collecte, utilisation communication, conservation ou destruction de renseignements personnels en contravention à la LPRPSP	x	x	x
Défaut d'informer les personnes concernées conformément aux articles 7 et 8 au moment de recueillir leurs renseignements personnels		x	x
Défaut de prendre les mesures de sécurité propres à assurer la protection des renseignements personnels conformément à l'article 10	x	x	x
Défaut d'aviser la CAI ou les personnes concernées par un incident de confidentialité qui présente un risque de préjudice sérieux	x	x	x
Défaut d'informer la personne visée par une décision automatisée ou ne pas lui donner l'occasion de présenter ses observations		x	x
Procéder ou tenter de procéder à l'identification d'une personne physique à partir de renseignements dépersonnalisés ou anonymisés sans l'autorisation de la personne qui les détient	x		x
Entraver le déroulement d'une enquête, d'une inspection ou l'instruction d'une demande par la CAI	x		
Exercer des représailles ou menacer une personne de représailles pour le motif qu'elle a de bonne foi déposé une plainte à la CAI ou collaboré à une enquête	x		x
Refuser ou négliger de se conformer, dans le délai fixé, à une demande de production de documents émise par la CAI	x		
Contrevenir à une ordonnance de la CAI	x		

1.2. Aspects procéduraux

	Sanction pénale	SAP	Dommages punitifs
Délai de prescription	5 ans	2 ans	3 ans
Avis de non-conformité préalable	Optionnel*	Oui	Non
Possibilité de conclure un engagement de conformité	Non	Oui	Non
Sanction imposée par la	Cour du Québec	Personne désignée par la CAI	Cour du Québec ou Cour supérieure (selon le montant de la réclamation)
Révision administrative	Non	Oui	Non
Droit d'appel ou de contestation	Oui – Cour supérieure	Oui – Cour du Québec	Sur permission d'un juge de la Cour d'appel (si la valeur du litige est de moins de 60 000 $)

* Le nouvel article 90.2 prévoit qu'un avis de non-conformité doit faire mention du fait que le manquement constaté par la CAI pourrait donner lieu à une SAP ou à une sanction pénale. Toutefois, l'obligation d'envoyer un avis de non-conformité à l'entreprise contrevenante se matérialise uniquement avant l'imposition d'une SAP (art. 90.4). Ainsi, il est incertain de savoir si l'introduction d'une poursuite pénale par la CAI sera nécessairement précédée par un avis de non-conformité (et donc d'un délai pour remédier au manquement). Ceci étant dit, l'article 92 précise que le recours pénal de la CAI est assujetti aux dispositions du *Code de procédure pénale*.

1.3. Sanctions

Sanction pénale	SAP	Dommages punitifs
Montant maximal de la sanction		
25 000 000 $ ou 4 % du chiffre d'affaires mondial de l'exercice financier précédant	10 000 000 $ ou 2 % du chiffre d'affaires mondial de l'exercice financier précédent	Montant des dommages-intérêts punitifs
Facteurs de détermination		
• La nature, la gravité, le caractère répétitif et la durée de l'infraction • La sensibilité des renseignements personnels concernés • Le fait que le contrevenant ait agi de façon intentionnelle ou avec négligence ou 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 l'empêcher, 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 associé	• La nature, la gravité, le caractère répétitif et la durée du manquement • La sensibilité des renseignements personnels concernés • Le nombre de personnes concernées par le manquement et le risque de préjudice associé • Les mesures prises par la personne en défaut pour remédier au manquement ou en atténuer les conséquences • Le degré de collaboration offert à la CAI • La compensation offerte par la personne en défaut, à titre de dédommagement, à toute personne concernée • La capacité de payer de la personne en défaut	Selon la jurisprudence

2. Responsabilité et gouvernance

La LPRPSP reconnaît formellement que toute entreprise est responsable d'assurer la protection des renseignements personnels qu'elle détient. Il découle de ce principe plusieurs obligations en matière de responsabilité et de gouvernance des données.

2.1. Responsable de la protection des renseignements personnels

Désignation. La LPRPSP prévoit que, par défaut, la personne ayant la plus haute autorité au sein de l'entreprise (p. ex. son PDG) doit veiller au respect de la mise en œuvre de la loi et exercer la fonction du responsable de la protection des renseignements personnels (« **PRP** »). Ce rôle de « responsable de la PRP » peut toutefois être délégué par écrit, en tout ou en partie, à toute personne, qu'il s'agisse d'une personne à l'interne ou d'un tiers. Selon les orientations de la CAI, même en cas de délégation, la plus haute autorité au sein de l'entreprise demeure ultimement imputable du respect de la LPRPSP. L'entreprise doit s'assurer que le titre et les coordonnées du responsable de la PRP sont accessibles sur son site Internet ou, à défaut, par tout autre moyen approprié.

Tâches. Le responsable de la PRP est appelé à assurer diverses fonctions, qui peuvent notamment inclure les tâches suivantes :

- Approuver les politiques et pratiques relatives aux renseignements personnels que l'entreprise doit adopter et mettre en œuvre, et assurer la formation interne quant à leur application. Voir la section 2.2 pour plus de détails sur ces politiques et pratiques.
- Participer aux évaluations des facteurs relatifs à la vie privée (« **EFVP** ») des projets d'acquisition, de développements et de refonte de systèmes d'information ou de prestation électronique de services et suggérer des mesures afin d'assurer la protection des renseignements personnels traités dans le cadre de ces systèmes. Voir la section 2.3 pour plus de détails sur les EFVP.
- Prendre part à la gestion des incidents de confidentialité, notamment par l'évaluation du préjudice causé, et consigner toute communication (faite sans consentement) à une entreprise ou organisme public susceptible de diminuer ce préjudice et agir à titre de personne-ressource auprès de la CAI. Voir la section 7.2 pour plus de détails sur les incidents de confidentialité.
- Recevoir et répondre aux demandes d'accès et de rectification ainsi qu'aux demandes liées à la portabilité des données et au droit à la désindexation. Voir la section 4 pour plus de détails sur les droits individuels.

Qualifications. La LPRPSP ne prévoit pas explicitement que le responsable de la PRP doit être situé au Québec ou avoir des connaissances particulières de la loi québécoise ou de la langue française. Une entité québécoise d'un groupe d'entreprises ayant des activités à l'international peut donc déléguer le rôle du responsable de la PRP à une personne qui exerce un rôle similaire à l'échelle nationale (p. ex. Canada), régionale (p. ex. Amérique du Nord) ou mondiale. Elle peut également retenir les services d'avocats spécialisés dans le domaine de la protection des renseignements personnels et de la vie privée afin d'aider le responsable de la PRP à exercer ses tâches.

Meilleures pratiques

1. **Déterminer les qualifications requises pour exercer le rôle de responsable de la PRP.** Les entreprises doivent déterminer si elles possèdent l'expertise nécessaire à l'interne ou si elles souhaitent externaliser ce rôle.
2. **Établir une description des rôles et responsabilités du responsable de la PRP.** Cette description doit tenir compte des obligations de la LPRPSP et de la réalité de l'entreprise.
3. **Désigner par écrit une personne à titre de responsable de la PRP.** Prévoir un programme de formation pour le responsable de la PRP.

2.2. Politiques en matière de gouvernance et de protection des renseignements personnels

Politiques et pratiques. La LPRPSP reconnaît formellement le devoir des entreprises d'établir et de mettre en œuvre des politiques et des pratiques en matière de gouvernance et de protection des renseignements personnels. Celles-ci doivent notamment prévoir l'encadrement applicable à :

- La conservation et la destruction des renseignements personnels;
- Les rôles et les responsabilités des membres du personnel tout au long du cycle de vie des renseignements personnels; et
- Un processus de traitement des plaintes relatives à la protection des renseignements personnels.

En outre, les entreprises sont tenues de publier des « informations détaillées au sujet de ces politiques et de ces pratiques » sur leur site Internet, ou par tout autre moyen approprié, en termes simples et clairs. Bien que le niveau de détail ne soit pas défini, il s'agit de présenter de manière accessible les pratiques de l'entreprise, y compris les informations mentionnées ci-dessus.

Les entreprises peuvent notamment intégrer ces informations dans une section de leur site Internet dédiée à la protection des renseignements personnels. Plusieurs entreprises ont d'ailleurs ce type de section (p. ex. un « Centre de protection des renseignements personnels ») regroupant toute l'information pertinente sur le programme de protection des renseignements personnels de l'entreprise. Ceci peut inclure, entre autres, un engagement envers la protection des renseignements personnels, une politique de confidentialité, une foire aux questions sur la vie privée, ou des renseignements sur les certifications de sécurité de l'entreprise.

Contenu. Contrairement à la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, qui est complétée par un Règlement précisant le contenu obligatoire des politiques de confidentialité des organismes publics, la LPRPSP ne prévoit rien de tel pour les entreprises. Toutefois, selon le Guide explicatif de la CAI, les politiques peuvent contenir :

- Le nom de l'entreprise, la date d'entrée en vigueur de la politique et la date de la dernière mise à jour;
- La façon dont les renseignements personnels sont recueillis par des moyens technologiques, le recours à des technologies d'identification, de localisation ou de profilage, ainsi que la manière d'activer ces fonctions (le cas échéant);
- L'identité des entités qui recueillent des renseignements personnels pour l'entreprise;
- Les catégories de renseignements personnels recueillis et les fins précises de la collecte;
- Les mesures offertes aux personnes pour refuser la collecte de certains renseignements personnels et les conséquences d'un tel refus;
- Les catégories de personnes au sein de l'entreprise qui ont accès aux renseignements personnels;
- En cas de communication à des tiers : les renseignements ou catégories de renseignements concernés, les fins de ces communications, les noms ou catégories de destinataires, ainsi que l'indication de tout transfert hors Québec (le cas échéant); et
- Les droits des personnes concernées, notamment le droit d'accès, le droit de rectification ou de mise à jour, et la possibilité de déposer une plainte auprès de l'entreprise selon le processus établi.

Meilleures pratiques

1. **Répertorier et régulièrement mettre à jour les politiques, pratiques et procédures en place relativement à la protection des renseignements personnels tout au long de leur cycle de vie.**
2. **Effectuer régulièrement un exercice de cartographie des données afin de documenter et mettre à jour les pratiques de l'entreprise en matière de gestion des renseignements personnels.**
3. **S'assurer de la mise en œuvre des politiques et procédures suivantes (ou les intégrer dans un « cadre interne relatif à la gestion des renseignements personnels »), selon les besoins et les activités de l'entreprise :**
    - 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.
    - Procédure relative aux méthodes de destruction des renseignements personnels et d'anonymisation, le cas échéant.

→ Suite à la page suivante

Meilleures pratiques

- Politique prévoyant les rôles et les responsabilités des membres du personnel tout au long du cycle de vie des renseignements.
- Politique et procédures relatives à la réception et au traitement de plaintes et de demandes de personnes souhaitant exercer leurs droits.
- Politique et procédures relatives à la sécurité des données.
- Politique de gestion des incidents de confidentialité et plan de réponse aux incidents.
- Politiques particulières en fonction des activités de l'entreprise, par exemple : politique sur l'utilisation des caméras de surveillance, politique sur l'utilisation de systèmes biométriques, politique sur l'utilisation de renseignements personnels pour la recherche et l'intelligence artificielle, etc.
- Politique d'évaluation des risques liés aux fournisseurs.

4. **Développer un programme de formation sur les règles relatives à la protection des renseignements personnels pour les employés qui gèrent ou ont accès à des renseignements personnels.**
5. **Faire approuver les politiques et pratiques par le responsable de la PRP.**
6. **Publier de l'information détaillée au sujet des politiques et pratiques sur le site Internet de l'entreprise (par ex., en l'insérant dans sa politique de confidentialité ou en créant une section distincte sur son site Internet).**

2.3. Évaluations des facteurs relatifs à la vie privée (EFVP)

Obligation d'effectuer une EFVP. Les entreprises doivent 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. La LPRPSP prévoit également deux autres situations où l'EFVP est obligatoire pour les entreprises : (1) la communication de renseignements personnels à l'extérieur du Québec et (2) la communication, sans le consentement des personnes concernées, à des fins d'étude, de recherche ou de production de statistiques dans le cadre d'une entente.

Selon l'Office québécois de la langue française (« **OQLF** »), un système d'information est constitué des ressources humaines (le personnel), des ressources matérielles (l'équipement) et des procédures permettant d'acquérir, de stocker, de traiter et de diffuser les éléments d'information pertinents pour le fonctionnement d'une entreprise (p. ex. base de données, logiciels d'application, procédures, documentation, etc.). Il faut différencier le système d'information du système informatique. Ce dernier ne constitue que la partie informatique du système d'information, notamment l'unité centrale de traitement, les périphériques, le système d'exploitation, etc. Quant à elle, la prestation électronique de

services est définie comme une « prestation de services gouvernementaux, sécurisés ou non, offerts aux citoyens par l'intermédiaire d'Internet ».

