MAI 2024

Document d'orientation du CIPVP : La protection de la vie privée et l'accès à l'information dans les contrats du secteur public avec des fournisseurs de services externes

Information and Privacy Commissioner of Ontario
Commissaire à l'information et à la protection de la vie privée de l'Ontario

Le présent document d'orientation du Bureau du commissaire à l'information et à la protection de la vie privée de l'Ontario (CIPVP) a pour but d'expliquer les droits que confèrent les lois ontariennes sur l'accès à l'information et la protection de la vie privée et les obligations qu'elles imposent, et de favoriser l'adoption de pratiques exemplaires sur le recours aux services de fournisseurs externes. Il ne saurait se substituer à ces lois et il ne contient pas de conseils juridiques. Il ne lie pas le Tribunal du CIPVP, qui peut être appelé à enquêter et à rendre une décision sur une plainte ou un appel en se fondant sur les circonstances et les faits pertinents. Pour obtenir une version à jour du présent guide, visitez **www.ipc.on.ca/fr**.

Remerciements

Le CIPVP a partagé une ébauche du présent document d'orientation avec un certain nombre de parties intéressées en Ontario, notamment :

- le gouvernement provincial;
- des municipalités;
- le secteur de l'éducation;
- les forces de l'ordre;
- le secteur des transports;
- le secteur des jeux et de l'alcool.

Le CIPVP remercie de leurs commentaires judicieux les institutions et les particuliers représentant ces secteurs. Les commentaires et demandes de renseignements concernant le présent document peuvent être adressés à **info-fr@ipc.on.ca**.

Table des matières

Introduction

Les institutions ontariennes font de plus en plus appel à des fournisseurs de services externes pour les aider à s'acquitter de leur mandat légal[1]. Ces fournisseurs traitent souvent des documents et des renseignements personnels qui sont soumis aux lois ontariennes sur l'accès à l'information et la protection de la vie privée.

Les accords d'externalisation peuvent porter à se demander qui a la garde et le contrôle des documents contenant des renseignements personnels, et brouiller ainsi la hiérarchie des responsabilités. Les partenariats public-privé deviennent plus courants, posant de nouveaux risques pour la vie privée et la sécurité qu'il faut gérer de manière concrète et fiable.

Une institution responsable doit tenir compte des facteurs touchant l'accès à l'information et la protection de la vie privée dans ses contrats d'externalisation, et conserver le contrôle des documents et des renseignements personnels, même lorsque des fournisseurs de services externes en ont la garde. Quelle que soit l'entité qui traite des données en leur nom, les institutions publiques de l'Ontario demeurent responsables de protéger les documents et les renseignements personnels dont elles ont le contrôle et de fournir un droit d'accès à ces documents et à ces renseignements.

Au sujet du présent document d'orientation

Le présent document d'orientation énonce les pratiques exemplaires recommandées pour faire preuve de diligence raisonnable et assurer la reddition de comptes en matière de protection de la vie privée et d'accès à l'information lors de la planification et de la conclusion d'accords avec des fournisseurs de services.

Le présent document est destiné aux institutions assujetties à la *Loi sur l'accès à l'information et la protection de la vie privée* (LAIPVP) ou à la *Loi sur l'accès à l'information municipale et à la protection de la vie privée* (LAIMPVP). Toutefois, d'autres organisations du secteur public pourraient également bénéficier de ces pratiques exemplaires et les adapter au besoin.

Les recommandations du présent document ont pour but d'aider les institutions à cerner les aspects relatifs à l'accès à l'information et à la protection de la vie privée lorsqu'elles achètent des services conformément à la LAIPVP et à la LAIMPVP. Cependant, il n'existe pas de solution universelle. Les exigences en matière d'accès à l'information et de protection de la vie privée doivent être évaluées au cas par cas.

---

1 Exemples de services que le gouvernement peut confier à des fournisseurs externes :

- l'exécution d'un programme ou la prestation d'un service pour le compte du gouvernement;
- l'implantation ou la gestion d'une base de données ou d'un système informatique;
- le soutien d'un système;
- les services de reprise en cas de sinistre;
- la prestation de services de consultation ou de recherche;
- l'administration d'un centre d'appels;
- le stockage de documents;
- le déchiquetage ou le recyclage externe de supports de données.

Le présent document porte sur les obligations en matière d'accès à l'information et de protection de la vie privée liées à l'externalisation de services comportant le traitement de documents ou de renseignements personnels. Pour des aspects plus généraux liés à l'approvisionnement, il est recommandé aux institutions de consulter le présent document d'orientation en parallèle avec d'autres exigences qui s'appliquent à elles, comme la **Directive en matière d'approvisionnement dans le secteur parapublic** (en vigueur le 1er avril 2024) du Conseil de gestion du gouvernement de l'Ontario et la directive sur l'approvisionnement pour la fonction publique de l'Ontario (en vigueur le 1er septembre 2023).

