KPMG

Protection et gouvernance des données

Opérationnalisation des nouvelles exigences et opportunités

JANVIER 2022

Nouvelles exigences en matière de protection des renseignements personnels

Après plus d'un an de discussions et de travaux parlementaires sur le projet de loi 64, la Loi modernisant des dispositions législatives en matière de protection des renseignements personnels a été sanctionnée le 21 septembre 2021 (LQ 2021, c. 25) (ci-après « Loi ») , entraînant par le fait même des modifications significatives à l'encadrement de la protection et au traitement des renseignements personnels (RP) applicables aux organisations et aux entreprises qui recueillent, traitent ou détiennent des renseignements personnels au Québec.

Les premières modifications entreront en vigueur le 22 septembre 2022. L'entrée en vigueur des autres modifications aura lieu en septembre 2023 et 2024.

Plus précisément, quelles sont les nouvelles exigences?

La Loi impose de nouvelles obligations, précise diverses exigences, accorde de nouveaux droits, et prescrit des mesures de gestion des risques en lien avec les projets et solutions qui engagent le traitement des RP, la communication à des tiers et l'externalisation. Elle préconise également la transparence pendant tout le cycle de vie des données. De plus, cette loi accorde plus de pouvoirs à l'autorité réglementaire. Les nouvelles exigences représentent une réforme similaire à celle découlant du Règlement général sur la protection des données (RGPD).

Nous décrivons dans les pages suivantes les exigences d'affaires qui découlent des changements induits par la Loi, tout en proposant un accompagnement des entreprises afin de leur faire prendre le virage numérique et de moderniser leur programme de protection de la vie privée et de gestion des données.

Une occasion à saisir

Les modifications découlant de l'entrée en vigueur de la Loi requièrent des changements importants aux processus et aux pratiques de traitement des données au sein des organisations. Ces changements obligés représentent du même coup l'occasion de revoir et d'optimiser la gouvernance des données, dont la conformité réglementaire est l'une des composantes.

Au-delà des obligations réglementaires, **la Loi représente également l'occasion de reprendre le contrôle sur les données et de valoriser cet actif stratégique,** permettant ainsi :

- **de mettre en œuvre une approche transparente et centrée sur le client et les employés** : la loi vise la protection des droits et des intérêts de vos clients et employés avant tout. Les exigences relatives au consentement et à l'exercice des droits des personnes permettront de communiquer clairement au sujet des mesures mises en place pour la protection des renseignements personnels des clients et employés et ainsi de renforcer le lien de confiance;

- **de renforcer la sécurité** : la mise en œuvre des exigences de la Loi contribuera à la position globale de sécurité de votre organisation;

- **de développer vos capacités en gestion de données** : en reprenant le contrôle, vous aurez une meilleure compréhension de vos données et une plus grande capacité à valoriser cet actif stratégique;

- **d'accélérer le virage numérique** : les données sont au centre des enjeux de transformation numérique. Les nouvelles exigences offrent la possibilité de mettre en place les fondements d'une saine gouvernance et gestion des données, qui est un accélérateur dans le virage numérique;

- **de mettre en place une stratégie de collecte et de gestion des consentements** qui vous rapproche de vos clients et employés et permet de mieux répondre à leurs besoins avec une gestion ciblée de leurs préférences.

Une approche holistique

KPMG privilégie une approche holistique et pragmatique qui s'appuie sur des compétences complémentaires et sur la collaboration avec des professionnels des données : cybersécurité, protection des renseignements personnels, gouvernance des données, automatisation, gestion documentaire, transformation numérique, gestion des identités et des accès, expérience client (« CX ») et gestion du changement.

L'approche doit être cohérente avec le cadre de gestion existant et devrait viser à :

- Organiser la gouvernance de données en définissant :
  - un modèle opérationnel cible;
  - des rôles et des responsabilités;
  - des politiques et des règles relatives à la gestion et à la protection des données;
  - des mesures pour suivre la progression et l'amélioration.
- Élaborer une stratégie de gestion du consentement qui soit réfléchie et intégrée au parcours client;
- Classer et à catégoriser les données et les actifs informationnels afin d'identifier et de cartographier les renseignements personnels;
- Revoir les politiques de sécurité et à renforcer les processus de gestion des incidents, ainsi que la gestion des accès et des contrôles;
- Sensibiliser vos équipes, à former vos employés et à vous accompagner dans ces importants changements organisationnels.

KPMG dispose d'un ensemble de capacités multidisciplinaires et complémentaires en services-conseils pour accompagner les entreprises dans leur parcours de conformité en matière de protection des renseignements personnels (PRP) et de gouvernance des données, de mêmes que dans la mise en place de solides stratégies de gestion du consentement.

Communiquez avec nous!

Jean-François De Rico
Associé responsable,
Protection de la vie privée
KPMG au Canada
jderico@kpmg.ca
418 577-3442

Catherine Nadeau
Directrice principale,
Gouvernance des données
KPMG au Canada
cnadeau@kpmg.ca
514 840-5350

La conformité aux nouvelles exigences

Une approche de renforcement de la conformité par rapport aux nouvelles exigences doit être basée sur les grands axes de travail suivant :

APPROCHE DE RENFORCEMENT DE LA CONFORMITÉ
→ **Évaluation de la situation actuelle**
→ **Définition de la cible et de l'appétit pour le risque**
→ **Analyse des écarts entre la situation actuelle et la cible de conformité**
→ **Définition et priorisation des plans d'actions (feuille de route)**
→ **Choix des solutions technologiques**
→ **Mise en œuvre, gestion du changement, sensibilisation/formation**

Nous décrivons ci-dessous les requis découlant des nouvelles exigences en fonction de leur incidence sur la gouvernance, les processus, la technologie et les ressources humaines :

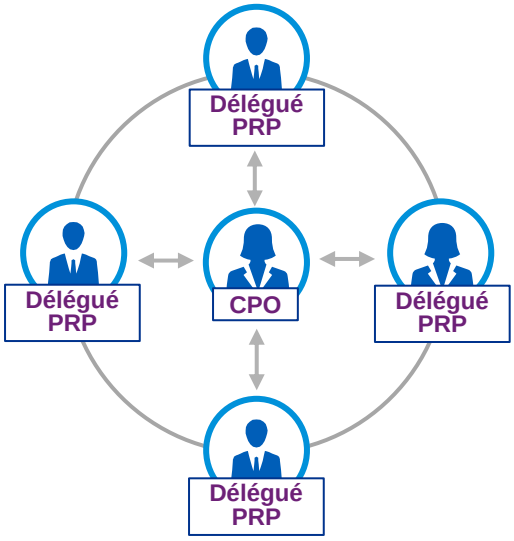
- Rôles et responsabilités
- Politiques, processus, solutions
- Évaluation d'impacts
- Collecte
- Confidentialité par défaut
- Consentement
- Communication à des tiers
- IA – Décision automatisée
- Portabilité
- Conservation, anonymisation, destruction
- Gestion et notification des incidents