Exemples de projets visés par l'obligation. La CAI a publié un Guide d'accompagnement pour réaliser une EFVP (« **Guide d'accompagnement sur les EFVP** »), mis à jour en avril 2024. Dans ce guide, la CAI offre des recommandations aux entreprises quant à la manière de réaliser une EFVP pour tout projet impliquant des renseignements personnels. Selon la CAI, les projets nécessitant la réalisation d'une EFVP sont ceux qui visent notamment à :

- Offrir un nouveau service public;
- Déployer, sur le Web, un service existant;
- Accroître la sécurité d'une installation;
- Contrer la fraude;
- Améliorer la détection d'un problème de santé rare;
- Vous conformer avec la réglementation;
- Conserver votre compétitivité;
- Offrir une expérience client plus agréable en créant la nouvelle version d'une plateforme.

Pas de portée rétroactive. L'obligation de procéder à une EFVP n'a pas de portée rétroactive. Ainsi, les entreprises n'ont pas à évaluer les systèmes existants avant l'entrée en vigueur des dispositions pertinentes de la LPRPSP, soit avant le 22 septembre 2023. Toutefois, la mise à jour substantielle d'un système existant (p. ex. plateforme de gestion de documents), devrait être considérée comme une « refonte » et devra donc faire l'objet d'une EFVP, y compris lorsqu'une EFVP a déjà été réalisée.

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 ». Soulignons qu'il s'agit là des mêmes critères que ceux prévus à l'article 10 de la LPRPSP afin de qualifier les mesures de sécurité qu'une entreprise doit prendre pour assurer la protection des renseignements personnels qu'elle détient. Ce critère vise à ce que l'envergure de l'EFVP soit adaptée à l'impact du projet sur la vie privée des personnes. 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 de personnes, par exemple. Notons que le Guide d'accompagnement sur les EFVP de la CAI fournit des outils utiles aux entreprises qui veulent se familiariser avec le processus, lequel doit être entamé dès le début du projet. La CAI a également publié un Modèle de rapport d'EFVP afin d'aider les entreprises dans cette démarche.

Portabilité des données. En outre, les entreprises doivent 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. Voir la section 4.3 pour plus de détails sur le droit à la portabilité des données.

Meilleures pratiques

1. **Développer une procédure interne sur les EFVP.** La procédure doit, notamment :
   - Définir les critères déclenchant l'obligation d'effectuer une EFVP. Par exemple, l'entreprise pourrait établir une matrice permettant d'évaluer la nécessité d'une EFVP en fonction des activités de l'entreprise.
   - Définir un processus pour s'assurer que les projets qui requièrent une EFVP soient identifiés dès le début du projet.
2. **Communiquer la procédure au sein de l'entreprise.**
   - Les entreprises peuvent désigner des responsables dans les départements susceptibles d'initier ces projets (p. ex. marketing, TI, intelligence d'affaires, approvisionnement).
   - Les responsables des départements doivent informer le responsable de la PRP dès le début d'un projet nécessitant une EFVP.
3. **Développer un gabarit pour la réalisation d'une EFVP, à l'aide par exemple du Modèle de rapport d'EFVP de la CAI.**
   - Le gabarit doit 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.

2.4. Paramètres de confidentialité et protection de la vie privée par défaut

Plus haut niveau de confidentialité. La LPRPSP prévoit qu'une entreprise 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. Cette exigence ne s'applique toutefois pas aux témoins de connexions (*cookies*).

Protection de la vie privée dès la conception. Cette exigence semble s'inspirer de l'approche de « protection de la vie privée dès la conception » en vertu notamment de l'article 25 du RGPD. Cette approche vise à assurer le respect du droit à la vie privée des personnes concernées 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 LPRPSP 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.

Meilleures pratiques

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. Effectuer un inventaire de toutes les technologies utilisées pour recueillir des renseignements personnels et déterminer si elles comportent des fonctions permettant de profiler, de localiser ou d'identifier un individu.
3. Déterminer si ces paramètres de confidentialité ou ces fonctions technologiques doivent être ajustés pour se conformer aux nouvelles exigences de confidentialité par défaut. Cela peut inclure l'ajustement de certains paramètres de confidentialité pour fournir le plus haut niveau de confidentialité par défaut et la mise en œuvre de nouveaux processus pour demander à l'utilisateur d'activer certaines fonctions.

3. Transparence et consentement

La LPRPSP établit des règles applicables en matière de transparence et de consentement.

3.1. Transparence et obligation d'information préalable au consentement

Termes simples et clairs. Sur le plan de la transparence, les entreprises ont une obligation de fournir certaines informations en « termes simples et clairs », quel que soit le moyen utilisé pour recueillir les renseignements.

Obligation de transparence. Dans ses Lignes directrices sur la validité du consentement (les « Lignes directrices sur le consentement ») et dans l'enquête menée conjointement sur TikTok (2025), la CAI énonce clairement que la transparence constitue par défaut la base légale pour recueillir des renseignements personnels. Cette approche est particulière au Québec et se distingue d'autres lois canadiennes ou internationales sur la protection des renseignements personnels, lesquelles encadrent la collecte de renseignements par le consentement.

Cette obligation de transparence survient lors de la collecte (et par la suite, sur demande) ou dans certains cas, uniquement sur demande et, le cas échéant, lors de l'utilisation de certaines technologies :

- **Lors de la collecte.** L'entreprise qui recueille des renseignements personnels auprès d'une personne doit, lors de la collecte et par la suite sur demande, l'informer : (1) des fins auxquelles ces renseignements sont recueillis; (2) des moyens par lesquels les renseignements sont recueillis; (3) des droits d'accès et de rectification prévus par la loi; (4) de son droit de retirer son consentement à la communication ou à l'utilisation des renseignements recueillis; et, le cas échéant, (5) du nom du tiers pour qui la collecte est faite; (6) 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; et (7) de la possibilité que les renseignements soient communiqués à l'extérieur du Québec.
- **Sur demande.** Une entreprise doit également informer, sur demande, la personne concernée : (1) des renseignements personnels recueillis auprès de lui; (2) des catégories d'employés qui ont accès à ses renseignements au sein de l'entreprise; (3) de la durée de conservation de ses renseignements; et (4) des coordonnées du responsable de la PRP. Lorsqu'elle recueille des renseignements personnels auprès d'une autre entreprise, une entreprise doit, à la demande de la personne concernée, l'informer de la source de ces renseignements, à moins qu'il s'agisse d'un dossier d'enquête constitué en vue de prévenir, détecter ou réprimer un crime ou une infraction à la loi.
- **Technologie d'identification, de localisation et de profilage.** Une entreprise qui recueille des renseignements personnels en ayant recours à une technologie qui comprend des fonctions permettant d'identifier, de localiser ou d'effectuer le profilage d'une personne doit préalablement informer la personne du recours à une telle technologie et des moyens offerts pour activer ces fonctions. 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 ». Cette exigence peut ainsi s'appliquer à diverses technologies, ainsi que dans différents contextes (p. ex. certains outils de surveillance des employés, les témoins de connexion et les technologies similaires utilisées pour la publicité ciblée, etc.).

L'interprétation de l'article 8.1 par la CAI confirme que l'emploi de ce type de ce type de technologies doit être explicitement permis par les personnes. En effet, dans ses Lignes directrices sur le consentement, la CAI statue que ces technologies doivent être désactivées par défaut. Dans tous les cas, à la lumière de l'interprétation de la CAI, il est nécessaire d'envisager de revoir l'utilisation de certaines technologies pour profiler, localiser ou identifier des personnes et de mettre en œuvre des processus pour demander à l'utilisateur d'activer certaines fonctions. On peut penser notamment aux bannières de consentement pour l'utilisation de cookies; en effet, les utilisateurs doivent être informés de l'utilisation de cookies et de la manière d'activer certaines fonctions, comme le profilage).

- **Collecte par l'entremise de moyens technologiques.** Une entreprise qui recueille des renseignements personnels par un moyen technologique doit publier sur son site Internet une politique de confidentialité rédigée en termes simples et clairs et la diffuser par tout moyen propre à atteindre les personnes concernées. L'expression « tout moyen propre » vise vraisemblablement à encourager une entreprise à informer les personnes de ses pratiques en matière de traitement des renseignements en utilisant des moyens pratiques et facilement accessibles. Une entreprise a les mêmes obligations de transparence (celles détaillées à l'art. 8.2) si sa pratique et/ou sa politique fait l'objet d'une modification. Voir la section 2.2 pour plus de détails sur le contenu des politiques de confidentialité.

D'autres lois canadiennes en matière de protection des renseignements personnels accordent aux personnes un droit similaire d'obtenir des renseignements sur le traitement des renseignements personnels. Toutefois, ce droit s'inscrit dans le cadre du droit d'accès, ce qui signifie qu'une entreprise 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 LPRPSP sépare ces deux droits, créant ainsi un régime plus souple pour les demandes faites en vertu des dispositions susmentionnées. Il est néanmoins recommandé d'agir avec diligence, car le fait de ne pas informer les personnes conformément à ces dispositions est l'une des situations énumérées qui donnent lieu expressément à l'imposition de SAPs (voir la section 1).

Prise de décision automatisée. La LPRPSP impose également des exigences de transparence pour une entreprise qui utilise des renseignements personnels pour rendre une décision fondée exclusivement sur le traitement automatisé de ces renseignements. Voir la section 3.4 pour les détails quant à ces exigences.

Meilleures pratiques

1. **Réviser et mettre à jour les politiques de confidentialité (tant celles visant les clients que celles visant les employés) et les formulaires et processus d'obtention du consentement. S'assurer que les éléments suivants sont 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 des fournisseurs de services (le cas échéant).
   - Transfert des renseignements à l'extérieur du Québec (le cas échéant).
2. **Développer et mettre en place un processus visant à répondre aux questions et aux demandes d'information suivantes des clients ou des employés :**
   - Nature des renseignements personnels recueillis par l'entreprise.
   - Catégories d'employés qui pourraient avoir accès aux renseignements personnels.
   - Durée de conservation applicable aux renseignements recueillis auprès de la personne.
   - Coordonnées du responsable de la PRP.
   - Source des renseignements recueillis auprès d'une autre entreprise (sauf si les renseignements ont été recueillis dans le cadre d'une enquête visant à prévenir, détecter ou réprimer un crime ou une infraction à la loi).
3. **Répertorier les technologies utilisées pour recueillir des renseignements personnels et déterminer si elles comportent des fonctions permettant de profiler, de localiser ou d'identifier une personne.**

   Le cas échéant, pour chaque fonction :

   - Vérifier si des processus adéquats sont en place pour informer les personnes, au moment de la collecte, de l'utilisation de la technologie et des moyens d'activer la fonction. Le cas échéant, envisager de mettre en place de nouveaux processus pour demander à l'utilisateur d'activer la fonction.
4. **Déterminer si des renseignements personnels (de clients ou d'employés) sont collectés par l'entremise de moyens technologiques. Le cas échéant :**
   - Faire l'inventaire de ces moyens technologiques.
   - Publier une politique de confidentialité sur le site Internet de l'entreprise détaillant ces collectes par l'entremise de moyens technologiques.
   - Diffuser la politique de confidentialité par tout moyen approprié pour atteindre les personnes concernées par la collecte de renseignements personnels par des moyens technologiques.
   - Mettre en place une procédure pour mettre à jour la politique de confidentialité afin de s'assurer qu'elle reflète bien les pratiques de l'entreprise et que les personnes sont adéquatement informés des changements.

3.2. Critère de nécessité et exigences du consentement

La LPRPSP fixe les modalités relatives à la forme du consentement, aux critères de validité du consentement et aux exigences relatives à l'obtention du consentement de mineurs. Elle prévoit également un critère de nécessité pour la collecte.

Critère de nécessité. La LPRPSP exige que toute entreprise qui entend recueillir des renseignements personnels identifie au préalable une fin sérieuse, légitime et précise à cette collecte. Une fois cette fin déterminée, l'entreprise ne peut recueillir que les renseignements strictement nécessaires à l'atteinte de cette finalité. Le critère de nécessité n'est pas facultatif : il s'impose en toutes circonstances, indépendamment de l'obtention d'un consentement. À noter que ce critère de nécessité s'impose à toute les étapes du cycle de vie des renseignements personnels, et non pas seulement au moment de recueillir le consentement. Selon les orientations de la CAI, une collecte n'est considérée nécessaire que si toutes les conditions suivantes sont réunies :

- La fin poursuivie est légitime, réelle et importante;
- La collecte est rationnellement liée à cette fin;
- Il n'existe pas de moyens moins intrusifs pour parvenir au même résultat; et
- L'avantage de la collecte pour l'entreprise l'emporte sur tout préjudice potentiel pour la personne concernée.

Ainsi, selon les décisions de la CAI Imprimeries Transcontinental Inc. (2024) (« **Décision Transcontinental** ») et 13859380 Canada Inc. (Crane Supply) (2025) (« **Décision Crane Supply** »), les entreprises recueillant des renseignements personnels doivent démontrer la nécessité de la collecte en démontrant :

1) Le « caractère légitime, important, réel de l'objectif qu'elle poursuit par cette collecte »; et
2) La « proportionnalité de l'atteinte à la vie privée que constitue cette collecte en lien avec les objectifs qu'elle poursuit ».