Si les contrats sont essentiels pour gérer les risques liés aux tiers, ils ne suffisent pas à eux seuls. Les institutions doivent faire preuve de diligence raisonnable à toutes les étapes de l'approvisionnement. Les recommandations du présent document sont donc structurées en une liste de vérification à cinq volets :

- **Partie 1 : Planification de l'approvisionnement** aspects à prendre en considération au moment de déterminer et d'évaluer les besoins de l'organisation et d'envisager de recourir à un fournisseur de services.
- **Partie 2 : Processus d'appel d'offres** aspects à envisager lors de l'élaboration ou de l'examen de documents d'appel d'offres, tels que des demandes de propositions.
- **Partie 3 : Sélection du fournisseur** aspects touchant l'accès à l'information et la protection de la vie privée dans le cadre des étapes d'évaluation et d'attribution du processus d'approvisionnement.
- **Partie 4 : Accord** aspects dont il faut tenir compte lors de la conclusion d'un accord avec un fournisseur de services.
- **Partie 5 : Gestion et expiration ou résiliation de l'accord** aspects à envisager tout au long de l'accord en ce qui concerne sa gestion, sa surveillance, son application et sa résiliation.

Le présent document d'orientation constituera un point de départ pour les discussions entre le service responsable des documents, le bureau de la protection de la vie privée, les services de l'approvisionnement, le personnel chargé des TI, le personnel responsable de la cybersécurité, les conseillers juridiques et l'équipe de gestion de projets. Il a pour but de fournir aux institutions le soutien nécessaire pour négocier et rédiger des modalités d'accord qui sont conformes aux lois ontariennes sur l'accès à l'information et la protection de la vie privée.

Nous invitons les institutions à adapter ces recommandations à leur situation et à les intégrer dans leurs processus d'approvisionnement.

Principes généraux

- Chaque institution assujettie à la LAIPVP ou à la LAIMPVP doit respecter les règles relatives à l'accès à l'information et à la protection de la vie privée énoncées dans cette loi[2].

2 Pour en savoir davantage sur vos obligations en matière d'accès à l'information et de protection de la vie privée en vertu de la LAIPVP et de la LAIMPVP, adressez-vous au **coordonnateur de l'accès à l'information et de la protection de la vie privée** de votre institution.

- Les institutions peuvent également être assujetties à des directives, accords commerciaux, politiques, normes et lignes directrices qui définissent des exigences supplémentaires liées à la transparence de leurs documents et à la protection des renseignements personnels.
- La LAIPVP et la LAIMPVP n'interdisent pas aux institutions du secteur public et parapublic de l'Ontario d'externaliser le traitement de documents et de renseignements personnels ni de stocker ces renseignements à l'extérieur de l'Ontario ou du Canada.
- Les institutions publiques de l'Ontario sont tenues d'exercer un contrôle réel sur les documents et les renseignements personnels, même lorsque des fournisseurs de services en ont la garde à des fins de traitement[3].
- Les institutions du secteur public et parapublic de l'Ontario qui externalisent le traitement de documents et de renseignements personnels demeurent responsables de respecter les lois ontariennes sur la protection de la vie privée relativement aux documents et renseignements personnels dont elles ont la garde ou le contrôle[4].
- Les fournisseurs de services ne peuvent pas déroger aux règles imposées à l'institution quant au traitement des renseignements personnels. Par exemple, ils ne peuvent pas utiliser des renseignements personnels à des fins secondaires comme le marketing ou l'amélioration des produits[5] sans le consentement indépendant des utilisateurs de leurs services.
- Pour respecter leurs obligations en matière de protection des renseignements personnels aux termes de la LAIPVP ou de la LAIMPVP, les institutions doivent veiller à ce que les fournisseurs de services qui traitent en leur nom des documents et des renseignements personnels respectent des exigences semblables ou équivalentes à celles auxquelles elles sont soumises.
- Il est essentiel de conclure avec les fournisseurs de services des contrats qui les engagent à respecter les obligations de l'institution en matière de protection de la vie privée et d'accès à l'information. Les institutions ne peuvent se soustraire à leurs obligations aux termes de la LAIPVP ou de la LAIMPVP en ne concluant pas d'accords contractuels appropriés avec des fournisseurs de services.
- S'il est nécessaire que les institutions signent des accords contraignants avec leurs fournisseurs de services, cela n'est pas suffisant. Elles doivent aussi recourir à des mesures de surveillance suffisantes pour s'assurer que les fournisseurs respectent les obligations qui leur incombent en vertu de l'accord.
- Les institutions doivent également être transparentes à l'égard des utilisateurs de leurs services quant à leur recours à un fournisseur de services pour recueillir des renseignements personnels en son nom, notamment en améliorant leurs avis de collecte.

---

3 Le bulletin d'interprétation **Garde ou contrôle** du CIPVP, publié en 2023, contient une liste de facteurs qui pourraient être pertinents afin de déterminer qui a la garde ou le contrôle d'un document. Il s'appuie sur le critère à deux volets établi dans l'arrêt ***Canada (Commissaire à l'information) c. Canada (Ministre de la Défense nationale)*, 2011 CSC 25 (CanLII), [2011] 2 RCS 306** de la Cour suprême du Canada et sur des ordonnances antérieures du CIPVP portant sur cette question. Voir également la section 2.3 du présent document, « Documents et renseignements personnels à traiter ».

4 *Ontario Criminal Code Review Board v. Hale*, **1999 CanLII 3805 (ON CA)**, aux paragraphes 32, 36 et 37.

5 L'utilisation de renseignements personnels pour élaborer ou améliorer des services peut être contraire aux fins autorisées. Voir le rapport sur une plainte relative à la protection de la vie privée **PI21-00001**.

Liste de vérification en matière d'accès à l'information et de protection de la vie privée

Partie 1 : Planification de l'approvisionnement

La présente section traite de facteurs pertinents pour déterminer et évaluer les besoins de l'institution et planifier le recours à un fournisseur de services.