Rôles et responsabilités

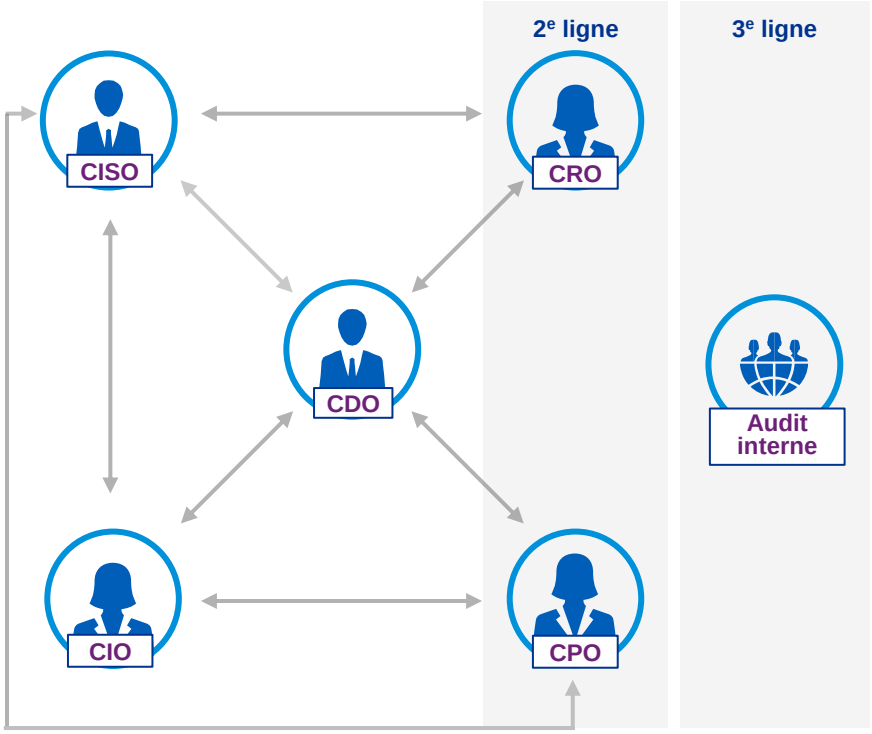
La gestion des risques relatifs à la PRP implique une prise en charge structurée par l'ensemble des organisations. Plus que jamais, les responsabilités et rôles relatifs à la gestion des RP doivent être développés, éclaircis, communiqués et compris.

Thèmes de conformité	Requis
Gouvernance **Rôles et responsabilités** **2022** **Fonctions - Intervenants** Haute direction Conseil d'administration Ressources humaines Art.3.1 LPRPSP Art. 8, 8.1 LADOPPRP[1]	→ **Désigner un responsable de la PRP (*Chief Privacy Officer* « CPO »)** → **Définir le modèle de délégation des responsabilités dans les secteurs d'activité et unités administratives** → **Définir les besoins et réaliser le processus de dotation** → **Définir, attribuer et documenter les rôles et responsabilités en lien avec l'opérationnalisation du programme de PRP** → **Définir une matrice d'assignation des responsabilités (de type RACI, « *Responsible, Accountable, Consulted, Informed* ») qui soit adaptée à la réalité de l'organisation afin d'arrimer les rôles et responsabilités du CPO avec ceux des autres dirigeants impliqués dans la gouvernance et la gestion des données (CISO, CIO, CDO, CRO) et l'audit interne selon le modèle des trois lignes de défense**

Modèle de délégation des responsabilités en matière de PRP



Relations entre les intervenants

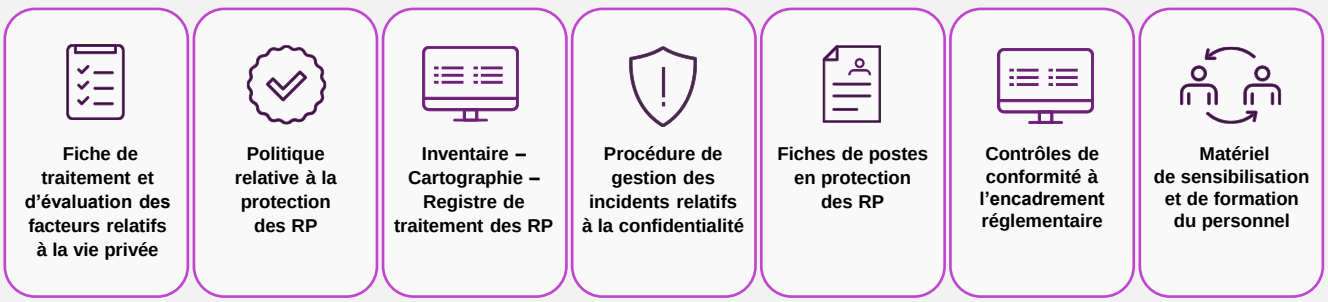


[1] L'obligation de désigner un responsable de l'accès aux documents existait avant la Loi.

Politiques, processus et solutions

Les obligations en matière de protection des RP nécessitent des organisations qu'elles documentent leurs pratiques, qu'elles fassent preuve de transparence à leur égard et qu'elles soutiennent l'exercice des droits des individus. Afin de supporter les activités de leur programme de PRP, les organisations devront considérer des solutions technologiques.