Dans le cadre du premier critère, la CAI a jugé, dans la Décision Transcontinental que, pour établir le caractère réel de l'objectif poursuivi par une entreprise, celle-ci doit établir que l'objectif « est soutenu par des évènements particuliers ou problématiques qui justifient la nécessité de la collecte de renseignements personnels et non simplement par des faits de nature hypothétique ».

Quant au second critère sur la proportionnalité de l'atteinte, la CAI établit, dans la Décision Crane Supply, que l'analyse doit déterminer trois éléments :

- **L'utilisation est rationnellement liée à chaque objectif.** Est-ce que la collecte est un moyen efficace d'atteindre les objectifs poursuivis?
- **L'atteinte est minimisée.** L'entreprise pouvait-elle utiliser d'autres moyens moins intrusifs permettant d'atteindre les objectifs visés?
- Les collectes effectuées par l'entreprise sont nettement plus utiles à l'entreprise que préjudiciables pour les personnes. Quelle est l'expectative de vie privée des personnes?

À défaut, la collecte ne doit pas être effectuée et, en cas de doute, les renseignements sont présumés non nécessaires. Selon les orientations de la CAI, la nécessité doit être évaluée par rapport à chacune des fins envisagées, et il appartient à l'entreprise d'en faire la démonstration. En règle générale, le refus de fournir de tels renseignements ne peut servir de motif pour refuser un produit, un service ou un emploi, sauf si la collecte est nécessaire à la conclusion ou à l'exécution d'un contrat, si elle est autorisée par la loi, ou s'il existe des motifs raisonnables de croire que la demande est illicite.

Forme du consentement. Pour ce qui est de la forme du consentement, la CAI reconnait que le consentement a été obtenu dès que l'obligation de transparence est respectée et que les individus fournissent leurs renseignements personnels. Selon nous, cela s'apparente à une forme d'échange de volonté où le fait d'accepter de fournir ses renseignements personnels constitue une manifestation de la volonté d'être lié. En ce sens, on pourrait dire que le consentement est présumé. Ceci étant dit, la LPRPSP dispose également qu'un renseignement personnel ne peut être utilisé au sein de l'entreprise qu'aux fins pour lesquelles il a été recueilli, ni communiqué à un tiers, à moins que la personne 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.

Ainsi, le consentement sous la LPRPSP peut être exprès ou implicite/présumé. Or, le consentement implicite ou présumé n'est possible, selon les Lignes directrices sur le consentement, que si les critères suivants sont respectés :

- L'utilisation ou la communication ne va pas à l'encontre des attentes raisonnables des personnes selon le contexte; et
- Aucun risque de préjudice grave n'émerge de l'utilisation ou de la communication prévue.

Certains ont adopté la position qu'il y a une incertitude relativement à l'interprétation à donner à ces dispositions, à savoir si un consentement manifesté de façon expresse doit être obtenu pour la collecte de renseignements personnels sensibles, et ce, même si l'entreprise s'est assuré de bien décrire les fins de collecte dans sa politique de confidentialité, puisqu'aucune distinction n'est faite entre renseignements personnels sensibles et non sensibles à l'article 8.3. Dans la mesure où les critères des articles 8 et 8.3 sont satisfaits, nous estimons que rien n'empêche l'utilisation d'un consentement implicite. 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. Or, la pratique générale est d'obtenir un consentement exprès pour les fins secondaires dès lors que la collecte implique des renseignements personnels sensibles en raison, non seulement de la nature des renseignements, mais aussi, des risques de sanction en cas de non-conformité à la LPRPSP (voir la section 1 pour plus d'informations sur les sanctions).

Par ailleurs, la CAI fait la distinction entre le consentement pour les fins dites « primaires » et les fins dites « secondaires » :

- Fins primaires : « désigne les fins auxquelles les renseignements personnels sont recueillis par une organisation. Elles concernent la fourniture d'un service ou d'un produit ou l'accès à un emploi. Elles sont annoncées lors de la collecte. »
- Fins secondaires : « désigne toutes les autres fins poursuivies par une organisation. »

Dans ses Lignes directrices sur le consentement, la CAI établit que le consentement pour les fins primaires peut être présumé pour autant que les personnes ont dûment reçu les informations requises par la loi (voir la section 2.2). Dans tous les cas, la collecte, l'utilisation ou la communication des renseignements personnels pour des fins primaires ou secondaires devra nécessiter un consentement valide. À noter qu'il existe une certaine incertitude concernant la définition exacte de « fins secondaires », celles-ci pouvant désigner des fins n'ayant pas été divulguées au moment de la collecte ou des fins qui ne sont pas essentielles au contrat ou service offert par l'entreprise.

Validité du consentement. Les Lignes directrices sur le consentement fournissent des précisions sur les critères de validité du consentement en vertu de la LPRPSP. Notamment, la CAI précise que, pour obtenir un consentement valide, les entreprises doivent respecter les critères suivants :

- **Le consentement doit être manifeste.** La CAI interprète le caractère manifeste du consentement comme étant évident et donné de façon qui démontre la volonté réelle de la personne concernée.
- **Le consentement doit être libre.** La liberté de choix ou de consentement implique un choix et un contrôle réel de la personne concernée. L'exercice du choix ne doit pas être influencé indûment et la personne ne doit pas subir un préjudice dit disproportionné. À noter que la CAI indique que le fait de ne pas donner son consentement doit être aussi simple que le donner. En d'autres mots, les options doivent être présentées équitablement, sans quoi le consentement peut être considéré comme étant invalide. Par ailleurs, la CAI réitère qu'une entreprise ne peut exiger la collecte de renseignements personnels comme condition de service à moins que celle-ci soit essentielle à la fourniture des produits ou l'accès à l'emploi (c'est-à-dire pour les fins primaires). Pour ce faire, la CAI indique que les entreprises ont l'obligation de permettre aux personnes de refuser la collecte de leurs renseignements personnels pour les fins secondaires (définies plus haut). Dans l'éventualité où les finalités de la collecte changent, il se peut que l'entreprise doive demander le consentement des personnes à nouveau.
- **Le consentement doit être éclairé.** La personne concernée doit comprendre ce à quoi elle consent et ce que cela implique. Selon la CAI, le consentement éclairé en est un qui est non seulement précis, mais fondé sur des connaissances appropriées. La personne donnant le consentement doit être apte à consentir, c'est-à-dire, ne pas avoir moins de 14 ans ou être inapte. Bien entendu, un consentement donné par des représentants autorisés sera considéré comme étant valide selon les Lignes directrices sur le consentement. Les informations indiquées à l'article 8 de la LPRPSP permettent l'obtention d'un consentement éclairé (voir la section 2.2 pour plus d'informations sur les politiques de confidentialité).
- **Le consentement doit être donné à des fins spécifiques.** Ce principe est fortement lié au principe précédent, soit le consentement éclairé. La CAI interprète ce dernier comme demandant un objet précis et circonscrit; c'est-à-dire, le(s) but(s) de l'utilisation ou de la communication de renseignements personnels doivent être définis le plus précisément possible. Les termes employés pour définir ces finalités doivent être adéquats et ne peuvent être vagues, larges ou imprécis. Ainsi, le consentement est restrictif et toute nouvelle finalité requiert un nouveau consentement.
- **Le consentement doit être granulaire.** La LPRPSP requiert que le consentement soit demandé pour chacune des fins visées. Selon les Lignes directrices sur le consentement, ce principe permet d'obtenir un consentement réellement libre, car il permet clairement aux personnes concernées de clairement manifester leur accord et désaccord avec les fins visées.

- **La demande de consentement doit être compréhensible.** La LPRPS requiert que la demande de consentement soit effectuée selon des termes simples et clairs. Selon les Lignes directrices sur le consentement, le principe entourant l'obtention d'un consentement compréhensible a comme objectif de garantir le caractère éclairé et assurer la spécificité du consentement.
- **Le consentement doit être temporaire.** Conformément à la LPRPSP, le consentement n'est valable que pour la durée nécessaire pour accomplir les fins visées par la demande. Ainsi, l'aspect temporaire du consentement se calcule, selon la CAI, soit en fonction d'un délai (p. ex. un nombre de jours, mois, etc.) ou d'un événement (p. ex. paiement est complété, etc.).
- **La demande de consentement doit être présentée de manière distincte.** La LPRPSP demande à ce que les demandes de consentement effectuées par écrit soient présentées de façon séparée de toute autre information. Ainsi, les Lignes directrices sur le consentement prévoient que la demande se doit d'être séparée, à titre d'exemple des conditions d'utilisation, des politiques de confidentialité, des signatures, etc.

Consentement de mineurs. Le consentement du mineur de moins de 14 ans est donné par le titulaire de l'autorité parentale ou par le tuteur. Le consentement du mineur de 14 ans et plus peut lui être donné par le mineur, par le titulaire de l'autorité parentale ou alors par le tuteur.

Meilleures pratiques

1. Faire l'inventaire des renseignements personnels collectés, utilisés et communiqués par l'entreprise (clients et employés) afin de déterminer :

- Ceux qui sont de nature sensible.
- Ceux relatifs à des mineurs.
- Ceux qui sont exclus du champ d'application de la loi (p. ex. coordonnées d'affaires).

2. Faire l'inventaire des formulaires de consentement ou autres documents utilisés pour obtenir le consentement des personnes concernées (clients 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.
- 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.

→ Suite à la page suivante

Meilleures pratiques

3. **Mettre en place un processus afin de s'assurer que sur demande d'une personne (clients ou employés) :**
    - L'entreprise a une procédure en place afin de lui prêter assistance et l'aider à comprendre la portée du consentement demandé.
4. **Mettre à jour la politique de classification ou de catégorisation de l'entreprise (ou tout autre document pertinent) afin d'y refléter :**
    - Les renseignements qui sont de nature sensible et ceux relatifs à des mineurs.
5. **Assurer un suivi diligent des consentements obtenus pour garantir que la volonté des clients est suivie et que tout changement apporté au consentement est appliqué au sein de l'entreprise. Ceci peut notamment se faire par l'utilisation d'une plateforme de gestion des consentements.**

3.3. Exceptions à l'exigence du consentement

La LPRPSP prévoit des exceptions au consentement, permettant l'utilisation ou la communication de renseignements personnels sans celui-ci dans des situations prédéterminées.

Utilisation sans consentement. En vertu de la LPRPSP, un renseignement personnel peut être utilisé à des fins autres que celles pour lesquelles il a été initialement recueilli, sans le consentement de la personne concernée, dans les situations suivantes :

- **Fins d'affaires légitimes.** Lorsque son utilisation est nécessaire à des fins de fourniture ou de livraison d'un produit ou de prestation d'un service demandé par la personne ou encore nécessaire à des fins de prévention et de détection de la fraude ou d'évaluation et d'amélioration des mesures de protection et de sécurité.
- **Intérêt de la personne.** Lorsque son utilisation est manifestement au bénéfice de cette dernière.
- **Recherche, analyse de données et IA.** Lorsque son utilisation est nécessaire à des fins d'étude, de recherche ou de production de statistiques et qu'il est dépersonnalisé, c'est-à-dire qu'il ne permet plus d'identifier directement une personne (voir ci-dessous pour plus d'informations sur la dépersonnalisation ou encore la section 6.2 sur l'anonymisation).
- **Fins compatibles.** Lorsque son utilisation est à des fins compatibles avec celles pour lesquelles il a été recueilli.

Communication sans consentement. En vertu de la LPRPSP, un renseignement personnel peut 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 adéquates sont prévues. Voir la section 5.1 pour plus de détails sur cette exception.

- **Recherche, analyse de données et IA.** Lorsque la communication est faite 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. 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'entreprise), bien qu'un cadre spécifique s'applique à ces types de projets de recherche. Voir ci-dessous pour des détails sur ce régime.
- **Transaction commerciale.** Lorsque la communication est nécessaire pour la conclusion d'une transaction commerciale (p. ex. l'aliénation ou la location d'une entreprise ou des actifs dont elle dispose, une modification de sa structure juridique par fusion ou autrement, l'obtention d'un prêt, de financement ou d'une sûreté), sous réserve qu'une entente soit conclue avec l'autre partie, stipulant que cette dernière s'engage : (1) à n'utiliser le renseignement qu'aux seules fins de la conclusion de la transaction commerciale; (2) à ne pas communiquer le renseignement sans le consentement de la personne à moins d'y être autorisée par la loi; (3) à prendre les mesures nécessaires pour assurer la protection du caractère confidentiel du renseignement; (4) à détruire le renseignement si la transaction commerciale n'est pas conclue ou si l'utilisation de celui-ci n'est plus nécessaire. Une fois la transaction commerciale conclue, si l'autre partie souhaite utiliser ou communiquer les renseignements personnels, elle ne peut le faire que dans la mesure prévue par la loi. Enfin, dans un délai raisonnable après la conclusion de la transaction commerciale, l'entreprise doit aviser la personne concernée qu'elle détient désormais ses renseignements personnels en raison de la transaction.