Avant de lancer un appel d'offres ou de recourir à un fournisseur de services, les institutions doivent tenir compte de leurs obligations en matière de protection de la vie privée et d'accès à l'information en vertu de la LAIPVP ou de la LAIMPVP et continuer de les respecter. Elles doivent être conscientes du risque pour l'accès à l'information et la protection de la vie privée que pose le fait de communiquer des renseignements personnels dont elles ont la garde à un fournisseur de services à des fins de traitement en leur nom. Avant d'entreprendre un projet ou une initiative d'approvisionnement, les institutions doivent tenir compte des pratiques exemplaires suivantes :

1.1 Planification préliminaire

- Ajouter la présente liste de vérification à leurs documents de planification ou l'intégrer dans ces documents, afin de relever les aspects touchant l'accès à l'information et la protection de la vie privée à envisager aux fins de l'achat de services externes.
- Demander à des experts pertinents, notamment le personnel du bureau de la protection de la vie privée, les avocats, le personnel de la sécurité de l'information et d'autres experts concernant les questions relatives à l'accès à l'information et à la protection de la vie privée que l'initiative ou le projet d'approvisionnement proposé pourrait soulever.
- Confirmer que l'objet du projet ou de l'initiative d'approvisionnement est conforme aux exigences opérationnelles de l'institution.
- Confirmer que la LAIPVP ou la LAIMPVP autorise la collecte, la conservation, l'utilisation ou la divulgation de renseignements personnels proposée dans le cadre de cette initiative.
- Déterminer l'instrument ou l'accord approprié pour régir l'activité d'approvisionnement envisagée et les procédures à suivre.
- Définir clairement les procédures à suivre pour demander, obtenir et documenter les autorisations nécessaires.

1.2 Définir les documents

- Déterminer clairement si le projet ou l'initiative d'approvisionnement concerne des documents et des renseignements personnels que possède l'institution[6].
- Énumérer et décrire les types de documents ou de renseignements personnels qui seront visés par l'accord, ainsi que la personne qui en est responsable.
- Confirmer les exigences des lois, règlements, accords, directives, politiques opérationnelles, normes et autres orientations en matière de protection de la vie privée qui s'appliquent aux documents ou aux renseignements personnels.
- Confirmer que seuls les documents ou renseignements personnels nécessaires et pertinents pour la prestation du service envisagé seront transférés au fournisseur de services. Préciser la quantité minimale à transférer à cette fin.

1.3 Déterminer et atténuer les risques pour la vie privée et la sécurité

- Déterminer les risques pour la vie privée et la sécurité associés au projet ou à l'initiative avant d'entamer la procédure d'approvisionnement ou de conclure un accord, et prendre les mesures qui s'imposent pour les atténuer, notamment en effectuant une évaluation de l'incidence sur la vie privée (EIVP) et, dans les cas pertinents, une évaluation de la menace et des risques (EMR).
- Déterminer si le fournisseur de services retenu devrait soumettre ses services, procédés ou technologies à une EIVP, à une EMR ou à une autre évaluation de sécurité avant de conclure l'accord ou à intervalles établis au cours de l'élaboration du projet ou de la durée du contrat.

1.4 Définir les exigences que doivent respecter les fournisseurs de services

- Définir le travail que doit effectuer le fournisseur de services en ce qui concerne le traitement des documents ou des renseignements personnels dans le cadre du projet ou de l'initiative.
- Établir une hiérarchie claire des responsabilités entre l'institution et le fournisseur de services et définir leurs rôles et responsabilités respectifs.
- Définir des exigences et des interdictions précises en matière d'accès, de protection de la vie privée et de sécurité à imposer au fournisseur de services[7].

---

6 Renseignements personnels sur les employés : si le projet d'externalisation comprend le traitement de renseignements personnels concernant des employés de l'institution, par exemple, dans le cas d'une initiative de ressources humaines, l'institution doit tenir compte des facteurs et prévoir les protections qui s'appliquent aux autres renseignements personnels sensibles dont elle a la garde ou le contrôle. La divulgation ou l'utilisation non autorisée de renseignements sur les employés peut exposer ceux-ci à des risques pour leur sécurité et à des risques financiers, et peut aussi exposer l'institution à des risques pour sa sécurité et à des risques juridiques et financiers.

7 Il est préférable de définir des règles et des responsabilités précises en matière de protection de la vie privée dans votre accord plutôt que d'exiger simplement le respect de la loi. Cela vaut en particulier lorsque la loi ontarienne ne s'applique généralement pas au fournisseur de services. Les fournisseurs ne connaissent peut-être pas les lois ontariennes sur l'accès à l'information et la protection de la vie privée, ou ne comprennent pas comment leurs dispositions peuvent s'appliquer dans le contexte de l'accord. Dans ce cas, il pourrait se révéler nécessaire de définir des exigences précises en matière de protection de la vie privée dans vos accords.

- Établir un processus de contrôle et d'évaluation de la conformité du fournisseur de services aux exigences relatives à l'accès à l'information, à la protection de la vie privée et à la sécurité, notamment en ce qui concerne le respect des obligations contractuelles et des normes de sécurité.
- Définir les qualifications, les titres ou les certifications en matière de protection de la vie privée ou de sécurité que le fournisseur de services ou les sous-traitants doivent posséder avant de fournir le service envisagé.
- Obtenir des renseignements sur les structures de gouvernance du fournisseur de services, par exemple le lieu où il exerce ses activités de traitement des données et ses affiliations avec des entités étrangères, et déterminer si celles-ci soulèvent des conflits juridiques ou constituent d'autres obstacles à la satisfaction de ses obligations contractuelles.