Thèmes de conformité	Requis
Gouvernance **Politiques, processus et solutions** **2023** **Fonctions - Intervenants** PRP Services juridiques Sécurité TI Communication	→ **Définir et opérationnaliser des politiques, pratiques et registres relativement aux éléments suivants :** ○ les rôles et les responsabilités des intervenants de l'organisation; ○ la collecte et le traitement des RP; ○ la conservation et la destruction des RP; ○ le traitement des plaintes; ○ les contrôles et les mesures de sécurité en place pour garantir la confidentialité (lorsque les RP sont recueillis par un moyen technologique); ○ la détection et la gestion des incidents de sécurité; ○ le registre des incidents de sécurité et les déclarations/avis; ○ les méthodes de dépersonnalisation et d'anonymisation. → **Publier sur le site Internet, de façon claire, précise et transparente, l'information relative aux politiques et des pratiques qui portent sur :** ○ la collecte et le traitement des RP; ○ la conservation et la destruction des RP; ○ les rôles et les responsabilités des intervenants de l'organisation; ○ le traitement des plaintes; ○ les contrôles et les mesures de sécurité en place pour garantir la confidentialité (lorsque les RP sont recueillis par un moyen technologique). → **Élaborer et opérationnaliser des processus internes efficaces afin de répondre aux demandes** : ○ d'information (RP recueillis, personnes y ayant accès, durée de conservation, coordonnées du responsable); ○ d'accès et de modification relativement aux RP recueillis; ○ de cessation de diffusion ou de désindexation; ○ d'explication des mécanismes de traitement automatisé; ○ de traitement des données biométriques; ○ de portabilité; ○ de retrait du consentement.
Art. 3.2, 8, 8.2, 12.1 LPRPSP Art. 63.3, 63.4, 65, 84 LADOPPRP	→ Définir les **exigences fonctionnelles**, procéder aux **choix et déployer des solutions en fonction de l'architecture technologique en place.**



Évaluation des impacts

La Loi formalise la bonne pratique qui consiste à évaluer les répercussions qu'on les projets qui impliquent le traitement de RP sur la vie privée. Ces évaluations permettent d'identifier les zones de risque puis d'y remédier alors que le projet à l'étude est encore en développement, diminuant ainsi les risques lorsque le projet voit le jour.

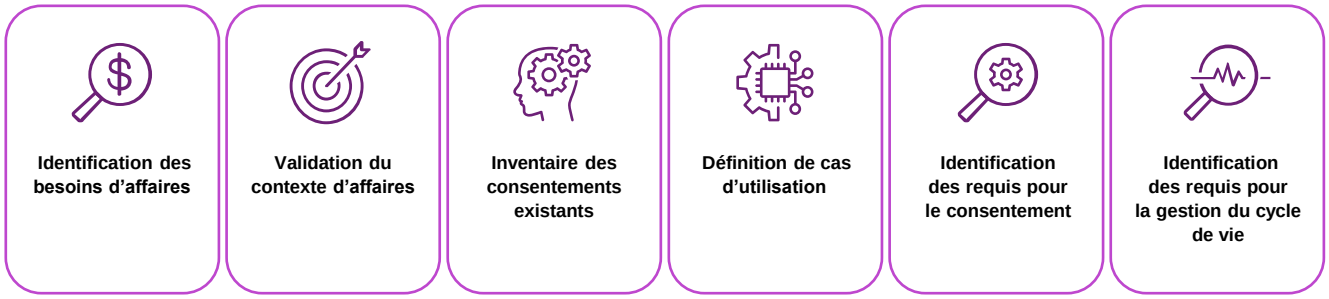
Thèmes de conformité	Requis
Évaluation des facteurs relatifs à la vie privée « EFVP » **2023** **Fonctions - Intervenants** PRP Affaires - Bureau de projet Gouvernance des données Développement de solutions Approvisionnement TI Art. 3.3 - 3.4, et 17 LPRPSP Art. 63.5, 70.1 LADOPPRP	→ Concevoir et déployer un processus d'analyse d'impact (EFVP dans la terminologie de la Loi) applicable à : ○ tout projet d'acquisition, de développement ou de refonte d'un système d'information ou de prestation électronique de services impliquant le traitement de RP; ○ la communication de RP à des tiers, aux fins de recherche; ○ la communication de RP à l'extérieur du Québec (*voir la section concernant la communication à des fournisseur et les solutions infonuagiques ci-dessous*). → Identifier les processus de gestion de projets et les catégories de projets visés, tels que : ○ Implantation d'un progiciel de gestion intégré (PGI) ou d'un HCM/ER comme *SAP-Success Factors et Workday;* ○ Implantation d'un CRM; ○ Acquisition d'une solution infonuagique (*cloud*) de recrutement de personnel ou de soutien client nécessitant le stockage de données clients ou la présence d'employés à l'extérieur du Québec; ○ Développement d'une API donnant accès à des données clients; ○ Déploiement d'une application mobile permettant l'accès au compte client. → Identifier et définir une grille d'évaluation des risques et les contrôles requis en regard des risques identifiés. → Définir les exigences fonctionnelles, procéder aux **choix et déployer des solutions technologiques afin de supporter les activités d'analyse d'impact.**

Consentement

Le renforcement de la conformité en PRP requiert que les entreprises identifient les requis applicables aux processus de sollicitation et de gestion des consentements, afin d'en assurer la conformité et de les intégrer dans leur stratégie et leurs processus d'affaires.