Renseignements relatifs à l'exercice d'une fonction d'affaire. La LPRPSP exclut les « renseignements personnels concernant l'exercice par la personne concernée d'une fonction au sein d'une entreprise » du champ d'application de ses sections II et III (c'est-à-dire, les exigences en matière d'avis et de consentement). Cela comprend « 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 ». Quoique cette exclusion puisse être utile à certaines entreprises qui souhaitent utiliser ce type de renseignements sans consentement, ces dernières doivent tout de même appliquer les exigences de la Loi canadienne anti-pourriel qui régissent l'utilisation d'adresses courriel (incluant celles de travail) pour transmettre des messages électroniques commerciaux.

Relations d'emploi. Il convient de souligner que la LPRPSP n'établit pas d'exception au consentement pour la collecte, l'utilisation ou la communication de renseignements personnels afin d'établir, gérer ou mettre fin à une relation d'emploi. Toutefois, l'absence d'une telle exception peut créer des difficultés pour les employeurs considérant les limites du modèle du consentement dans le contexte des relations employeur/employé. Selon les Lignes directrices sur le consentement de la CAI, il est effectivement difficile de considérer le consentement d'un employé dans ses relations avec son employeur comme étant « libre » en raison du déséquilibre de pouvoir inhérent à la relation d'emploi. Un employé peut croire, à tort ou à raison, que son emploi serait compromis par un refus de consentement. En revanche, si un employé refuse que son employeur collecte, utilise ou communique ses renseignements personnels à des fins de pratiques administratives courantes, cela pourrait empêcher l'employeur de poursuivre ses activités et de remplir ses obligations légales. La CAI invite ainsi les entreprises à prendre des mesures d'atténuation adaptées à leur contexte, notamment en

veillant à la neutralité des demandes de consentement, en offrant des solutions de rechange lorsque possible et en assurant une transparence accrue.

Exception pour la communication à des fins de recherche. La LPRPSP permet de communiquer des renseignements personnels à des fins de recherche sous certaines conditions, incluant :

- La réalisation d'une EFVP arrivant aux conclusions suivantes : (1) les renseignements personnels sont nécessaires pour atteindre l'objectif de la recherche; (2) il est déraisonnable d'exiger de la personne requérante qu'elle obtienne le consentement des personnes concernées; (3) 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; (4) les renseignements sont utilisés de manière à en assurer la confidentialité, et (5) seuls les renseignements nécessaires sont communiqués.
- Une vérification diligente des politiques et pratiques de l'entreprise requérante. Ceci est d'autant plus important puisque, si la personne requérante est victime d'un incident de confidentialité compromettant les renseignements communiqués (voir la section 7.2 sur les incidents de confidentialité), l'entreprise divulgatrice pourrait faire l'objet d'un examen minutieux advenant une enquête de la CAI.
- La conclusion d'une entente entre les parties qui stipule notamment les modalités d'accès, les mesures de sécurité, les conditions d'utilisation, de communication et de conservation, et l'obligation d'aviser la CAI et l'entreprise divulgatrices en cas d'incident de confidentialité ou de violations de l'entente.
- Un avis à la CAI de l'entente intervenue entre les parties, qui entrera en vigueur 30 jours suivant sa réception par celle-ci. À noter que bien que la LPRPSP n'accorde pas explicitement à la CAI le pouvoir de résilier l'entente si celle-ci ne remplit pas toutes les exigences, la CAI pourrait ordonner à l'entreprise divulgatrice de ne pas communiquer les renseignements jusqu'à ce que l'entente soit révisée pour inclure les éléments requis, suspendre l'entente ou exercer ses autres pouvoirs de surveillance prévus dans la loi.

Exception pour la recherche et les analyses internes. La LPRPSP autorise les entreprises à utiliser, sans le consentement des personnes, les renseignements personnels qu'elles détiennent à des fins d'étude, de recherche ou de production de statistiques, à condition que ceux-ci soient dépersonnalisés.

Étant donné que l'exception au consentement prévue à l'article 12 s'applique à l'utilisation des renseignements personnels au sein de l'entreprise, il est tout naturel d'interpréter les termes « étude » ou « recherche » comme englobant l'analyse commerciale. En effet, par analogie avec la définition d'un « projet de recherche » trouvée dans la Loi sur les renseignements de santé et de services sociaux, l'analyse commerciale constitue elle aussi une démarche structurée visant le développement des connaissances et l'innovation. 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 3.4).

La LPRPSP prévoit qu'un renseignement personnel est « dépersonnalisé lorsqu'il ne permet plus d'identifier directement la personne concernée ». Cette définition correspond essentiellement à la notion de « pseudonymisation » des données telle qu'elle est généralement comprise, notamment dans le Règlement général sur la protection des données (« **RGPD** »). À titre comparatif, la LPRPSP

prévoit également des critères pour l'anonymisation des renseignements personnels en précisant qu'un renseignement concernant une personne physique est anonymisé lorsqu'il ne permet plus, de façon irréversible, d'identifier directement ou indirectement cette personne (voir la section 6.2 pour plus d'informations sur l'anonymisation).

Il est intéressant de noter que le libellé de l'article 12 prévoit aussi clairement qu'aucun consentement n'est nécessaire, même lorsque ces renseignements sont sensibles préalablement à leur anonymisation.

Dans la décision Val-des-Cerfs (2022), la CAI a considéré que les données transmises par l'organisme à son partenaire pour le développement de l'algorithme étaient des renseignements personnels dépersonnalisés et non des renseignements anonymisés, puisque les mesures prises par l'entreprise n'étaient pas irréversibles. La CAI a conclu que les renseignements dans la base de données permettent à l'organisme d'identifier les élèves en utilisant d'autres données recueillies tout au long de leur cheminement scolaire (p. ex. identification indirecte). Il sera intéressant de suivre l'évolution de cette décision afin de voir si le raisonnement sera adopté dans d'autres instances.

La LPRPSP reconnaît le risque de réidentification lié aux renseignements dépersonnalisés en obligeant les entreprises 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 ». D'ailleurs, bien que cela ne soit pas expressément indiqué, il serait conforme à la définition des renseignements personnels sensibles prévue par la LPRPSP (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. Contrairement à l'anonymisation, un renseignement dépersonnalisé demeure un renseignement personnel soumis à la LPRPSP.

Il est important de noter que la recherche interne menée en vertu des dispositions susmentionnées peut nécessiter la réalisation d'une EFVP lorsqu'elle s'inscrit dans le cadre d'un projet d'acquisition, de développement et de refonte d'un système d'information ou de prestation électronique de services (voir la section 2.3).

Meilleures pratiques

1. **Faire régulièrement l'inventaire des utilisations pouvant faire l'objet d'une exception à l'exigence du consentement afin de déterminer si ces dernières tombent sous l'application des exceptions suivantes :**
    - Utilisation nécessaire à des fins de fourniture ou de livraison d'un produit ou de prestation d'un service demandé par la personne concernée.
    - Utilisation nécessaire à des fins de prévention et de détection de la fraude.
    - Utilisation nécessaire à des fins ou d'évaluation et amélioration des mesures de protection et de sécurité.
    - 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 des fins d'étude, de recherche ou de production de statistiques (et les renseignements sont dépersonnalisés).

→ Suite à la page suivante

Meilleures pratiques

2. **Faire l'inventaire des communications pouvant faire l'objet d'une exception à l'exigence du consentement afin de déterminer si ces dernières tombent sous l'application des exceptions suivantes :**
   - 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.
3. **Mettre en place une procédure visant à gérer les communications de renseignements personnels dans un contexte de transaction d'affaires ou de recherche.**
4. **Faire preuve de prudence lorsque l'entreprise se base sur l'exception des « fins compatibles » pour utiliser des renseignements personnels sensibles dans le cadre de recherches internes. Lorsque les renseignements sont sensibles, la CAI peut se demander si l'utilisation à une fin secondaire correspond aux attentes raisonnables de la personne plutôt que de se demander si cette utilisation est « objectivement » compatible avec les fins initiales.**
5. **Prendre les mesures nécessaires pour réduire le risque de réidentification, lorsque l'entreprise utilise des renseignements dépersonnalisés en vertu de l'exception pour les « fins d'étude ou de recherche » et adopter des mesures plus rigoureuses pour éviter la réidentification lorsque les renseignements personnels sous-jacents aux renseignements dépersonnalisés sont sensibles.**
6. **Mettre en place une procédure visant à effectuer une évaluation des facteurs relatifs à la vie privée si la recherche interne s'inscrit dans le cadre d'un « projet d'acquisition, de développement et de refonte d'un système d'information ou de prestation électronique ».**

3.4. Prise de décision automatisée

La LPRPSP impose des obligations de notification pour les entreprises utilisant des renseignements personnels pour prendre une décision concernant une personne, qui est fondée exclusivement sur le traitement automatisé de ces renseignements, c'est-à-dire qu'aucune intervention humaine n'est impliquée. Il pourrait s'agir, par exemple, de situations où une entreprise 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 client ou en utilisant un système biométrique.

Exigences en matière de notification et d'information. La LPRPSP exige que les entreprises informent les personnes 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. Les entreprises utilisant des technologies pour prendre des décisions basées exclusivement sur le traitement automatisé de renseignements personnels devraient aussi indiquer cette utilisation dans leur politique de confidentialité.

La LPRPSP oblige également les entreprises à informer, sur demande, la personne visée par une telle décision :

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

L'expression « traitement automatisé » n'est pas définie dans la LPRPSP. D'éventuelles lignes directrices de la CAI seront donc essentielles pour circonscrire la portée des exigences introduites à l'article 12.1. Bien que les modifications introduites par la LPRPSP semblent viser la prise de décision automatisée au moyen d'algorithmes technologies d'intelligence artificielle (IA) et dont l'incidence sur les droits individuels est majeure, le libellé de cette disposition est rédigé de façon suffisamment large pour inclure toutes sortes d'autres processus automatisés de prise de « décision ». En l'absence de définition claire, plusieurs entreprises ont choisi de limiter son application aux décisions qui ont une certaine incidence sur les droits et obligations des individus (excluant ainsi, par exemple, la publicité ciblée).

Il convient de mentionner que l'expression « traitement automatisé » semble être repris du RGPD 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 du règlement, des Lignes directrices sur l'interprétation des dispositions du RGPD régissant le traitement automatisé. 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 ». La CNIL en France a aussi produit sa propre interprétation des termes. La LPRPSP ne comporte pas de telles restrictions, ce qui compliquera sans doute un travail d'interprétation de la CAI. En l'absence de lignes directrices, les entreprises peuvent toutefois se préparer aux 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 ».

L'obligation d'informer la personne « des raisons » ayant mené à la décision semble équivaloir d'exiger une 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 la personne moyenne. Bien que la mention des « principaux facteurs et paramètres » donne une indication quant au niveau de détail requis, les entreprises doivent, en l'absence de lignes directrices, faire preuve de prudence afin d'éviter de communiquer des renseignements qui pourraient (1) divulguer des secrets commerciaux ou violer le droit de propriété intellectuelle de l'entreprise ou de tiers (comme les fournisseurs de services qui fournissent la technologie de traitement automatisé) ou (2) permettre à des tiers mal intentionnés de s'infiltrer dans leur système.

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'entreprise en mesure de réviser la décision ». Les activités de traitement automatisé qui visent des personnes 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 la LPRPSP n'accorde pas aux personnes un droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé (comme celui prévu par le 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. En d'autres termes, l'entreprise 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 entreprises 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, elles doivent être prêtes à évaluer les observations soumises par les personnes 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.

Meilleures pratiques

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 entreprises peuvent avec prudence envisager de suivre l'interprétation donnée au « traitement automatisé » en vertu du RGPD.**
2. **Mettre en place une procédure pour s'assurer que lorsqu'une entreprise prend des décisions fondées exclusivement sur le traitement automatisé de renseignements personnels, elle :**
   - En informe les personnes par l'entremise de sa politique de confidentialité;
   - a mis en place une procédure conforme aux meilleures pratiques prévues dans la section 4.
3. **Faire preuve de prudence dans la communication des raisons ayant mené à la décision, qui pourraient :**
   - Révéler des secrets commerciaux ou violer les droits de propriété intellectuelle de l'entreprise ou de tiers (comme les fournisseurs de technologies de traitement automatisé);
   - Permettre à des tiers mal intentionnés d'infiltrer le système.
4. **Être prêt à évaluer les observations des personnes 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.**

4. Droits individuels

En vertu de la LPRPSP, les personnes se voient accorder plusieurs droits individuels : un droit d'accès aux renseignements personnels, un droit de rectification, un droit de contrôler la diffusion de leurs renseignements personnels (également connu sous le nom de « droit à la désindexation »), un droit à la portabilité des données, un droit d'être informé d'une prise de décision automatisée et de soumettre des observations (voir la section 3.4) et un droit d'obtenir des renseignements sur le traitement des données (voir la section 3.1).