1.5 Établir les méthodes d'évaluation

- Déterminer comment évaluer la capacité du fournisseur de services éventuel à se conformer aux exigences en matière d'accès à l'information, de protection de la vie privée et de sécurité, et les documents à fournir à l'appui de cette évaluation[8].
- Envisager la nécessité d'une visite ou d'une inspection sur place, d'une évaluation préliminaire, d'une certification de conformité ou de tout autre moyen d'évaluer les capacités du fournisseur de services éventuel.

Partie 2 : Appel d'offres

Cette section décrit les aspects pertinents en matière d'accès à l'information, de protection de la vie privée et de sécurité à envisager lors de l'élaboration ou de l'examen de documents d'appel d'offres.

L'institution qui fait appel à un fournisseur de services pour traiter des documents ou des renseignements personnels en son nom doit s'appuyer sur les activités de planification précédentes et définir les responsabilités et les interdictions en matière d'accès à l'information, de protection de la vie privée et de sécurité dans ses documents d'appel d'offres et dans l'accord éventuel. Ces documents doivent définir les règles relatives à la gestion des documents et à la protection des renseignements personnels. En conséquence, les institutions devraient procéder comme suit.

8 Par exemple, montrer qu'a été mis en place un système de gestion de la sécurité de l'information répondant aux normes **ISO 27001**, ou des **rapports sur les contrôles SOC 2 Type II** de l'American Institute of Chartered Public Accountants (AICPA), qui visent à fournir des renseignements détaillés et des précisions sur les contrôles établis dans une organisation de services en matière de sécurité, de disponibilité et d'intégrité de traitement des systèmes que cette organisation utilise pour traiter les données des utilisateurs et assurer la confidentialité des renseignements traités. Ces rapports sont importants pour assurer la surveillance de l'organisation et des programmes de gestion des fournisseurs ainsi que la surveillance réglementaire.

2.1 Cadre législatif

- Préciser les lois sur la protection de la vie privée ou les autres lois pertinentes qui s'appliquent aux activités de traitement du fournisseur de services, et si plusieurs lois s'appliquent, expliquer comment les exigences des lois ontariennes sur la protection de la vie privée seront respectées.

2.2 Exigences en matière de conformité

- Exiger du fournisseur de services qu'il respecte les modalités de l'accord et les lois et règlements applicables en matière de protection de la vie privée et d'accès aux renseignements personnels.
- Exiger du fournisseur de services qu'il traite les documents et renseignements personnels uniquement aux fins énoncées dans l'accord.
- Interdire toute autre activité faisant intervenir des documents et des renseignements personnels sans l'autorisation écrite préalable de l'institution.
- Exiger du fournisseur de services qu'il veille à ce que ses employés, mandataires et autres représentants qui ont accès aux documents ou renseignements personnels respectent les lois applicables et les modalités de l'accord.
- Déterminer s'il y a lieu de vérifier le casier judiciaire des personnes ayant accès aux documents ou aux renseignements personnels et, dans l'affirmative, exiger du fournisseur de services qu'il effectue cette vérification avant de leur accorder l'accès aux documents ou aux renseignements personnels.
- Préciser si le fournisseur de services est autorisé à faire appel à des sous-traitants pour effectuer des travaux liés à l'accord et, dans l'affirmative, lui demander d'identifier ces sous-traitants et de s'assurer qu'ils respectent les mêmes normes que lui ou des normes équivalentes, le cas échéant[9].
- Indiquer les lois qui régissent l'interprétation et l'application de l'accord (p. ex., les lois de l'Ontario) et le tribunal ou l'autre instance devant lesquels les différends en vertu de l'accord seront tranchés (p. ex., la Cour supérieure de justice de l'Ontario).

2.3 Documents et renseignements personnels à traiter

- Définir dans l'accord les termes « document » et « renseignements personnels » afin que toutes les parties à l'accord s'entendent sur leur sens (p. ex., en utilisant les définitions de la LAIPVP ou de la LAIMPVP).
- Décrire les types de documents et de renseignements personnels auxquels le fournisseur de services aura accès et qu'il devra traiter, en s'appuyant sur la section 1.2 du présent document, « Définir les documents ».

9 Si votre fournisseur de services est autorisé à recourir à des sous-traitants, vous devez déterminer les éléments de la liste de vérification qui s'appliquent également aux sous-traitants, et la manière dont les obligations de ces sous-traitants en matière de protection de l'accès et de la vie privée sont définies dans votre accord.

- Préciser les documents et les renseignements personnels dont chaque partie à l'accord a la garde.
- Préciser que l'institution conserve le contrôle des documents et renseignements personnels qu'elle communique au fournisseur de services ou que ce dernier recueille pour son compte en vue de leur traitement.
- Déterminer les activités ou services, le cas échéant, qui doivent recourir uniquement à des données dépersonnalisées ou anonymisées, et définir le sens de ces termes[10].
- Si les activités de traitement nécessitent des renseignements personnels, définir la quantité minimum de renseignements requis pour les accomplir.