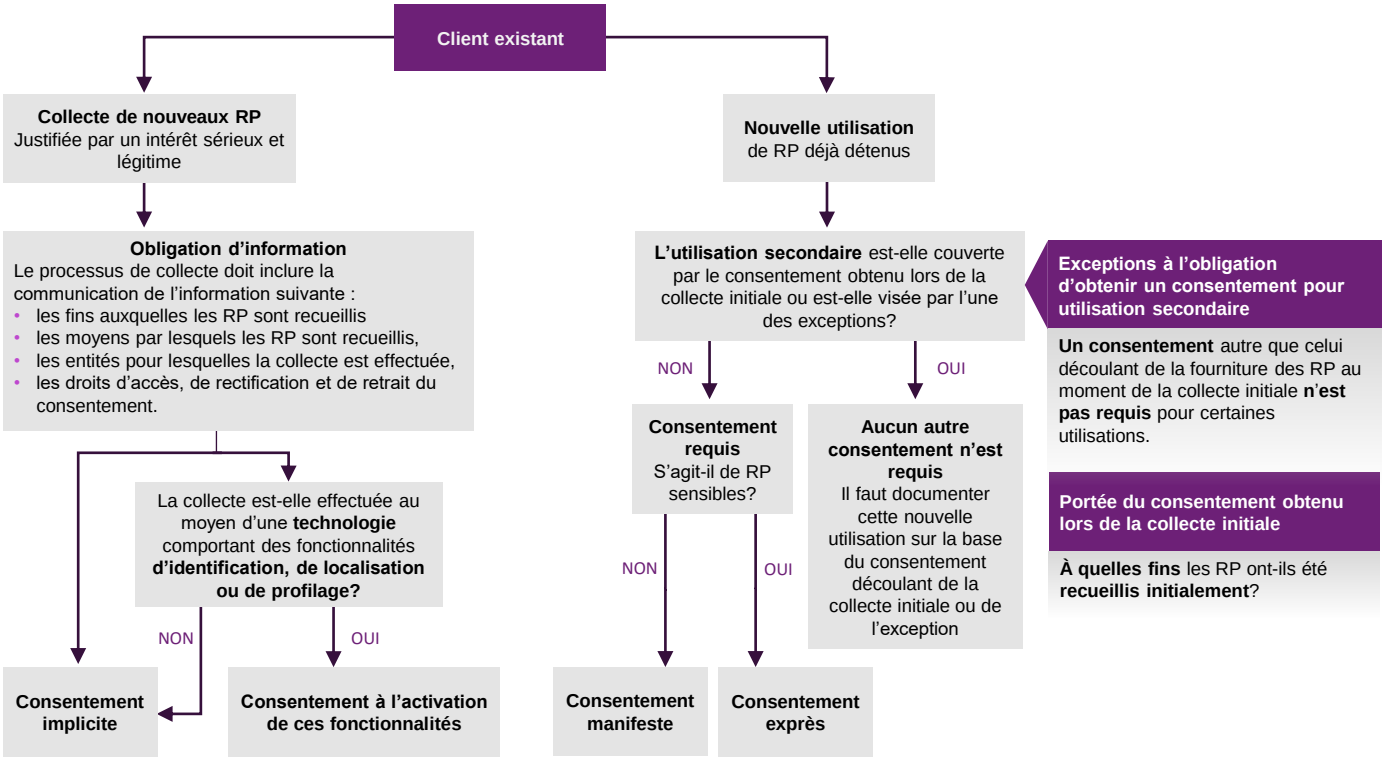
Les organisations doivent identifier les requis de conformité de la PRP sur la base des besoins d'affaires, des entités impliquées, des activités de traitement, des personnes visées, du contexte et du type de RP.

Approche de détermination des requis pour le consentement :



Nous recommandons de compléter l'identification des requis de conformité PRP par la réalisation d'aiguilleurs afin d'appuyer les secteurs dans la définition de leurs stratégies de sollicitation et de gestion des consentements.

Exemple d'aiguilleur pour appuyer les secteurs d'affaires :



Consentement

Les exigences et exceptions au consentement

- **Collecte** - Un processus **transparent** comportant la communication de l'information prescrite (fins, moyens, tiers destinataires, droits de la personne) implique un **consentement implicite** à l'utilisation et la communication des RP aux fins sérieuses et légitimes indiquées au moment de la collecte.
- **Fins secondaires -** Un **consentement** autre que celui découlant de la fourniture des RP au moment de la collecte initiale **est requis** pour des utilisations autres que les fins sérieuses et légitimes indiquées au moment de la collecte initiale ou qui sont couvertes par l'une des exceptions prévues par la loi
- **Exceptions -** Un **consentement** autre que celui découlant de la fourniture des RP au moment de collecte initiale **n'est pas requis** pour d'autres utilisations qui sont :
    - compatibles avec celles pour lesquelles il a été recueilli;
    - manifestement à l'avantage de la personne concernée;
    - nécessaires à des fins de prévention et de détection de la fraude ou d'évaluation et d'amélioration des mesures de protection et de sécurité;
    - nécessaires à la fourniture d'un produit ou à la prestation d'un service demandé par la personne concernée;
    - nécessaires à des fins d'étude, de recherche ou de production de statistiques, et que les RP sont dépersonnalisés.

Thèmes de conformité	Requis
Consentement **2023** **Fonctions – Intervenants** PRP Expérience client Affaires – Bureau de projet Gouvernance des données Développement de solutions TI Art. 12, 14 LPRPSP Art. 53,1 LADOPPRP	→ Identifier les utilisations i) pour lesquelles l'organisation dispose déjà du consentement, ii) qui constituent des utilisations secondaires visées par une exception (art. 12), iii) qui requièrent un consentement supplémentaire. → Analyser les parcours clients et les canaux de communication afin de cibler les occasions de sollicitation de consentements. → Réviser les interfaces utilisateurs, outils, solutions et scénarios de collecte de consentement afin d'assurer : ○ la sollicitation du consentement de façon transparente, à des fins spécifiques et distinctement de toute autre information; ○ la journalisation ou la documentation du consentement; ○ la capacité de recevoir et de traiter des avis de retrait de consentement. → Mettre en œuvre les processus et solutions requises pour consolider les consentements recueillis de différentes sources et assurer la comptabilisation des consentements pour toute utilisation secondaire des RP. → Définir les exigences fonctionnelles et procéder aux **choix des solutions en fonction de l'architecture technologique en place.** → Planifier le déclencheur du mécanisme/processus de renouvellement du consentement. → Établir un mécanisme visant à solliciter et à obtenir le consentement **explicite** pour l'utilisation d'un **renseignement personnel sensibles.** → Définir des méthodes de **dépersonnalisation** des RP aux fins de **recherche** ou de production de **statistiques**

Collecte

Un processus **transparent** comportant la communication des informations prescrites (fins, moyens, tiers destinataires, droits de la personne) implique un **consentement implicite** à l'utilisation et à la communication des RP aux fins sérieuses et légitimes indiquées au moment de la collecte.

Thèmes de conformité	Requis
Notification au moment de la collecte **2023** **Fonctions – Intervenants** PRP Affaires Expérience client TI Art. 4, 8, 8.3 LPRPSP Art. 65 LADOPPRP	→ Inventorier les **processus impliquant la collecte de RP et identifier les données et métadonnées saisies** afin de valider : ○ les RP effectivement recueillis; ○ les fins pour lesquelles les RP sont recueillis (intérêts sérieux et légitimes); ○ les RP qui sont nécessaires à ces fins; ○ les RP dont la collecte est recherchée à des fins secondaires. → Revoir les **avis et communications** afin d'intégrer les mentions : ○ des fins auxquelles ces renseignements sont recueillis; ○ des moyens par lesquels les renseignements sont recueillis; ○ des droits d'accès et de rectification prévus par la loi; ○ de son droit de retirer son consentement à la communication ou à l'utilisation des renseignements recueillis; ○ des catégories de tiers à qui les RP seront communiqués et la possibilité de communication à l'extérieur du Québec le cas échéant. → Mettre en place des **mesures de contrôle d'accès** afin de restreindre l'accès, l'utilisation et la communication des RP aux fins énoncées, ainsi que des mécanismes de surveillance. → Mettre en œuvre des procédures organisationnelles, dont un **registre de traitement** ou une **cartographie des flux de données,** afin de : ○ permettre l'exercice des droits d'accès, de rectification, de retrait du consentement; ○ répondre aux demandes d'information. → Documenter les activités de collecte.