4.1. Droit d'accès et de rectification

Toute personne a le droit, en vertu de la LPRPSP, de savoir si une entreprise détient des renseignements personnels à son sujet et d'y avoir accès. Elle peut aussi en demander la rectification lorsque l'information est inexacte, incomplète ou équivoque, ou lorsque sa collecte, sa communication ou sa conservation n'est pas autorisée par la loi. L'entreprise doit alors apporter les correctifs appropriés et mettre à jour les dossiers concernés.

L'accès aux renseignements personnels est gratuit, sauf frais limités au coût de transcription, reproduction ou transmission, annoncés d'avance et fixés par le Règlement sur les frais.

Format de la demande. Une entreprise ne doit prendre en considération que les demandes formulées par écrit par une personne qui prouve qu'elle est bel et bien la personne concernée par les renseignements personnels ou par un représentant autorisé, tel qu'un titulaire de l'autorité parentale.

Délai de réponse à la demande. Le responsable de la PRP doit répondre à la demande par écrit dans les 30 jours suivants sa réception. Cependant, l'entreprise peut soumettre une demande à la CAI dans cette période initiale de 30 jours pour prolonger le délai de réponse. Contrairement à d'autres lois canadiennes en matière de protection des renseignements personnels, aucune limite n'est fixée concernant le nombre total de jours pour lequel la CAI peut prolonger le délai.

Refuser la demande. Lorsque la demande est refusée, le responsable de la PRP doit répondre par écrit, motiver le refus, indiquer la disposition sur laquelle le refus est fondé (le cas échéant) et informer le demandeur des recours qui lui sont disponibles et du délai pour les exercer. Sur ce dernier point, l'entreprise doit informer le demandeur de son droit de soumettre une demande d'examen de mésentente à la CAI dans les 30 jours suivant le refus d'accéder aux renseignements. Sur demande, le responsable de la PRP doit également aider le demandeur à comprendre le refus.

Repérage complet et sérieux. Pour assurer le respect de ces droits, le responsable de la PRP doit effectuer un repérage complet et sérieux des renseignements personnels visés par toute demande adressée à l'entreprise. Pour l'appuyer dans cette démarche, la CAI met à disposition une Fiche d'information précisant les bonnes pratiques à chaque étape.

Restrictions au droit d'accès. Le droit d'accès n'est pas absolu. Ainsi, l'entreprise saisie d'une demande d'accès peut refuser de les communiquer, notamment lorsque la divulgation des renseignements est susceptible de révéler l'identité d'un tiers et de nuire sérieusement à un tiers n'y ayant pas consenti ou d'avoir une incidence sur une procédure judiciaire en cours, ou si la demande est manifestement abusive.

4.2. Droit à la désindexation

La LPRPSP donne aux personnes le droit de contrôler la diffusion de leurs renseignements personnels, notamment par les entreprises qui facilitent la diffusion de ces renseignements, comme les moteurs de recherche, les éditeurs de contenu et les intermédiaires en ligne (p. ex. réseaux sociaux). Ce droit, également connu sous le nom de droit à la désindexation, a pour principal objectif de renforcer le contrôle des personnes sur leur réputation et leur vie privée en ligne en limitant l'accès du public aux renseignements personnels lorsque leur diffusion est illégale ou porte gravement atteinte à la réputation ou à la vie privée. Contrairement au droit à l'oubli prévu par le RGPD, le droit à la désindexation du Québec n'est pas un droit à l'effacement des renseignements personnels en soi, mais plutôt un droit plus limité de restreindre la diffusion des renseignements.

Notons au passage que le droit de demander la suppression des renseignements personnels est prévu à l'article 28 de la LPRPSP et à l'article 40 du CCQ, lesquels prévoient trois situations où une personne peut demander à une entreprise de supprimer un renseignement personnel qu'elle détient à son sujet : (1) lorsque le renseignement est périmé; (2) lorsque la conservation du renseignement n'est plus justifiée au regard de la finalité pour laquelle il a été recueilli; ou (3) lorsque le renseignement a été recueilli de manière non conforme à la loi.

Portée du droit à la désindexation. En vertu de ce droit, une personne peut empêcher une entreprise de diffuser ses renseignements personnels ou peut demander à ce que soit désindexé (ou, pour être plus précis, « déréférencer » des résultats de recherche) un hyperlien rattaché à son nom permettant d'accéder à un renseignement personnel, lorsque la diffusion de ce renseignement (1) contrevient à la loi ou à une ordonnance judiciaire ou (2) cause un préjudice grave relatif au droit au respect de sa réputation ou de sa vie privée.

En pratique, cela signifie qu'une entreprise qui reçoit ce type de demande doit non seulement conclure que le préjudice existe réellement et qu'il n'est pas simplement hypothétique ou potentiel, mais aussi qu'il l'emporte sur le droit du public à l'information et sur la liberté d'expression de l'éditeur ou du créateur de contenu, et que la mesure demandée n'est pas excessive pour empêcher la perpétuation du préjudice. Pour faire cette évaluation, l'entreprise doit spécifiquement prendre en compte un certain nombre de facteurs prescrits, tels que : le statut de personnalité publique de la personne, l'âge de la personne, les types de renseignements personnels diffusés, le contexte et le temps écoulé depuis la diffusion.

Il est intéressant de noter que ce droit prévoit la possibilité de « réindexer » les hyperliens rattachés au nom d'une personne lorsque cela peut empêcher une atteinte grave à la réputation ou à la vie privée d'une personne.

Format de la demande. Ces types de demandes suivent exactement le même processus que les demandes d'accès et de rectification. Toutefois, lorsqu'une telle demande est accueillie, le responsable de la PRP doit répondre par écrit et fournir une attestation que les renseignements ne sont plus diffusés ou que l'hyperlien a été désindexé ou réindexé, selon le cas.

Bien que la LPRPSP donne aux héritiers, aux successeurs, aux liquidateurs d'une succession et à un certain nombre d'autres personnes la possibilité d'exercer le droit d'accès ou de rectification d'une personne décédée, il n'est pas clair si cette autorisation vaut également pour le droit à la désindexation.

Évaluation du bien-fondé de la demande. Étant donné que le demandeur est généralement mieux placé pour apporter des éléments de preuves à l'appui de sa demande, c'est à ce dernier qu'incombe le fardeau d'établir que la diffusion des renseignements personnels est en fait illégale ou qu'elle cause un préjudice grave à sa réputation ou à sa vie privée.

4.3. Droit à la portabilité des données

Considérée comme une extension au droit d'accès, la portabilité des données accorde aux personnes un droit supplémentaire de recevoir les renseignements personnels informatisés recueillis auprès d'eux 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 ». Ces renseignements doivent également être communiqués sous la forme d'une transcription écrite et intelligible. Pour plus de renseignements, voir notre article *La Loi 25 n'a pas dit son dernier mot : des réponses à vos questions sur le droit à la portabilité des données au Québec*.

Signification d'un « format technologique structuré et couramment utilisé ». Les termes « structuré », « couramment utilisé » et « technologique » ne sont pas explicitement définis dans la LPRPSP, et leur signification est susceptible de varier selon l'industrie ou le secteur concerné. Selon les orientations du Gouvernement du Québec, les formats ouverts, tels que CSV, XML et JSON, accompagnés de métadonnées utiles à la compréhension de leur signification, sont adaptés au droit de portabilité des données.

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. 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. Afin de protéger les intérêts commerciaux des entreprises, y compris les algorithmes utilisés pour générer des données inférées, le droit à la portabilité des données exclut expressément de son champ d'application les renseignements personnels qui ont été créés ou inférés à partir des renseignements recueillis auprès de la personne. Les données inférées peuvent par exemple prendre la forme de déductions sur la probabilité qu'un client achète certains produits ou services ou encore 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 (voir la section 2.3 pour plus d'informations sur les EFVP).

Format de la demande. Ce type de demandes suit exactement le même processus que les demandes d'accès et de rectification.

Exemptions à la portabilité des données. Le droit à la portabilité, comme le droit d'accès qu'il complète, n'est pas absolu. L'entreprise saisie d'une demande en vertu de ce droit peut refuser de les communiquer pour les raisons suivantes :

- **En présence de difficultés pratiques sérieuses.** Lorsque la fourniture des renseignements dans un format technologique structuré et couramment utilisé « soulève des difficultés pratiques sérieuses » pour l'entreprise qui reçoit la demande, cette dernière peut être exemptée de l'obligation de se conformer à cette exigence. De telles difficultés peuvent notamment résulter des coûts importants et/ou de la complexité que nécessite le transfert des renseignements vers le format approprié ou à un

tiers. Une entreprise qui invoque un tel motif doit être en mesure de faire la preuve de telles difficultés si jamais la demande devait être révisée par la CAI.

- **Si une restriction au droit d'accès s'applique.** Comme la portabilité constitue une extension du droit d'accès, les dispositions qui autorisent les entreprises à refuser l'accès à certains renseignements sont applicables. En ce sens, les renseignements personnels informatisés dont la divulgation serait susceptible de révéler des renseignements personnels sur une tierce personne sont susceptibles d'être exclus des exigences d'accès et de portabilité en vertu de l'article 40 de la LPRPSP.
- **Si la demande est manifestement abusive**, les entreprises peuvent refuser la portabilité si les demandes sont manifestement infondées ou excessives, notamment en raison de leur caractère répétitif, systématique ou non conforme à l'objet de la loi, à condition d'obtenir une autorisation de la CAI.

Meilleures pratiques

1. **Dresser un inventaire des pratiques susceptibles de faire intervenir les droits individuels susmentionnés afin de déterminer si ces pratiques relèvent de l'une des situations suivantes :**
   - L'entreprise diffuse un contenu susceptible de contenir des renseignements personnels ou exploite un outil de recherche en ligne ou un service d'indexation similaire qui génère des résultats de recherche (sous forme d'hyperliens) sur la base du nom d'une personne.
   - L'entreprise collecte des renseignements personnels informatisés auprès des personnes.
2. **Dresser un inventaire des politiques et procédures existantes pour le traitement des demandes relatives à la vie privée ou de tout document similaire (clients ou employés) et les examiner pour s'assurer que :**
   - L'entreprise est capable de reconnaître et de répondre à une demande (verbale ou écrite) d'information sur le traitement des données.
   - L'entreprise est en mesure de fournir, sur demande, des renseignements personnels informatisés à la personne, ou à une personne ou une entreprise autorisée par la loi à recueillir de tels renseignements, dans un format technologique structuré et couramment utilisé.
3. **Si l'entreprise diffuse des renseignements personnels ou exploite un outil de recherche en ligne, mettre en place une procédure pour garantir que :**
   - L'entreprise est en mesure de recevoir, d'évaluer et de répondre à une demande de droit à la désindexation dans les délais prescrits.
   - L'entreprise a mis en place un processus lui permettant de déterminer si la diffusion des renseignements personnels (i) contrevient à la loi ou à une ordonnance judiciaire ou cause un préjudice grave au droit de la personne au respect de sa réputation ou de sa vie privée; et (ii) le cas échéant, cause un préjudice qui l'emporte sur le droit du public à l'information et sur la liberté d'expression de l'éditeur ou du créateur de contenu.
   - L'entreprise est en mesure de vérifier l'identité du demandeur qui fait la demande (conformément aux lois applicables).
   - L'entreprise est en mesure de fournir des attestations (si la demande est acceptée) que les renseignements ne sont plus diffusés ou que l'hyperlien a été désindexé ou réindexé, selon le cas.

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

La LPRPSP énonce des exigences en matière d'impartition et de communication de renseignements à l'extérieur du Québec.

5.1. Impartition

Transparence. Tel qu'indiqué à la section 3.1, la LPRPSP requiert que l'entreprise indique à la personne, 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 aux fins décrites dans la politique de confidentialité de l'entreprise. Ceci implique que la politique de confidentialité de l'entreprise doit indiquer que les renseignements personnels pourront être transmis à ses fournisseurs de services (catégorie de tiers) ou nommer ceux-ci individuellement.

Exception au consentement. Tel qu'indiqué à la section 3.3, la LPRPSP permet la communication de 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. Cette exception permet donc à l'entreprise de transmettre des renseignements personnels à ses mandataires et fournisseurs de services sans que la personne n'ait à consentir à ceci, sous réserve de dispositions contractuelles spécifiques entre l'entreprise et ses fournisseurs de services. Nous référons au paragraphe « Entente écrite » ci-dessous pour les exigences relatives aux annexes de protection des renseignements personnels.

Obligation d'effectuer une EFVP. 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'entreprise, celle-ci doit procéder à une EFVP. Bien que cette responsabilité incombe à l'entreprise, les fournisseurs de services doivent collaborer à cet exercice. Nous référons à la section 2.3 pour les exigences relatives aux EFVP.