2.4 Demandes d'accès à des documents et à des renseignements personnels dont le fournisseur de services a la garde

- Déterminer les représentants de l'institution et du fournisseur de services qui seront désignés responsables des communications relatives aux demandes de documents ou de renseignements personnels dont le fournisseur de services a la garde.
- Préciser l'obligation du fournisseur de services d'informer les personnes-ressources désignées de l'institution lorsqu'il reçoit des demandes d'accès officielles ou informelles à des documents et à des renseignements personnels dont il a la garde.
- Si le fournisseur de services reçoit une demande d'accès directement du public, exiger qu'il informe sans délai l'auteur de la demande que toute demande d'accès doit être adressée par écrit directement à l'institution[11].
- Si le fournisseur de services reçoit une demande d'accès de la part des forces de l'ordre, exiger qu'il en informe sans délai les personnes-ressources désignées de l'institution, qu'il refuse d'accorder l'accès sans mandat et qu'il demande aux forces de l'ordre d'adresser leur demande directement à l'institution.

2.5 Collecte de renseignements personnels par le fournisseur de services

- Décrire les obligations du fournisseur de services et les interdictions liées à la collecte ou à la création de renseignements personnels, et notamment :
    - o préciser le pouvoir du fournisseur de services de recueillir des renseignements personnels au nom de l'institution;
    - o limiter les fins auxquelles le fournisseur de services peut recueillir des renseignements personnels aux termes de l'accord;

10 Pour que des renseignements soient considérés comme étant « dépersonnalisés », tous les éléments qui (i) permettent d'identifier directement un particulier ou (ii) peuvent être utilisés, seuls ou avec d'autres renseignements, pour identifier un particulier, doivent être retirés.

11 Selon les procédures d'accès prévues dans la LAIPVP et la LAIMPVP, les demandes de renseignements dont une institution a la garde ou le contrôle doivent être adressées directement à l'institution. Soulignons que le par. 62 (1) de la LAIPVP et le par. 49 (1) de la LAIMPVP n'autorisent pas l'institution à déléguer cette attribution à un fournisseur de services.

- préciser les renseignements personnels que le fournisseur de services peut recueillir[12] et limiter les éléments de données autorisés à ceux qui sont nécessaires à l'exécution des activités définies dans l'accord.
- préciser le mode de collecte (c.-à-d. collecte directe ou indirecte); si la collecte est directe, s'assurer qu'elle est dûment autorisée[13].
- exiger que soient donnés des avis de collecte appropriés[14].

2.6 Utilisation et conservation de documents ou de renseignements personnels par le fournisseur de services

- Définir les obligations du fournisseur de services et les interdictions liées à l'utilisation et à la conservation de documents ou de renseignements personnels dont il a la garde, notamment :
  - définir les obligations du fournisseur de services liées à la conservation des documents et des renseignements personnels (p. ex., suivre un calendrier de conservation établi, rendre les documents et les renseignements personnels, les détruire de façon sécurisée);
  - interdire au fournisseur de services de supprimer ou de modifier des documents ou des renseignements personnels, sauf dans les cas prévus par l'accord ou sur autorisation écrite préalable;
  - définir les obligations du fournisseur de services et les interdictions liées à la gestion des copies de sauvegarde de documents et de renseignements personnels.
- Préciser les obligations du fournisseur de services et les interdictions liées à l'utilisation et à la conservation des renseignements personnels qu'il traite, notamment :
  - limiter les fins auxquelles ces renseignements personnels peuvent être utilisés;
  - exiger du fournisseur de services qu'il prenne des mesures raisonnables pour s'assurer que les renseignements personnels dont il a la garde soient correctement documentés, complets et mis à jour en fonction des besoins;
  - définir les obligations du fournisseur de services quant à la rectification[15] de renseignements personnels à la demande de l'institution, y compris le suivi des divulgations de renseignements personnels, afin de permettre la notification des rectifications ou des déclarations de désaccord[16].

12 À noter que la collecte comprend également la création de nouveaux renseignements personnels par le fournisseur de services dans le cadre de ses activités contractuelles. Un exemple serait celui d'un fournisseur de services qui soumet à des analyses les renseignements personnels de particuliers dans une base de données, puis qui crée de nouvelles catégories et y affecte les particuliers en se fondant sur les résultats de l'analyse.

13 Par. 39 (1) de la LAIPVP et par. 29 (1) de la LAIMPVP.

14 Dans la plupart des cas, il s'agit de reproduire l'avis de collecte de l'institution et d'indiquer où il est possible de le trouver dans son site Web. Strictement parlant, la personne responsable d'une institution ne peut pas déléguer au fournisseur de services son obligation de donner des avis de collecte. Voir les par. 62 (1) de la LAIPVP et 49 (1) de la LAIMPVP.

15 Cette tâche incombe à l'institution. En vertu de l'article 47 de la LAIPVP et de l'article 36 de la LAIMPVP, le droit à la rectification ou au désaccord n'est conféré que si l'accès a été accordé à l'auteur de la demande en réponse à une demande d'accès.