Fonctions d'identification, de localisation et de profilage

La collecte de RP effectuée à l'aide de technologies comportant des fonctions d'identification, de localisation et de profilage s'accompagne de conditions supplémentaires : la confidentialité par défaut (impliquant que ces fonctions doivent être activées par la personne elle-même) et une obligation d'information.

Le profilage 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.

Thèmes de conformité	Requis
Collecte impliquant identification – localisation – profilage **2023** **Fonctions – Intervenants** PRP Affaires – Bureau de projet Gouvernance des données Développement de solutions TI Art. 8.1 LPRPSP Art. 65.0.1 LADOPPRP	Dans les cas d'une collecte qui implique des fonctionnalités d'identification, de localisation ou de profilage : ○ les **fonctionnalités doivent être désactivées par défaut** sans nécessité d'intervention de la part de l'utilisateur; ○ les avis et notifications relatifs à la collecte doivent dénoncer le recours à ces fonctionnalités et à la façon de les activer. → Cette exigence s'applique notamment aux fonctionnalités des sites, applications et témoins ou traceurs de navigation, de marketing comportemental et de localisation. → Revoir les configurations par défaut des systèmes, applications et interfaces utilisateurs visées, dont la collecte des identifiants d'équipements et d'appareils. → Analyser les parcours clients et canaux de communication afin de cibler les occasions de demande d'activation de ces fonctionnalités. → Modifier les interfaces utilisateurs pour intégrer les avis et demandes. → Intégrer et activer des fonctionnalités de journalisation pour confirmer l'activation de fonctionnalités.

Confidentialité par défaut

L'obligation de confidentialité par défaut est une nouveauté importante de la Loi. Elle impose que tout produit ou service technologique soit configuré par défaut de façon à restreindre le traitement de renseignements personnels : il reviendra à l'utilisateur d'activer volontairement les fonctionnalités supplémentaires.

Thèmes de conformité	Requis
Collecte par l'entremise d'un produit ou service technologique **2023** **Fonctions – Intervenants** PRP Affaires – Bureau de projet Gouvernance des données Développement de solutions Approvisionnement TI Art. 9.1 LPRPSP Art. 63.6.1 LADOPPRP	→ Inventorier les produits/services/solutions technologiques qui impliquent la collecte de RP du public : ○ Applications mobiles et sites Internet, incluant les fonctionnalités et témoins ou traceurs de navigation, de marketing comportemental; ○ Plateforme de communication technologique; ○ Solutions impliquant des accès aux identifiants d'équipement et d'appareils. → Revoir les configurations par défaut de chacun afin d'assurer **le plus haut niveau de confidentialité**, sans aucune intervention. → Les paramètres offrant un choix aux utilisateurs doivent être désactivés : ○ L'activation est offerte à l'utilisateur seulement. → Laisser le libre choix à l'utilisateur de configurer ses paramètres de confidentialité en activant, par sa volonté, les fonctionnalités qui recueillent les RP. → Intégrer le principe de minimisation de la collecte de données et les exigences de confidentialité par défaut dans les processus de conception et de développement des systèmes et des applications. → Analyser les parcours clients et les canaux de communication afin de cibler les occasions de demande d'activation de ces fonctionnalités. → Modifier les interfaces utilisateurs pour intégrer les notifications et demandes. → Intégrer et activer des fonctionnalités de journalisation des confirmations d'activation de fonctionnalités. **Exclusions** : ○ les paramètres de confidentialité d'un témoin de connexion sont expressément exclus; ○ La portée de l'exigence réfère à l'offre d'un produit ou d'un service « au public » et ne s'applique donc pas aux solutions déployées en milieu de travail – *il est toutefois important de noter que les exigences relatives aux fonctionnalités de profilage et de géolocalisation mentionnées précédemment s'appliquent quant à elles en milieu de travail.*

Recours à des fournisseurs

Une organisation demeure responsable des renseignements personnels qui lui sont confiés, y compris lorsqu'elle fait affaires avec des fournisseurs dans le cadre de ses activités. C'est donc dire l'importance de bien gérer ces relations contractuelles. En outre, la Loi encadre précisément la communication de RP à l'extérieur du Québec.

Thèmes de conformité	Requis
Communication à des fournisseurs / prestataires de solutions infonuagiques Transfert hors Québec **2023** **Fonctions – Intervenants** PRP Approvisionnement Gestion des risques Gouvernance des données TI – Affaires Services juridiques Art. 17, 18. 3 LPRPSP Art. 67.2, 70.1 LADOPPRP	→ Revoir les processus d'approvisionnement et de gestion des risques applicables aux fournisseurs de services afin d'identifier : ○ Les projets impliquant l'accès aux RP ou leur communication à des fournisseurs de services, par exemple dans le cadre de conversion/migration de données ou d'intégration de systèmes d'information; ○ Les projets de migration vers des solutions infonuagiques (SAAS, PAAS, IAAS); ○ Identifier les projets impliquant le transfert de RP (accès, stockage, hébergement) à l'extérieur du Québec. → Revoir les encadrements contractuels minimaux relativement à la PRP (listes de vérification des exigences minimales, clauses standards, consentement au traitement des données), afin de couvrir : ○ les limites quant au traitement et à la conservation des RP par le fournisseur; ○ les mesures de sécurité appliquées; ○ la notification d'incidents de confidentialité; ○ un mécanisme de contrôle/vérification. → Lorsque le projet implique la **communication / le transfert de RP à l'extérieur du Québec** : ○ évaluer le territoire ou les pays; ○ déterminer la sensibilité des RP et leur utilisation; ○ adopter un positionnement d'entreprise sur les juridictions adéquates; ○ réaliser une analyse d'impact (EFVP dans la terminologie de la Loi) afin de déterminer si les RP bénéficieraient d'une protection adéquate à l'endroit où ils sont transférés et hébergés. → En cas de risque, convenir de **mesures de mitigation** : ○ techniques : cryptage ou dépersonnalisation des RP; ○ organisationnelles : restriction au partage avec les autorités étrangères.