Entente écrite. La LPRPSP requiert en outre que le traitement de renseignements personnels par un fournisseur de services soit sujet à un contrat écrit devant inclure les mesures que le fournisseur de services doit prendre :

- **Protéger le caractère confidentiel du renseignement personnel communiqué.** Le contrat doit 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;

- **N'utiliser les renseignements que dans le cadre de l'exécution du contrat.** Le contrat doit donc prohiber l'utilisation des renseignements personnels par le fournisseur pour ses fins propres ou pour les fins d'un tiers;
- **Ne pas conserver les renseignements personnels après l'expiration du contrat;**
- **Aviser sans délai le responsable de la protection des renseignements personnels 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
- **Permettre au responsable de la protection des renseignements personnels d'effectuer toute vérification relative à cette confidentialité.**

Au-delà de ce qui est exigé par la LPRPSP, une entente écrite de cette nature comprend entre autres les éléments suivants :

- Informer l'entreprise de toute demande reçue d'une personne concernée relative à des renseignements personnels ou à tout droit susceptible de découler des lois canadiennes en matière de protection des renseignements personnels;
- Informer l'entreprise de toute demande de divulgation émanant d'un organisme gouvernemental ou réglementaire et coopérer avec celle-ci; et
- Encadrer, restreindre ou interdire les transferts de renseignements personnels à l'extérieur du Québec/Canada.

Obligation de notifier les violations des obligations de confidentialité. La LPRPSP requiert également que le fournisseur de services avise sans délai le responsable PRP de l'entreprise 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 les incidents de confidentialité. La CAI n'a pas encore clarifié si les parties peuvent aménager 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'entreprise. 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. La CAI n'a pas encore clarifié 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.

Ces deux obligations (entente écrite et obligation de notifier les violations des obligations de confidentialité) ne s'appliquent pas lorsque le fournisseur de services est un organisme public au sens de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels ou un membre d'un ordre professionnel.

Meilleures pratiques

1. **Politique de confidentialité.** Réviser la politique de confidentialité de l'entreprise pour s'assurer qu'elle indique que les renseignements personnels pourront être transmis à ses fournisseurs de service. Si l'entreprise le souhaite, la politique pourra nommer ces fournisseurs.
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 :
   - 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'entreprise en cas de violation ou tentative de violation des obligations de confidentialité; et
   - La possibilité pour l'entreprise de demander tout document et d'effectuer toute vérification relative à la confidentialité des renseignements.
4. **Recenser les fournisseurs de services traitant des renseignements personnels pour l'entreprise.** L'entreprise devra alors :
   - Déterminer si un contrat écrit conforme aux exigences de la pratique 2 a bien été conclu avec chaque fournisseur de services; et
   - Dans la négative, transmettre le modèle de contrat de traitement des renseignements personnels décrit à la pratique 3 ci-dessus aux fournisseurs de services concernés.
5. **Communiquer avec les fournisseurs de services existants dont les systèmes/prestations requièrent que l'entreprise mène une EFVP.** Sur la base de la liste mentionnée à la pratique 4 ci-dessus, l'entreprise devrait prévoir de :
   - Communiquer avec chaque fournisseur de services existant que l'entreprise souhaite impliquer dans 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'entreprise va mener une EFVP pour laquelle elle aura besoin de sa collaboration; et
   - Lorsque le modèle d'EFVP aura été développé par l'entreprise, celui-ci devrait être transmis aux fournisseurs de services pour qu'ils aident l'entreprise à compléter les informations factuelles et techniques relatives aux systèmes/services concernés.
6. **Effectuer les EFVP.** Une EFVP devra être menée par l'entreprise 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.

5.2. Transferts hors Québec

Transparence. Tel qu'indiqué à la section 3.1, l'entreprise qui collecte des renseignements personnels auprès de personnes 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.

Obligation d'effectuer une EFVP. Les transferts de renseignements personnels à l'extérieur du Québec sont une préoccupation majeure de la LPRPSP, telle que modifiée par la Loi 25. Ainsi, une entreprise 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 est tenue d'effectuer une EFVP qui tient compte des facteurs suivants :

- La sensibilité des renseignements,
- La finalité de leur utilisation,
- Les mesures de protection, y compris contractuelles, qui s'y appliqueront, et
- Le régime juridique applicable dans l'État de réception, notamment les principes de protection des renseignements personnels qui y sont applicables. Il est à noter que la LPRPSP fait référence à des « principes », et non à une « loi » sur la protection des renseignements personnels.

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 le transfert sera autorisé. Notons que la LPRPSP ne précise pas en quoi consistent les principes de protection des renseignements personnels généralement reconnus et ne définit pas explicitement la notion de protection adéquate. Selon le Guide d'accompagnement sur les EFVP de la CAI, on entend par « protection adéquate » une protection « offrant des garanties juridiques (législation de l'État de destination) et contractuelles (entente avec l'entreprise destinataire) respectant l'ensemble des principes de protection généralement reconnus et appropriés en regard de la sensibilité et de la finalité des renseignements impliqués. » De plus, selon ce même guide, les principes de protection des renseignements personnels généralement reconnus sont « des règles générales permettant d'assurer la protection des renseignements personnels, mais également le respect des droits et des intérêts des personnes concernées en cette matière. »

La CAI y énumère également plusieurs principes clés, soit :

- Responsabilité
- Détermination des fins
- Limitation de la collecte
- Consentement
- Protection dès la conception et par défaut
- Limitation de l'utilisation, de la communication et de la conservation
- Exactitude
- Sécurité
- Transparence
- Droits des personnes concernées
- Recours

Entente écrite. Si l'EFVP démontre que les renseignements traités à l'étranger feront l'objet d'une protection adéquate, l'entreprise doit conclure avec le tiers une entente écrite qui tient compte, notamment des résultats de l'EFVP et, le cas échéant, des modalités convenues dans le but d'atténuer les risques identifiés dans le cadre de cette évaluation.

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 18.3, 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.

Meilleures pratiques

1. **Réviser la politique de confidentialité de l'entreprise pour préciser que les renseignements personnels pourront être communiqués à l'extérieur du Québec (et non simplement du Canada).**
2. **Effectuer une cartographie des renseignements communiqués en dehors du Québec.** Cet exercice permettra d'obtenir une description des flux de renseignements. L'entreprise 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 (p. ex. dans le cadre d'un service sous-traité vers une filiale située dans un pays tiers); et
   - 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; et
   - Le régime juridique applicable dans l'État de réception.
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 ».
   - Dans un premier temps, faute d'indication plus précise sur ce point, les entreprises pourront vérifier si la législation de l'État en question respecte les principes de protection de la vie privée figurant dans le Guide d'accompagnement pour réaliser une EFVP.

→ Suite à la page suivante

Meilleures pratiques

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 18.3 décrites à la section 5.1, et
   - Prévoir des mesures de protection modulables en fonction des résultats de l'EFVP.
6. **Préparer un modèle de contrat (ou de clauses) avec les tiers non-fournisseurs de services situés hors du Québec.** Ce modèle devra :
   - Imposer aux tiers de respecter les principes de protection des renseignements personnels généralement reconnus; et
   - Prévoir des mesures de protection modulables en fonction des résultats de l'EFVP.
7. **Compléter la procédure d'impartition décrite à la section 5.1 pour refléter les exigences liées à la communication de données en dehors du Québec.**

6. Conservation et destruction

Le LPRPSP énonce des exigences particulières aux entreprises en matière de conservation et de destruction des renseignements personnels.

6.1. Conservation et destruction

Période de conservation. Les entreprises ne doivent conserver que les renseignements personnels nécessaires aux fins pour lesquels ils ont été recueillis. Cette période correspond au moment pendant lequel les renseignements sont détenus, peu importe leur forme, support ou degré d'utilisation. Pendant ce temps, l'entreprise doit veiller à ce que les renseignements demeurent à jour et exacts lorsqu'ils servent à prendre une décision à propos d'une personne et appliquer des mesures de sécurité adaptées pour en assurer la protection.

Aussitôt que les renseignements personnels ne sont plus nécessaires pour les objectifs préalablement déterminés, ceux-ci doivent être détruits de manière sécuritaire ou anonymisés (voir la section 6.2 pour plus de détails sur cette alternative). La seule restriction à cette obligation de destruction est le délai de conservation prévu par une loi (p. ex. Loi canadienne sur les sociétés par actions, Loi de l'impôt sur le revenu, etc.).

Procédure de destruction. La méthode de destruction doit être adaptée au support et au niveau de confidentialité des documents et assurer la destruction définitive des renseignements personnels qu'ils contiennent. Afin d'assurer l'efficacité de cette démarche, la CAI recommande aux entreprises de mettre en place une procédure de gestion documentaire, désigner des responsables chargés de son application et en informer tout le personnel.

Cette procédure doit permettre d'inventorier les types de documents contenant des renseignements personnels, de définir des niveaux de confidentialité en fonction de leur sensibilité, de leur finalité, de leur quantité, de leur répartition et de leur support, et de distinguer les supports afin d'appliquer des méthodes de conservation et de destruction adaptées. Enfin, les entreprises devraient prévoir un calendrier de conservation conforme aux exigences légales, en rappelant que la notion de « document » englobe l'ensemble des supports physiques ou numériques.

Le choix d'une méthode de destruction adaptée est essentiel pour assurer la destruction définitive des renseignements personnels, puisqu'une technique appropriée pour un support physique (p. ex. papier) ne conviendra pas nécessairement aux supports numériques. À cet égard, la CAI fournit des orientations précisant les méthodes de destruction adaptées à chaque type de support.

La destruction des documents contenant des renseignements personnels peut être réalisée à l'interne ou confiée à un prestataire externe lorsque l'équipement de l'entreprise ne permet pas de le faire de façon sécuritaire. Dans ce dernier cas, un contrat écrit doit encadrer la prestation afin de garantir la confidentialité et la sécurité des renseignements, en précisant notamment le procédé utilisé, les engagements de confidentialité, l'entreposage sécuritaire, la possibilité d'audit par l'entreprise et l'obligation de rapporter toute violation. En attendant la prise en charge par le fournisseur, l'entreprise demeure responsable de sécuriser adéquatement les documents à détruire.

6.2. Anonymisation

Définition. Un renseignement est considéré anonymisé lorsqu'il est « en tout temps, raisonnable de prévoir dans les circonstances qu'il ne permet plus, de façon irréversible, d'identifier directement ou indirectement » une personne. Un renseignement anonymisé ne constitue plus un renseignement personnel et échappe ainsi au régime juridique qui s'y applique. Les renseignements anonymisés se distinguent des renseignements dépersonnalisés (voir la section 3.3 pour plus de détails).

Possibilité d'anonymisation. La LPRPSP prévoit l'anonymisation comme alternative à la destruction des renseignements personnels. Ainsi, suivant l'accomplissement de la finalité de leur collecte, il est possible de conserver les renseignements personnels en procédant à leur anonymisation pour les utiliser à des fins sérieuses et légitimes. Notons que l'article 23 ne traite pas de l'anonymisation effectuée avant ce moment précis du cycle de vie du renseignement personnel, mais seulement de celle qui intervient une fois la finalité initiale accomplie. Ceci dit, cela ne veut pas dire que l'anonymisation n'est permise qu'à titre d'alternative à la destruction. Nous sommes d'avis que rien n'interdit l'anonymisation à d'autres étapes précédentes du cycle de vie des renseignements personnels.

Selon la CAI, l'anonymisation des renseignements personnels comporte des limites importantes : il est pratiquement impossible de garantir qu'un renseignement anonymisé ne puisse jamais être réidentifié, surtout compte tenu des avancées technologiques. Certains types de données, comme les renseignements génétiques, biométriques ou ceux relatifs à la géolocalisation, sont si distinctifs qu'ils échappent difficilement à une réidentification potentielle. Ainsi, l'anonymisation demeure associée à des risques d'incidents de confidentialité, et toute tentative de réidentifier une personne à partir de tels renseignements est passible de sanctions.

Procédure d'anonymisation. Les entreprises doivent procéder à l'anonymisation des renseignements personnels suivant les « meilleures pratiques généralement reconnues » et « selon les critères et modalités déterminés par règlement ». En vertu du Règlement sur l'anonymisation des renseignements personnels, elles sont tenues de respecter les obligations suivantes :

- Établir les fins « sérieuses et légitimes » pour lesquelles les renseignements anonymisés seront utilisés.
- Réaliser le processus d'anonymisation sous la supervision d'une personne compétente en la matière. Pour ce faire, les entreprises devraient confier la supervision à un professionnel qualifié en anonymisation et en protection des renseignements personnels, ou, à défaut d'expertise interne, recourir aux services d'un fournisseur externe.
- Retirer tous les renseignements permettant d'identifier directement la personne concernée (nom, coordonnées, NAS, etc.) avant de procéder à l'anonymisation. Ces données deviennent alors des renseignements dépersonnalisés au sens de la LPRPSP.
- Effectuer une analyse préliminaire des risques de réidentification, en tenant compte notamment des critères d'individualisation, de corrélation et d'inférence, ainsi que des renseignements raisonnablement disponibles pouvant être utilisés pour identifier une personne.
- Déterminer, en fonction des risques de réidentification, les techniques d'anonymisation à privilégier (p. ex. randomisation et généralisation), en veillant à ce qu'elles soient conformes aux meilleures pratiques généralement reconnues à l'échelle internationale.