16 Voir l'alinéa 47 (2) c) de la LAIPVP et l'alinéa 36 (2) c) de la LAIMPVP.

2.7 Divulgation de renseignements personnels par le fournisseur de services

- Définir les obligations du fournisseur de services et les interdictions liées à la divulgation de renseignements personnels dont il a la garde, notamment :
    - o définir les obligations du fournisseur de services en matière de confidentialité[17];
    - o limiter les fins auxquelles les renseignements personnels peuvent être transférés ou divulgués à une autre partie aux termes de l'accord, en précisant à qui et dans quelles conditions ils peuvent l'être, à savoir :
        - » les fins auxquelles l'autre partie peut utiliser ou divulguer les renseignements personnels;
        - » la façon dont les documents ou renseignements personnels doivent être protégés ou éliminés;
        - » la façon dont la communication de renseignements personnels sera surveillée et dont les règles connexes seront appliquées;
    - o interdire la divulgation de renseignements personnels à des fins qui ne sont pas prévues dans l'accord;
    - o exiger que le fournisseur de services dépersonnalise les renseignements personnels dans certaines situations (p. ex., avant la divulgation à certaines parties) et préciser ce que signifie « dépersonnaliser »;
    - o exiger que le fournisseur de services informe immédiatement les personnes-ressources désignées de l'institution de toute demande de divulgation de renseignements personnels à des fins qui ne sont pas autorisées dans l'accord;
    - o exiger que le fournisseur de services informe immédiatement les personnes-ressources désignées de l'institution de toute divulgation non autorisée de renseignements personnels, conformément aux obligations en matière d'atteinte à la vie privée et de plaintes que prévoit l'accord.

17 Dans son rapport d'enquête sur la protection de la vie privée **PC12-39**, le CIPVP a examiné le Service automatisé de délivrance des permis du ministère des Richesses naturelles et souligné que le contrat que le ministère avait conclu comprenait [traduction] « des dispositions rigoureuses protégeant les renseignements personnels dont il a le contrôle et limitant leur utilisation par le mandataire » ainsi qu'une disposition de confidentialité indiquant que « renseignements confidentiels » s'entendait de [traduction] « tous les renseignements personnels que le ministère est tenu de ne pas divulguer ou peut refuser de divulguer en vertu d'une loi fédérale ou provinciale ou autrement en droit ». Le mandataire doit respecter les obligations suivantes aux termes du contrat en ce qui concerne les renseignements :

- protéger les renseignements et en préserver la confidentialité;
- limiter la divulgation de renseignements confidentiels aux seules personnes qui ont besoin de les connaître aux fins du contrat et qui ont été explicitement autorisées à les recevoir;
- ne pas divulguer, détruire, exploiter ou utiliser, directement ou indirectement, des renseignements confidentiels (sauf aux fins du contrat ou si une ordonnance d'un tribunal judiciaire ou administratif l'exige), sans avoir obtenu au préalable le consentement écrit du ministère et, en ce qui concerne les renseignements confidentiels détenus par le ministère au sujet d'un tiers, le consentement écrit du tiers en question;
- ne pas vendre de renseignements personnels sans le consentement du ministère et des tiers concernés.

2.8 Obligations du fournisseur de services relativement aux mesures de protection

- Définir les exigences minimales des programmes de protection de la vie privée et de sécurité du fournisseur de services, y compris le nom et les coordonnées du cadre responsable de la protection de la vie privée et de la sécurité, les politiques et pratiques en matière de protection de la vie privée et de sécurité et la formation dispensée aux employés et aux sous-traitants en la matière.
- Établir des contrôles d'accès aux documents ou aux renseignements personnels dont le fournisseur de services a la garde, et notamment limiter qui peut y accéder et à quelles fins.
- Exiger que le fournisseur de services sécurise les documents et les renseignements personnels, qu'ils soient sur papier ou sous forme électronique, sur place ou en transit, et qu'il prenne notamment des mesures raisonnables d'ordre matériel, technique et administratif correspondant au degré de sensibilité des renseignements, afin d'empêcher l'accès, l'utilisation ou la divulgation non autorisés, la perte ou le vol, l'altération, la copie, la détérioration, la destruction ou l'amalgame avec d'autres documents.
- Définir des exigences concernant les aspects suivants :
    - effectuer la surveillance et l'audit des contrôles d'accès, et exiger une piste de vérification pour confirmer que l'accès a été accordé uniquement aux parties autorisées;
    - assurer la tenue à jour des logiciels, et installer les rustines de sécurité;
    - mettre à l'essai et vérifier les mesures de sécurité;
    - fournir de la documentation sur le programme de sécurité;
    - vérifier la conformité à l'accord et aux recommandations éventuellement formulées à l'issue de l'audit.
- Exiger du fournisseur de services qu'il sépare les renseignements personnels liés à l'accord des autres renseignements dont il a la garde.
- Préciser les obligations du fournisseur de services et les interdictions liées à l'emplacement et au déplacement des documents et des renseignements personnels, y compris les copies de sauvegarde.
- Définir les exigences relatives au plan de reprise après sinistre et de continuité des activités du fournisseur de services et de ses sous-traitants relativement aux documents et aux renseignements personnels dont ils ont la garde.