IA - Décision automatisée

Nouvel aspect de la protection des renseignements personnels, l'encadrement relatif à la prise de décisions automatisées à l'égard d'une personne nécessite une connaissance détaillée de ses processus décisionnels par l'organisation, de même qu'une transparence et des garanties procédurales visant la protection des personnes.

Thèmes de conformité	Requis
Décision automatisée **Intelligence artificielle** **2023** **Fonctions – Intervenants** PRP Affaires – Bureau de projet Gouvernance des données Développement de solutions Approvisionnement TI Art. 12.1 LPRPSP Art. 65.2 LADOPPRP	→ Répertorier les processus impliquant le traitement automatisé de RP aux fins d'une prise de décision à l'égard des employés ou des clients, par exemple : ○ L'accessibilité des clients à des produits, services ou avantages sur la base de leur situation financière, d'un profil de risque ou de leur état de santé; ○ L'admissibilité de candidats à des emplois ou d'employés à des promotions; ○ L'admissibilité à des privilèges en raison d'un statut, d'un profil de compétence ou d'un profil de risque. → Revoir les configurations des systèmes, applications et interfaces utilisateurs afin de s'assurer d'informer toute personne concernée du traitement automatisé et des RP utilisés. Par exemple, si le traitement découle d'un formulaire, celui-ci devra être révisé afin de permettre à la personne : ○ de savoir, avant ou au moment de la décision, que la décision est le résultat d'un traitement automatisé; ○ de connaître les RP qui sont utilisés pour rendre la décision; ○ d'être informée des raisons, des facteurs et des paramètres ayant mené à la décision; ○ de faire rectifier les RP ayant mené à la décision; ○ de faire réviser la décision par quelqu'un ayant le pouvoir de la modifier.

Conservation, destruction, anonymisation

La période de conservation des RP doit être restreinte à la durée requise pour les fins identifiées et à la durée de conservation applicable. Il est possible d'anonymiser les RP à la fin de leur période de conservation, afin de pouvoir continuer à en tirer de la valeur. Cette pratique doit être bien encadrée.

Thèmes de conformité	Requis
Conservation / Destruction / Anonymisation / décommissionnement de système **2023** **Fonctions – Intervenants** PRP Gouvernance des données TI Art. 23 LPRPSP Art. 73 LADOPPRP	→ Élaborer et mettre en œuvre un calendrier de conservation des RP (p. ex. : exigences précises pour chaque type de RP). → Mettre en place un mécanisme de destruction automatisé ou systématique des RP en fonction des exigences de conservation. → Définir des seuils de risque de réidentification cibles. → Prévoir des mécanismes/méthodes d'anonymisation des RP en fonction des seuils définis. → Identifier, pour chacun des RP visés les besoins d'affaires reflétant un intérêt sérieux et légitime donnant ouverture à l'anonymisation. → Établir une procédure de sursis en cas de litige soulevant une obligation de préservation.

Portabilité

Le droit à la portabilité des données est le plus récent droit accordé aux individus relativement aux données recueillies par une organisation à son sujet. Les organisations devront s'appuyer sur une connaissance approfondie des processus de collecte et des capacités de traçabilité des données détenues.

Thèmes de conformité	Requis
Portabilité **2024** **Fonctions – Intervenants** PRP Gouvernance des données Expérience client TI Art. 27 LPRPSP Art. 84 LADOPPRP	→ Valider la capacité **d'identification des RP recueillis auprès de la personne** (par rapport aux RP générés ou inférés). → Mettre en œuvre une **capacité de traçabilité des données** afin **de cartographier les flux de données.** → Définir les exigences fonctionnelles, procéder aux **choix et déployer des solutions technologiques aux fins d'assurer la traçabilité et le traitement des demandes.** → Développer un ou des **API pour automatiser le processus** de transmission et de réception de demande de communication. → Assurer **l'interopérabilité des solutions déployées** avec les normes du secteur en voie de développement. → Revoir les processus de conversion et d'accueil des clients (*onboarding*) afin **d'intégrer les fonctionnalités de portabilité dans les parcours clients.**

Gestion et notification des incidents

La gestion des incidents est cruciale à la protection des RP. L'aspect potentiellement public des incidents et leurs répercussions sur les personnes et l'organisation exigent des capacités de détection, de traitement et de suivi. Des processus clairs, la formation des employés, la mise en place d'une cellule de crise et des exercices périodiques sont des composantes importantes de la gestion des incidents.

Thèmes de conformité	Requis
Incident de confidentialité **2022** **Fonctions – Intervenants** PRP Sécurité Services juridiques Communication TI Finance	→ Mettre en place un **processus de gestion des incidents de confidentialité** et des atteintes à la vie privée, puis documenter le processus dans un plan (le « plan ») ○ La portée du plan doit inclure : l'accès, l'utilisation, la perte ou la communication non autorisée d'un renseignement personnel **ou toute autre atteinte à la protection d'un tel RP**, comme : ▪ la transmission de fichiers joints à des destinataires erronés; ▪ l'utilisation non autorisée d'identifiants compromis; ▪ la perte de support/de média; ▪ l'accès non autorisé en contexte de télétravail; ▪ les intrusions réseaux; ▪ l'exfiltration de données par attaquants externes ou internes; ▪ les attaques de type rançongiciel. ○ Identifier les intervenants concernés : ▪ membres de la direction; ▪ conseiller juridique; ▪ conseil d'administration. ○ Établir une grille de leurs rôles et responsabilités (RACI) et un processus de soumission à un niveau supérieur pour : ▪ gérer l'investigation et la résolution de l'incident; ▪ gérer les communications internes et externes; ▪ évaluer les risques de préjudice découlant de l'incident; ▪ déterminer un processus de notifications (qui, quand, comment) afin d'informer les personnes suivantes lors d'une violation : • la Commission d'accès à l'information (CAI); • les personnes concernées par l'incident de sécurité; • les tiers concernés, dont les clients qui sont responsables du traitement des RP. → Le plan comprend un moins un arbre ou un critère décisionnel afin d'établir les orientations en matière **de communications internes et publiques.** → Créer et déployer une **formation obligatoire pour les employés** au moment de l'embauche, redonnée annuellement (p. ex. : analyse d'impact, détection et gestion d'incidents, application des procédures organisationnelles). → Procéder annuellement à **des simulations d'incidents relatifs à la confidentialité** afin de tester et de renforcer les capacités de réponse, la gestion sur la base de scénarios et la séquence d'injection correspondant aux scénarios de risques. → Intégrer à la politique de confidentialité des exigences relatives aux processus de notifications de violation incluant les informations pertinentes sur la PRP. → Mettre en place et maintenir un registre d'incidents relatifs à la confidentialité.