- Établir des mesures de protection et de sécurité raisonnables pour réduire les risques de réidentification, conformément aux exigences de la LPRPSP.
- Effectuer une analyse démontrant que les risques résiduels de réidentification demeurent très faibles, en tenant compte des circonstances, de la nature des renseignements, des critères d'individualisation, de corrélation et d'inférence, ainsi que des moyens raisonnablement disponibles pour réidentifier une personne. Le Règlement sur l'anonymisation précise que ce critère n'exige pas la démonstration d'un risque nul.
- Procéder à une évaluation périodique des renseignements anonymisés, en mettant à jour l'analyse des risques de réidentification à une fréquence déterminée selon les risques résiduels précédemment identifiés, afin de démontrer que les renseignements demeurent anonymisés. À défaut, ils cessent d'être considérés comme tels.
- Tenir un registre d'anonymisation consignant la description des renseignements anonymisés, les fins d'utilisation, les techniques et mesures de sécurité appliquées, ainsi que les dates des analyses de risques de réidentification et de leurs mises à jour. Ce registre doit être conservé aussi longtemps que nécessaire afin de permettre à l'entreprise de démontrer sa conformité.

De plus, toute entreprise qui collecte des renseignements personnels doit établir et appliquer des règles de gouvernance encadrant notamment leur destruction, lesquelles doivent obligatoirement inclure, le cas échéant, des dispositions relatives à l'anonymisation.

Meilleures pratiques

1. **Élaborer un calendrier de conservation clair et conforme aux lois applicables, précisant pour chaque catégorie de documents la durée de conservation et le moment où la destruction ou l'anonymisation doit être effectuée.**
2. **Mettre en place une procédure de gestion documentaire encadrée par des responsables désignés, incluant l'inventaire des documents, la classification par niveaux de confidentialité et la formation du personnel.**
3. **Sélectionner des méthodes de destruction adaptées aux supports et au degré de sensibilité des renseignements, en suivant les orientations de la CAI et en s'assurant que les données soient détruites de façon définitive et sécuritaire.**
4. **Définir clairement les fins sérieuses et légitimes justifiant l'anonymisation, en s'assurant qu'elles soient documentées et intégrées aux règles de gouvernance de l'entreprise.**
5. **Évaluer et gérer les risques de réidentification de façon continue, en appliquant des techniques reconnues (randomisation, généralisation) et en tenant compte des critères prévus par le Règlement, afin de garantir que les risques résiduels demeurent très faibles.**
6. **Conserver un registre complet et à jour du processus d'anonymisation, incluant les renseignements anonymisés, les fins d'utilisation, les techniques employées, les mesures de sécurité et les résultats des analyses de risques, afin de démontrer la conformité en tout temps.**

7. Cybersécurité et gestion des incidents de confidentialité

Le LPRPSP impose des mesures de protection des renseignements personnels aux entreprises et fait de la notification des incidents de confidentialité une obligation.

7.1. Cybersécurité

Mesures de sécurité. Les entreprises 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, et plus les mesures de sécurité devront être robustes. Il est important de noter que les entreprises demeurent responsables de la protection des renseignements qu'elles détiennent, même lorsqu'ils sont sous la garde d'un tiers.

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.

Le CAI fournit plusieurs exemples de mesures à adopter par les entreprises. Parmi celles-ci on retrouve :

- Des mesures de gouvernance (p. ex. mettre sur pied un comité de sécurité de l'information et de protection des renseignements personnels et concevoir et mettre à jour des politiques et pratiques de gouvernance des renseignements personnels suffisamment robustes);
- Des mesures tactiques (p. ex. concevoir un plan d'action annuel et former et sensibiliser les employés);
- Des mesures opérationnelles (p. ex. octroyer des droits d'accès, élaborer des modèles types et les réviser périodiquement et utiliser un protocole d'identification robuste);
- Des mesures techniques (p. ex. contrôler les accès aux bureaux, aux salles des serveurs, aux salles de câblage, au système d'alarme, et restreindre l'accès aux locaux ou aux classeurs où sont conservés des documents papier contenant des renseignements personnels); et
- Des mesures techniques (p. ex. favoriser les identifiants et les mots de passe forts, assurer le chiffrement des communications et des informations stockées, mettre en place un coupe-feu, etc.).
- Elle propose également la démarche suivante pour assurer la sécurité des renseignements personnels :
- Prendre connaissance et respecter vos obligations en matière de protection des renseignements personnels;
- Cartographier les renseignements personnels détenus par l'entreprise et en apprécier la sensibilité;
- Repérer et analyser les risques et leurs effets possibles sur la vie privée des personnes concernées;
- Choisir des mesures de sécurité adaptées au contexte et aux risques susmentionnés;

- Mettre en œuvre les mesures de sécurité retenues;
- Évaluer l'efficacité des mesures déployées;
- Assurer un suivi continu et réviser ces mesures au besoin.

Mesures de protection. En matière d'EFVP, la LPRPSP prévoit que le responsable de la PRP puisse suggérer, à toute étape d'un projet, des « mesures de protection des renseignements personnels » applicables au projet (voir la section 2.3 sur les EFVP). Ces « mesures de protection » décrites à l'article 3.4 de la loi s'ajoutent ainsi à celles de mettre en place les mesures de sécurité appropriées prévues à l'article 10 de la LPRPSP. À tout événement, le responsable de la PRP devrait collaborer en continu avec un expert en sécurité pour assurer une cohérence dans l'identification et la mise en place des mesures de sécurité et de protection.

Meilleures pratiques

1. **Catégoriser les actifs informationnels de manière à y attribuer des mesures de sécurité correspondant au niveau de catégorisation.**
   - Les niveaux de catégorisation devraient tenir compte du niveau de sensibilité des renseignements personnels, et des besoins en confidentialité, intégrité et disponibilité.
2. **Mettre en place un système de collaboration entre le responsable de la PRP et le département de sécurité de manière à ce que les mesures de sécurité et de protection soient effectives et cohérentes d'un projet à l'autre.**
   - Au besoin, former un comité pour la PRP réunissant le responsable de la PRP, de la sécurité, de la gouvernance et des TI.
3. **Si applicable, mettre à jour les procédures afin que le personnel n'entre pas en communication avec des agents d'évaluation du crédit si un gel de sécurité a été porté à un dossier en vertu de la *Loi sur les agents d'évaluation du crédit*.**

7.2. Incidents de confidentialité

Incident de confidentialité. Le Québec est la troisième juridiction au Canada, avec le fédéral et l'Alberta, à se doter d'un régime de notification obligatoire des incidents de confidentialité présentant un « risque de préjudice sérieux ». La LPRPSP définit la notion d'incident de confidentialité comme étant l'accès, l'utilisation, la communication non autorisée, la perte de renseignements personnels ou toute autre atteinte à la protection de renseignements personnels. Cette définition étant plutôt large, toute atteinte, brèche ou incident de sécurité touchant les renseignements personnels tombe sous l'application de l'article 3.6 de la loi. Parmi les différents types d'incidents de confidentialité, on retrouve par exemple 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 est la seule juridiction au Canada à inclure l'utilisation non autorisée de renseignements personnels dans sa définition d'incident de confidentialité.

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 notion de « risque de préjudice sérieux » proposée par le législateur québécois se distingue subtilement à celle de « risque réel de préjudice grave » prévue à la Loi sur la protection des renseignements personnels et les documents électroniques (« **LPRPDÉ** ») et la Personal Information Protection Act (« **PIPA** ») de l'Alberta, le terme « réel » ayant été omis. De plus, contrairement à la LPRPDÉ, la LPRPSP 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 (p. ex. 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'entreprise ou publiés sur le Web caché (*Dark Web*), ils risquent d'être utilisés à de mauvaises fins.

Bien que les critères d'évaluation de la LPRPDÉ et de la PIPA soient en apparence similaires avec le test formulé par la LPRPSP, il se peut que la CAI interprète les obligations de notification de manière plus stricte, puisque le risque de préjudice sérieux n'aura pas à être réel pour que se déclenche l'obligation de notification. Dans tous les cas, le responsable de la PRP devra être consulté pour effectuer cette évaluation.

Notification des incidents. Si l'entreprise détermine que l'incident présente un risque de préjudice sérieux pour les personnes touchées, elle doit aviser la CAI ainsi que toute personne concernée par l'incident, à défaut de quoi la CAI pourra lui ordonner de le faire. Il est également prévu que l'entreprise peut, à sa discrétion, aviser toute personne ou organisme susceptible de réduire le risque de dommage, 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 protection des renseignements personnels doit enregistrer la communication. Aucun délai n'est prévu pour la notification des incidents, mais celle-ci devra se faire avec « diligence », selon l'article 3.5 de la LPRPSP.

Si un incident de confidentialité se produit chez un fournisseur de services tiers ou un sous-traitant à qui des renseignements personnels ont été externalisés, certaines conditions relatives à la notification des incidents devraient être prévues contractuellement (voir la section 5). Toutefois, puisque ces obligations de notification s'appliquent à toute entreprise, et ce, peu importe le rôle qui leur est attribué, dans le traitement des renseignements personnels, un fournisseur de services ou un sous-traitant pourrait être tenu de signaler l'incident puisque l'obligation s'applique à « toute personne exploitant une entreprise qui a des motifs de croire que s'est produit un incident de confidentialité impliquant des renseignements personnels qu'elle détient ».

Malgré qui précède, soulignons qu'une personne concernée par un incident de confidentialité n'a pas à être avisée si un tel avis est 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.

Avis à la CAI. En vertu du Règlement sur les incidents de confidentialité, les renseignements suivants doivent être notifiés à la CAI lorsque l'entreprise constate qu'un incident de confidentialité présentant un risque de préjudice sérieux a eu lieu :

- Le nom de l'entreprise ayant fait l'objet de l'incident de confidentialité et, le cas échéant, le numéro d'entreprise du Québec qui lui est attribué en vertu de la Loi sur la publicité légale des entreprises;
- Le nom et les coordonnées de la personne à contacter au sein de l'entreprise relativement à l'incident;
- Une description des renseignements personnels visés par l'incident ou, si cette information n'est pas connue, la raison justifiant l'impossibilité de fournir une telle description;
- Une brève description des circonstances de l'incident et, si elle est connue, sa cause;
- La date ou la période où l'incident a eu lieu ou, si cette dernière n'est pas connue, une approximation de cette période;
- La date ou la période au cours de laquelle l'entreprise a pris connaissance de l'incident;
- Le nombre de personnes concernées par l'incident et, parmi celles-ci, le nombre de personnes qui résident au Québec ou, s'ils ne sont pas connus, une approximation de ces nombres;
- Une description des éléments qui amènent l'entreprise à conclure qu'il existe un risque qu'un préjudice sérieux soit causé aux personnes concernées;
- Les mesures que l'entreprise a prises ou entend prendre afin d'aviser les personnes dont un renseignement personnel est concerné par l'incident, de même que la date où les personnes ont été avisées ou le délai d'exécution envisagé;
- Les mesures que l'entreprise a prises ou entend prendre à la suite de la survenance de l'incident, notamment celles visant à diminuer les risques qu'un préjudice soit causé ou à atténuer un tel préjudice, et celles visant à éviter que de nouveaux incidents de même nature ne se produisent, de même que le délai où les mesures ont été prises ou le délai d'exécution envisagé;
- Le cas échéant, une mention précisant qu'une personne ou un organisme situé à l'extérieur du Québec et exerçant des responsabilités semblables à celles de la CAI à l'égard de la surveillance de la protection des renseignements personnels a été avisé de l'incident.

Il est à noter que la CAI a publié un formulaire d'avis pour signaler un incident de confidentialité. Toutefois, ce formulaire semble requérir plus d'informations que ce que le règlement exige.

Avis aux personnes concernées. Le Règlement sur les incidents de confidentialité prévoit également que la notification aux personnes concernées par un risque de préjudice sérieux à la suite d'un incident de confidentialité doit contenir :

- Une description des renseignements personnels visés par l'incident ou, si cette information n'est pas connue, la raison justifiant l'impossibilité de fournir une telle description;
- Une brève description des circonstances de l'incident;
- La date ou la période où l'incident a eu lieu ou, si cette dernière n'est pas connue, une approximation de cette période;

- Une brève description des mesures que l'entreprise a prises ou entend prendre à la suite de la survenance de l'incident, afin de diminuer les risques qu'un préjudice soit causé;
- Les mesures que l'entreprise suggère à la personne concernée de prendre afin de diminuer le risque qu'un préjudice lui soit causé ou afin d'atténuer un tel préjudice;
- Les coordonnées permettant à la personne concernée de se renseigner davantage relativement à l'incident.

Mitigation des risques. La LPRPSP oblige les entreprises ayant des « motifs de croire » qu'un incident de confidentialité a eu lieu de prendre des « mesures raisonnables pour diminuer le risque 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 tiers assurant la garde ou l'hébergement des renseignements personnels, tel qu'un fournisseur de services ou un sous-traitant. En pratique, cela signifie que les entreprises doivent prendre toutes les mesures appropriées et raisonnables afin de prévenir le préjudice pouvant être causé aux personnes à la suite de l'incident, et ce, même si l'incident ne présente pas de risque de préjudice sérieux. Les mesures à prendre doivent être déterminées en fonction du type d'incident et du contexte applicable, mais peuvent 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 dommage est de 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 un spécialiste de la gestion des incidents.