2.9 Obligations en cas d'atteinte à la vie privée ou de plainte concernant la protection de la vie privée

- Définir ce qui constitue une atteinte à la vie privée.
- Définir les obligations du fournisseur de services, notamment :
    - maîtriser et évaluer l'atteinte à la vie privée;
    - signaler immédiatement l'atteinte à la vie privée aux personnes-ressources désignées de l'institution;
    - signaler l'atteinte à la vie privée aux autres parties et organismes de réglementation pertinents dès que possible ou, sous la forme, selon les autres exigences et dans les délais établis par la loi, le cas échéant;
    - communiquer avec l'institution pour déterminer qui avisera les parties concernées et quand et comment elles seront avisées;
    - faire enquête sur la cause de l'atteinte à la vie privée en collaboration avec l'institution et fournir à celle-ci les résultats de son enquête en temps opportun;
    - prendre des mesures correctives pour éviter d'autres atteintes à la vie privée.
- Préciser que le fournisseur de services doit :
    - assumer la responsabilité des actes de négligence, des actes intentionnels ou des omissions ayant causé l'atteinte à la vie privée;
    - indemniser l'institution pour tout dommage causé en raison de l'atteinte à la vie privée;
    - payer ou rembourser les coûts engagés en raison de l'atteinte à la vie privée (p. ex., pour informer les personnes concernées par les renseignements).
- Exiger du fournisseur de services qu'il gère les questions et plaintes sur ses pratiques en matière de protection des renseignements personnels dont il a la garde.
- Exiger du fournisseur de services qu'il informe immédiatement les personnes-ressources désignées de l'institution lorsqu'il reçoit une plainte qui pourrait porter sur les obligations de l'institution en vertu de la LAIPVP, de la LAIMPVP ou de toute autre loi applicable.

2.10 Surveillance de la conformité du fournisseur de services à l'accord

- Définir comment l'accès à l'information, la protection de la vie privée et les mesures de sécurité seront surveillées afin de garantir la conformité du fournisseur de services à l'accord, y compris comment et quand la vérification de la conformité ou les audits doivent être effectués (p. ex., visites sur place ou inspections de la part de l'institution, ou vérification indépendante par une tierce partie convenue).
- Préciser les exigences en matière de production de rapports et la documentation que le fournisseur de services doit produire pour démontrer sa conformité aux politiques et procédures de sécurité et de protection de la vie privée, aux audits de sécurité et aux certifications en matière de protection de la vie privée et de sécurité.

- Exiger du fournisseur de services qu'il donne un préavis en cas de modifications importantes apportées aux mesures de sécurité et de protection de la vie privée, aux processus opérationnels ou aux travaux ou services sous-traités qui pourraient avoir une incidence sur ses obligations en vertu de l'accord, y compris, sans s'y limiter, sa capacité à respecter ces obligations.
- Préciser les obligations du fournisseur de services en matière d'EIVP en cas de changements importants au cours de la période visée par l'accord, y compris les circonstances où une EIVP est nécessaire, et qui peut l'effectuer si ce n'est pas l'institution elle-même (l'institution, le fournisseur de services ou une autre partie désignée).
- Définir les responsabilités en cas de manquement aux modalités de l'accord de la part du fournisseur de services ou de ses employés, mandataires, autres représentants et sous-traitants, notamment en cas d'omissions ou d'actes intentionnels ou commis par négligence et liés à la collecte, à l'utilisation, à la divulgation, à la conservation, à la protection ou à la disposition non autorisées de documents et de renseignements personnels.
- Préciser que le fournisseur de services est tenu d'informer l'institution en cas de changement de propriété ou de contrôle de tout ou partie de ses activités et en cas de procédure de faillite ou d'insolvabilité engagée par ou contre lui.
- Préciser que le fournisseur de services doit coopérer et participer à toute enquête liée à la conformité aux modalités de l'accord de services.
- Préciser que le fournisseur de services doit contribuer à ce que l'institution se conforme rapidement aux ordonnances du CIPVP concernant l'accès aux documents ou la protection des renseignements personnels dont il a la garde.
- Demander au fournisseur de services de se familiariser avec les dispositions de la LAIPVP ou de la LAIMPVP concernant les infractions.

Partie 3 : Sélection du fournisseur

La présente section décrit les aspects touchant l'accès à l'information et la protection de la vie privée dans le cadre des étapes d'évaluation et d'attribution du processus d'approvisionnement.

Il incombe à votre institution de sélectionner un fournisseur de services qui est en mesure de respecter les modalités de l'accord et les autres exigences applicables.

Pour ce faire, votre institution doit :

- évaluer les fournisseurs de services éventuels afin de déterminer s'ils comprennent les exigences établies en matière d'accès à l'information et de protection de la vie privée et peuvent les respecter;
- veiller à ce qu'une personne ayant une connaissance suffisante de l'accès à l'information, de la protection de la vie privée et de la sécurité, de même que des modalités prévues dans les documents d'appel d'offres, participe au processus d'évaluation et soit disponible pour résoudre les problèmes et répondre aux questions;
- veiller à ce que les fournisseurs de services éventuels produisent tous les documents appropriés relatifs aux exigences en matière d'accès à l'information, de protection de la vie privée et de sécurité avant leur sélection;
- mener toute activité nécessaire à la collecte de renseignements suffisants pour évaluer les fournisseurs de services (p. ex., visites sur place, entretiens);
- veiller à ce que les aspects de l'évaluation relatifs à l'accès à l'information, à la protection de la vie privée et à la sécurité soient assortis d'une pondération et de critères appropriés en fonction de la sensibilité, de la portée et de l'ampleur des renseignements personnels qui seront traités;
- veiller à ce que les aspects du processus de sélection relatifs à l'accès à l'information, à la protection de la vie privée et à la sécurité fassent l'objet d'une évaluation approfondie de la part d'experts en la matière, selon des critères établis;
- s'assurer que les fournisseurs de services éventuels savent que les documents qu'ils soumettent ou communiquent dans le cadre du processus d'approvisionnement sont assujettis aux dispositions de la LAIPVP ou de la LAIMPVP en matière d'accès à l'information, et leur faire part de cette exigence tout au long du processus d'évaluation.