Art. 3.5 et 3.8 LPRPSP
Art. 63.3 LADOPPRP

SANCTIONS

Les manquements ou violations aux obligations prévues par la loi seront désormais assujettis à des sanctions importantes de nature administrative ou pénale.

Nous anticipons que la Commission d'accès à l'information adoptera une approche proactive comme ce fut le cas lors de l'entrée en vigueur du RGPD. Les écarts de conformité sont susceptibles d'entraîner des conséquences monétaires importantes, la divulgation de renseignements sensibles des clients, la perte de confiance de la clientèle et un risque dévastateur d'atteinte à la réputation.

Infractions	Manquements	Sanctions maximales
Administratives* Art. 90.1 et ss LPRPSP	→ Omet de déclarer un incident de confidentialité. → Recueille, utilise, communique, conserve ou détruit des renseignements en contravention à la loi. → Ne prend pas les mesures de sécurité nécessaires pour protéger les RP. → Omet de satisfaire aux exigences requises concernant les décisions automatisées. → L'action d'une tierce partie. → Ne satisfait pas à ses obligations en matière de transparence.	**Personne physique** : 50 000 $ **Personne morale** : 10 000 000 $, ou 2 % du chiffre d'affaires Prescription : **2 ans** à compter de la date du manquement
Pénales Art. 91, 92 et ss LPRPSP Art. 158-159 LADOPPRP	→ Omet de déclarer un incident de confidentialité. → Recueille, utilise, communique, conserve ou détruit des renseignements en contravention à la loi. → Ne prend pas les mesures de sécurité nécessaires pour protéger les RP. → Demande à un autre agent d'évaluation de crédit des RP après avoir été avisé d'un gel de sécurité. → Tente de procéder à la réidentification d'une personne à partir de renseignements dépersonnalisés ou anonymisés sans l'autorisation des personnes qui les détiennent. → Entrave le déroulement d'une enquête ou d'une inspection de la Commission d'accès à l'information du Québec (CAI). → Menace un individu de représailles pour avoir déposé une plainte ou collaboré avec la CAI. → Contrevient à une ordonnance de la CAI. → Néglige de produire les documents demandés dans les délais fixés par la CAI.	**Personne physique** : 100 000 $ **Personne morale** : 25 000 000 $, ou 4 % du chiffre d'affaires (la plus élevée des deux situations) Récidive : sanctions doublées Prescription : **5 ans** suivant l'infraction

*Les infractions administratives s'appliquent aux organisations du secteur privé.

Cadre de gestion de la protection des RP – Vue détaillée

Gouvernance et modèle opérationnel

- Modèle de gouvernance et d'opérations
- Matrice des rôles et responsabilités – arrimage avec les autres responsables de la donnée
- Services juridiques en appui à la PRP
- Habilitation technologique
- Expérience client

Politiques, avis et consentement

- Politique de PRP interne
- Politique de PRP externe
- Cadre stratégique et gestion du changement
- Avis et consentement
- Consentement des mineurs

Cartographie des données

- Cartographie et flux des données

Formation et sensibilisation

- Formation
- Sensibilisation

Risques, contrôles et surveillance

- Risques et contrôles
- Surveillance des contrôles de sécurité et PRP
- Assurance indépendante

Processus, procédures et technologies

- Protection de la vie privée dès la conception (*Privacy by Design* ou *PbD*)
- Communications transfrontières
- Droits des individus
- Gestions des plaintes
- Requêtes d'agences externes

Gestion de la réglementation

- Veille réglementaire
- Relations avec les organismes de réglementation
- Dépôts réglementaires

Sécurité pour la protection des données

- Sécurité pour la protection des données
- Pseudonymisation and anonymisation
- Chiffrement des données

Gestion du cycle de vie de l'information

- Collecte et minimalisation des données
- Classification des données
- Exactitude des données
- Conservation des données
- Destruction des données

Stratégie des données

- Stratégie des données et feuille de route
- Acquisition de données
- Partage de données
- Marketing
- IA, profilage et prise de décision automatisée
- Utilisation éthique des données

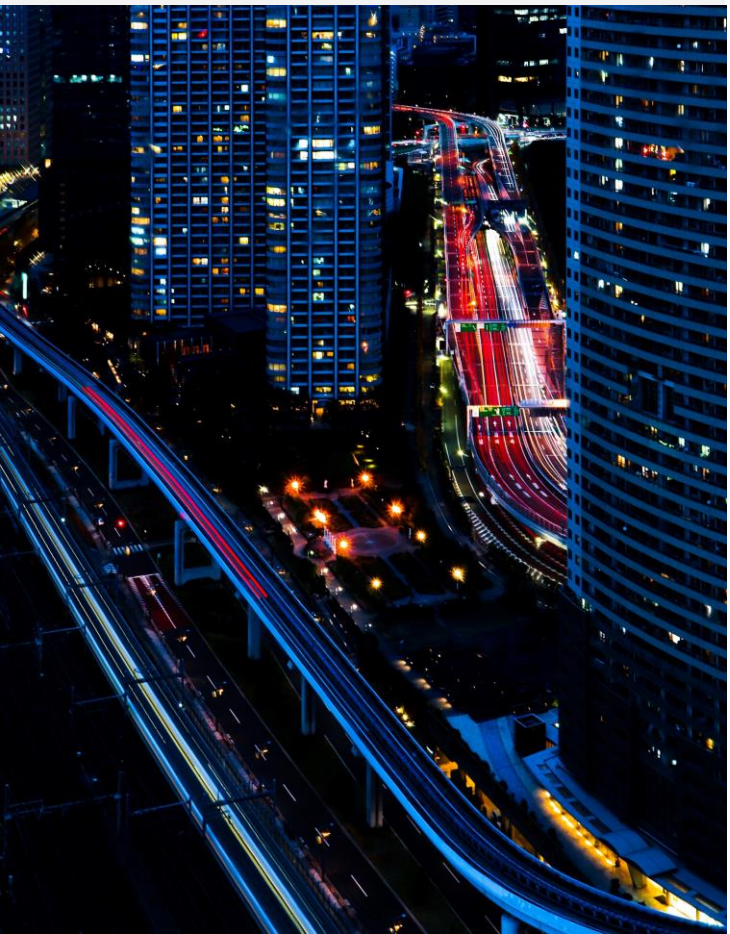
Gestion des tiers

- Diligence raisonnable
- Entente de partage de données
- Contrats avec les tiers
- Assurance des tiers
- Fusions et acquisitions