Registre des incidents. Les entreprises doivent également tenir un registre des incidents de confidentialité, qui doit contenir les renseignements suivants :

- Une description des renseignements personnels visés par l'incident ou, si cette information n'est pas connue, la raison justifiant l'impossibilité de fournir une telle description;
- Une brève description des circonstances de l'incident;
- La date ou la période où l'incident a eu lieu ou, si cette dernière n'est pas connue, une approximation de cette période;
- La date ou la période au cours de laquelle l'entreprise a pris connaissance de l'incident;
- Le nombre de personnes concernées par l'incident ou, s'il n'est pas connu, une approximation de ce nombre;
- Une description des éléments qui amènent l'entreprise à conclure qu'il existe ou non un risque qu'un préjudice sérieux soit causé aux personnes concernées, tels que la sensibilité des renseignements personnels concernés, les utilisations malveillantes possibles de ces renseignements, les conséquences appréhendées de leur utilisation et la probabilité qu'ils soient utilisés à des fins préjudiciables;
- Si l'incident présente un risque qu'un préjudice sérieux soit causé, les dates de transmission des avis à la Commission d'accès à l'information et aux personnes concernées de même qu'une mention indiquant si des avis publics ont été donnés par l'entreprise et la raison pour laquelle ils l'ont été, le cas échéant;
- Une brève description des mesures prises par l'entreprise, à la suite de la survenance de l'incident, afin de diminuer les risques qu'un préjudice soit causé.

Les renseignements contenus au registre doivent être tenus à jour et conservés pendant une période minimale de cinq ans après la date ou la période au cours de laquelle l'entreprise a pris connaissance de l'incident.

Pouvoirs de la CAI. La CAI dispose de plusieurs pouvoirs d'ordonnance en lien avec les incidents de confidentialité. Elle peut notamment ordonner à toute personne d'appliquer les mesures jugées pertinentes afin de protéger les droits des personnes concernées.

Pour plus d'informations sur la manière de prévenir les incidents de confidentialité, veuillez consulter le guide explicatif et la liste de contrôle de la CAI.

Cas particulier des entités réglementées par l'Autorité des marchés financiers. En octobre 2024, l'Autorité des marchés financiers (« **AMF** ») a publié le Règlement sur la gestion et le signalement des incidents de sécurité de l'information de certaines institutions financières et des agents d'évaluation du crédit (« **Règlement de l'AMF** »). Entré en vigueur en avril 2025, le Règlement de l'AMF établit un cadre rigoureux visant à s'assurer que les institutions financières exerçant au Québec mettent en œuvre des mesures proactives pour gérer et signaler les incidents de sécurité de l'information. Les institutions visées comprennent notamment les assureurs, les fédérations et caisses, les institutions de dépôts, les sociétés de fiducie et les agents d'évaluation du crédit.

Le Règlement de l'AMF exige que les institutions financières mettent en œuvre une politique globale de gestion des incidents de sécurité de l'information, laquelle doit inclure des procédures pour détecter, évaluer et répondre aux incidents au sein de l'entreprise, ainsi que ceux impliquant des tiers à qui des activités ont été confiées. Cette politique doit aussi prévoir les modalités de signalement des incidents aux dirigeants et gestionnaires de l'institution, ainsi qu'à toute autre partie prenante, incluant possiblement les consommateurs, les organismes de réglementation et les fournisseurs de services.

Lorsqu'un incident de sécurité de l'information ayant un risque d'occasionner des répercussions négatives est signalé à un dirigeant ou gestionnaire de l'institution, l'institution doit à son tour en informer l'AMF dans un délai de 24 heures. Cette déclaration doit également couvrir tout incident signalé à un autre organisme d'application de la loi ou de réglementation, y compris tout incident de confidentialité déclaré simultanément à la CAI. La déclaration doit être transmise à l'aide du formulaire prescrit par l'AMF, suivie de mises à jour tous les trois jours jusqu'à ce que l'incident soit maîtrisé, puis d'un rapport détaillé dans les 30 jours suivant la résolution. Le Règlement de l'AMF impose aussi aux institutions financières de tenir à jour un registre des incidents de sécurité de l'information, en assurant l'intégrité des données consignées pendant au moins cinq ans. Enfin, il prévoit l'imposition de SAPs en cas de non-conformité.

Meilleures pratiques

1. **Définir une structure organisationnelle prévoyant des rôles et responsabilités clairs en matière de prévention, de gestion et de réponse aux incidents.**
    - Les responsabilités devraient être détaillées et précises en fonction des rôles.
2. **Élaborer et, le cas échéant, mettre à jour la politique de gestion des incidents de l'entreprise de manière à y inclure les nouvelles obligations, et**
    - 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 services 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'entreprise rapidement;
    - Les clauses reflètent la nouvelle définition d'un incident de confidentialité;
    - Le fournisseur est en mesure de communiquer à l'entreprise toutes les informations requises pour lui permettre d'évaluer le risque de préjudice sérieux.
4. **Définir un programme de formation en matière de prévention et de gestion des incidents.**
5. **Tenir un registre au sein de l'entreprise 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'entreprise juge que l'incident ne comporte pas de préjudice sérieux pour les personnes concernées.

8. Biométrie

8.1. Notions

Définition de biométrie. La biométrie (qui signifie littéralement « mesure du corps humain », en grec) est une pratique qui permet l'analyse mathématique des caractéristiques biologiques, morphologiques ou comportementales d'une personne. Lorsque nous parlons de biométrie au sens de la Loi concernant le cadre juridique des technologies de l'information (« **LCCJTI** »), nous nous rapportons aux systèmes déployés pour identifier ou confirmer l'identité d'une personne en utilisant ses données biométriques, telles que les empreintes digitales, la structure de l'iris ou de la rétine, la géométrie de la main ou du visage, ou la voix. Il s'agit d'une nuance importante, puisque les données biométriques sont considérées comme des renseignements personnels sensibles et que ces derniers sont assujettis aux lois sur la protection des renseignements personnels applicables aux secteurs public et privé, et ce, quel que soit le but pour lequel elles sont employées.

Identification et authentification. L'identification et l'authentification sont les principales fonctions de la biométrie. Chacune de ces fonctions dispose de composantes techniques qui lui sont propres, générant ainsi des risques juridiques distincts. Alors que la notion d'« identification » signifie de trouver une identité dans une base de données pour déterminer qui est une certaine personne, la notion d'« authentification » consiste plutôt à vérifier ou à confirmer l'identité de cette personne. Par exemple, l'identification peut être utilisée pour autoriser ou refuser un accès (c'est-à-dire que la présence des données biométriques capturées a été confirmée dans la base de données), alors que l'authentification permet plutôt de vérifier ou de confirmer que la personne est bien celle qu'elle prétend être. La fonction d'identification soulève généralement plus de risques techniques et juridiques puisqu'une base de données biométriques doit être instaurée, ce qui n'est pas nécessairement le cas pour la fonction d'authentification.

Il convient de noter que la CAI adopte une interprétation large et libérale de la notion de vérification de l'identité, estimant que l'objectif premier est d'assurer la protection des renseignements personnels de nature biométrique. Pour interpréter les termes « vérification » et « confirmation », la CAI se réfère au Document d'orientation du Commissariat à la protection de la vie privée du Canada, lequel distingue l'identification de l'authentification. Elle assimile la vérification de l'identité à un processus d'identification, qui vise à établir l'identité d'une personne en comparant ses données biométriques à celles d'une base de données. Elle précise en outre que l'identification ne requiert pas nécessairement une confirmation nominative, mais peut également résulter d'un processus d'association à un groupe restreint de personnes préalablement répertoriés.

Identité. La CAI adopte également une interprétation élargie de la notion d'identité, intégrant sa dimension numérique. Elle considère que l'identité ne se limite pas aux informations d'état civil, mais comprend toute donnée permettant de distinguer une personne des autres. S'appuyant sur l'article 44 de la LCCJTI, la CAI insiste sur le fait que les caractéristiques biométriques d'une personne sont intrinsèquement liées à son identité. Enfin, la CAI insiste sur la nécessité d'adopter une approche globale, tenant compte de l'effet combiné des opérations plutôt que de les examiner isolément.

En d'autres termes, il faut considérer l'effet combiné de l'ensemble des opérations effectuées par le système et considérer ces différentes phases comme étant interdépendantes, et ce, puisque les caractéristiques biométriques sont indissociables de l'identité des personnes.

8.2. Exigences

La LCCJTI et la LPRPSP prévoient quelques dispositions visant à encadrer l'utilisation des bases de données biométriques afin d'en assurer une certaine sécurité. Parmi les obligations incombant aux entreprises figurent l'obligation de réaliser une EFVP, d'obtenir le consentement exprès et de faire une déclaration à la CAI, tels que décrits plus amplement ci-dessous.

Critère de nécessité. Les entreprises doivent s'assurer que la collecte de renseignements biométriques est nécessaire :

- **Les objectifs poursuivis sont légitimes, réels et importants.** Selon le Guide sur la biométrie de la CAI, pour qu'une entreprise puisse démontrer le caractère réel de l'objectif, cette dernière doit prouver qu'elle vise à résoudre une problématique précise ou réelle qui justifiait la collecte de renseignements personnels, en particulier des données biométriques. Cet objectif ne devait pas être à atteindre dans le futur ou être hypothétique. Pour déterminer l'importance d'un objectif, les entreprises doivent prouver que la collecte de données biométriques ne vise pas simplement l'atteinte d'un objectif usuel, courant et intrinsèque à la gestion d'une entreprise. Selon une la décision de la CAI à l'encontre de Metro inc. (2025), bien que le souhait de contrôler les accès aux locaux est un objectif que poursuit toute entreprise, ces dernières doivent présenter des éléments de preuve démontrant un besoin spécial de recueillir et de traiter des données biométriques afin de mieux protéger ses locaux.
- **L'atteinte à la vie privée des personnes concernées est proportionnelle aux objectifs poursuivis.** Selon la LPRPSP, la collecte de renseignements personnels doit être proportionnelle aux objectifs poursuivis. Globalement, les avantages tirés de leur collecte et de leur traitement doivent l'emporter sur l'atteinte à la vie privée des personnes concernées. Il revient aux entreprises d'établir que la collecte est rationnellement liée à ses objectifs, que l'atteinte à la vie privée est minimisée et qu'il n'existe pas d'autres moyens moins intrusifs, et que la collecte de ces renseignements est nettement plus utile que préjudiciable aux personnes concernées. Dans la Décision Transcontinental (2025), celle-ci a conclu que l'absence de consentement exprès suffit à établir une telle atteinte, indépendamment de la finalité poursuivie.

Il convient de noter que le critère de nécessité doit impérativement être respecté pour recueillir des données biométriques, et ce sans égard à l'obtention du consentement. Cela dit, la CAI a systématiquement conclu, à une exception près, que l'utilisation de la biométrie ne satisfaisait pas aux critères permettant d'atteindre le seuil de nécessité. Tout récemment, la CAI a réitéré que cette obligation de nécessité ne peut être contournée, et ce, même lorsque la personne concernée a consenti à la collecte et à l'utilisation de ses données biométriques.

EFVP. Les entreprises doivent procéder à une EFVP avant de déployer tout système biométrique afin d'identifier les risques juridiques et les contrôles à instaurer afin d'atténuer ces risques. À noter que l'EFVP peut faciliter l'analyse de la nécessité de la collecte.

Consentement exprès. Les entreprises ont l'obligation d'obtenir le consentement exprès des personnes pour la collecte de leurs données biométriques. De plus, puisque les personnes doivent être libres de refuser la collecte de leurs données biométriques ou de retirer leur consentement, une solution alternative (p. ex. cartes d'accès, jetons uniques, etc.) doit être prévue. La CAI a publié un modèle de formulaire de consentement à cet effet.

Déclaration à la CAI. Les entreprises doivent déclarer à la CAI l'utilisation de procédés ou systèmes biométriques destinés à la vérification ou à la confirmation de l'identité ainsi que la création d'une banque de caractéristiques ou de mesures biométrique – dans ce cas, la déclaration doit être faite au moins 60 jours avant la mise en service de la banque. 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. La CAI a publié sur son site Internet un formulaire pour déclarer l'utilisation d'un système biométrique. Il est à noter que le même formulaire est utilisé pour la déclaration d'un système biométrique et d'une banque de caractéristiques ou de mesures 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 :

Hélène Deschamps Marquis
Associée
T 514.954.3102
hdeschampsmarquis@blg.com

Frédéric Wilson
Associé
T 514.954.2509
fwilson@blg.com

Élisabeth Lesage-Bigras
Avocate principale
T 514.395.2749
elesagebigras@blg.com

Patrick Laverty-Lavoie
Avocat principal
T 514.395.3887
plavertylavoie@blg.com

Candice Hévin
Avocat principal
T 514.954.2588
chevin@blg.com

Matt Saunders
Avocat-conseil
T 514.954.318
msaunders@blg.com

Cléa Jullien
Avocate
T 514.395.2714
cjullien@blg.com