Gestion des incidents

- Gestion des incidents de confidentialité
- Enquêtes et gestion de la preuve
- Processus de déclaration et de notification d'incident

Questions que se posent les organisations des secteurs privé et public



Ai-je une vision claire des renseignements personnels qui sont recueillis et traités pour mon organisation ou au sein de celle-ci?

Où, quand, par qui et dans quel but ces RP sont-ils obtenus?

Où ces RP sont-ils conservés et pour combien de temps?

Ai-je confiance en la capacité de mon organisation à détecter et à gérer efficacement un incident de confidentialité?

Est-ce que nous validons et contrôlons la conformité des fournisseurs en matière de confidentialité et de sécurité?

Quel sera l'effet de l'entrée en vigueur des nouvelles exigences sur les activités de notre entreprise?

Quels sont les risques de non-conformité actuels de mon organisation?

Pourquoi KPMG?

Un leader canadien en matière de protection des renseignements personnels et en gestion des données.

KPMG a réalisé de nombreux projets en matière de protection des renseignements personnels, de gouvernance et de gestion des données dans plusieurs secteurs d'activité.

Nous reconnaissons les défis découlant de l'entrée en vigueur de la Loi et disposons de l'expérience et des ressources requises pour vous aider dans l'identification des écarts et des lacunes de votre situation actuelle, et pour mener à bien votre projet de mise en conformité.

« Nous nous démarquons par notre approche fondée sur le respect de la vie privée "dès la conception et par défaut", qui vise à intégrer et à automatiser les principes de la PRP dans le cadre de l'élaboration et du développement de processus, de produits ou de services qui nécessitent le traitement de renseignements personnels. »

JEAN-FRANÇOIS DE RICO

Associé, Services-conseils KPMG

Vie privée – Gestion des risques technologiques – Cybersécurité

Aide-mémoire

Septembre 2022

- Responsable de la protection de la vie privée
- Tiers (transactions commerciale et recherche)
- Incidents de confidentialité
- Biométrie
- Protection des dénonciateurs
- Obligation de coopérer avec la CAI

Septembre 2023

- Politiques et procédures
- Évaluation des facteurs relatifs à la vie privée (ÉFVP)
- Confidentialité par défaut
- Dépersonnalisation
- Anonymisation
- Tiers et transferts hors du Québec
- Avis de confidentialité
- Transparence (en général)
- Consentement
- Limitation de la finalité
- Limitation de la collecte
- Conservation et destruction
- Effacement
- Prise de décision automatisée et profilage

Septembre 2024

- Portabilité

C’est l’occasion de reprendre le contrôle sur vos données et de valoriser cet actif stratégique.

L’approche KPMG

Une approche holistique et pragmatique qui s’appuie sur des compétences complémentaires et sur la collaboration des professionnels de la donnée :

- **Cybersécurité**
- **Protection des renseignements personnels**
- **Gouvernance et gestion des données**
- **Automatisation**
- **Gestion documentaire**
- **Transformation numérique**
- **Gestion des identités et des accès**
- **Expérience client**
- **Gestion du changement**

Nous privilégions une approche holistique qui s'appuie sur les expériences complémentaires et la collaboration éprouvée de nos professionnels

Notre équipe est composée de professionnels chevronnés œuvrant dans des domaines complémentaires. Ils ont à cœur de produire du travail de grande qualité. Ils ont fréquemment l'occasion de travailler ensemble, et de faire bénéficier nos clients d'une approche multidisciplinaire et de solutions mûrement réfléchies.

Si la dimension internationale d'un sujet le requiert, KPMG peut vous faire profiter de son réseau international de professionnels de la vie privée.

Notre équipe

Protection de la vie privée

Jean-François De Rico
Associé responsable,
Protection de la vie privée
KPMG au Canada
jderico@kpmg.ca
418 577-3442

François Senécal
Directeur principal,
Protection de la vie privée
KPMG au Canada

Raphaël Jauvin
Directeur principal,
Protection de la vie privée
KPMG au Canada

Abigail Dubiniecki
Directrice,
Protection de la vie privée
KPMG au Canada

Virginie Bernier
Conseillère principale,
Protection de la vie privée
KPMG au Canada

Jean-Luc Nicholson
Conseiller principal,
Protection de la vie privée
KPMG au Canada

Camélia Jamali
Conseillère,
Protection de la vie privée
KPMG au Canada

Sylvia Kingsmill
Leader mondiale, Confidentialité informatique
KPMG au Canada

Gouvernance et gestion des données

Catherine Nadeau
Directrice principale,
Gouvernance des données
KPMG au Canada
cnadeau@kpmg.ca
514 840-5350

Emmanuel Thoorens
Directeur principal,
Gouvernance des données
KPMG au Canada

Alexandre Longeval
Directeur,
Gouvernance des données
KPMG au Canada

Cynthia Viau-Mainville
Directrice,
Gestion documentaire
KPMG au Canada

Transformation numérique

Patricia Boisclair
Directrice principale,
Stratégie et transformation numérique
KPMG au Canada

Jenna Yee
Directrice,
Stratégie et transformation numérique
KPMG au Canada

Cybersécurité

Yassir Bellout
Associé,
Cybersécurité
KPMG au Canada

Claudio Francavilla
Directeur principal,
Cybersécurité
KPMG au Canada

Expérience client

Derek Derouin
Directeur principal,
Expérience client
KPMG au Canada

Guillaume Baur
Directeur,
Expérience client
KPMG au Canada

Vincent De Bruille
Consultant,
Expérience client
KPMG au Canada

Gestion du changement

Julie Grenier
Directrice,
Gestion du changement
KPMG au Canada

kpmg.ca/fr