Partie 4 : Accord

La présente section traite des aspects dont il faut tenir compte lors de la conclusion d'un accord avec le fournisseur de services.

L'accord de services doit refléter la portée et les produits livrables de l'approvisionnement et contenir toutes les exigences relatives à l'accès à l'information, à la protection de la vie privée et à la sécurité qui ont été définies dans les documents d'appel d'offres.

Les institutions doivent mettre en place des mesures contractuelles et de surveillance raisonnables pour assurer l'accès aux documents et aux renseignements personnels dont elles ont le contrôle, ainsi que leur protection et leur sécurité[18].

Les modalités contractuelles qui pourraient être nécessaires et pertinentes pour faire en sorte que toutes les mesures raisonnables soient prises pour assurer la confidentialité et la sécurité des renseignements personnels dont l'institution a le contrôle sont notamment les suivantes[19] :

- Propriété des données : Le contrat doit prévoir que l'institution a la propriété exclusive de tous les documents et renseignements personnels visés par l'accord.
- Renseignements confidentiels : Le contrat doit définir les renseignements confidentiels comme étant tous les renseignements personnels que l'institution est tenue de protéger en vertu de la législation provinciale ou fédérale ou autrement en droit, et le fournisseur de services doit être tenu de préserver la confidentialité et la sécurité de ces renseignements et d'en limiter l'accès aux seules personnes qui ont besoin d'en prendre connaissance dans le cadre de leurs fonctions en vertu du contrat et qui ont été expressément autorisées à les recevoir.
- Collecte, utilisation et divulgation : Le contrat doit prévoir que le fournisseur de services ne peut, directement ou indirectement, utiliser, recueillir ou divulguer des documents ou des renseignements personnels à des fins non autorisées par l'institution. À moins que le fournisseur de services n'obtienne une autorisation préalable expresse et écrite de l'institution, l'accès aux biens, à la technologie ou aux renseignements de l'institution ou leur utilisation doivent lui être interdits à moins d'être nécessaires à l'exécution de ses obligations contractuelles envers l'institution.
- Avis de divulgation imposée par force de loi : Le contrat doit prévoir que si le fournisseur de services est légalement contraint à divulguer des renseignements confidentiels de l'institution, il doit en informer celle-ci dans les plus brefs délais afin de lui permettre de demander une ordonnance préventive ou de prendre toute autre mesure qui s'impose pour empêcher ou limiter cette divulgation. De plus, le fournisseur de services ne doit divulguer que la partie des renseignements confidentiels qu'il est légalement contraint à divulguer.
- Sous-traitance : Le contrat doit prévoir que le fournisseur de services n'est pas autorisé à sous-traiter tout ou partie du contrat sans l'accord écrit préalable de l'institution. Si l'institution accepte que le fournisseur de services sous-traite certains services, le sous-traitant doit être identifié et soumis à des obligations contractuelles identiques ou équivalentes à celles qui ont été imposées au fournisseur de services.

---

18 Conformément aux exigences établies à l'art. 4 du Règl. de l'Ont. 460 et aux art. 4 et 5 du Règl. de l'Ont. 459 pris en application de la LAIPVP, ainsi qu'à l'art. 3 du Règl. de l'Ont. 823 pris en application de la LAIMPVP.

19 Ces modalités contractuelles s'appuient sur le rapport concernant une plainte relative à la protection de la vie privée **PR16-40**. Ce rapport énumère les dispositions contractuelles qui peuvent être pertinentes pour déterminer si une institution a respecté son obligation de prendre toutes les mesures raisonnables pour assurer la confidentialité et la sécurité des renseignements personnels dont elle a le contrôle. Le CIPVP a utilisé des dispositions contractuelles semblables comme cadre d'évaluation dans le cadre d'enquêtes concernant des fournisseurs de services externes. Voir par exemple **MC18-48**, **MC17-52**, **MC18-17** et **PI21-00001**.

- Sécurité : Le contrat doit prévoir que le fournisseur de services doit garantir la sécurité et l'intégrité de tous les documents et renseignements personnels dont il a la garde. Il doit conserver les renseignements personnels et les documents dans un endroit sûr et séparé, à l'abri de la perte, de l'altération, de la destruction ou de l'amalgame avec d'autres documents et bases de données. En outre, il doit mettre en œuvre et appliquer des mesures et procédures raisonnables d'ordre matériel, administratif et technologique pour protéger les renseignements.
- Audits : Le contrat doit prévoir que le fournisseur de services se soumettra à des audits annuels de conformité en matière de protection de la vie privée et de sécurité, pendant toute la durée du contrat. L'accord doit préciser qui effectuera ces audits, quand et comment. Ces audits peuvent comprendre l'examen des EIVP, des EMR et d'autres évaluations de la vulnérabilité.
- Conservation et destruction : Le contrat doit prévoir que le fournisseur de services doit rendre tous les renseignements confidentiels à l'institution au plus tard à la fin du contrat, sans en conserver de copie ou de partie. Le contrat doit également établir un calendrier de conservation et de destruction pour le fournisseur de services.

Il est à noter que ces dispositions contractuelles recommandées ne font pas autorité et ne sont pas exhaustives. Il y a lieu de consulter les experts pertinents de l'institution (énumérés à la section 1.1 du présent document, « Planification préliminaire »), y compris ses avocats, pour déterminer si toutes les mesures raisonnables ont été prises pour protéger les documents ou les renseignements personnels visés par l'accord en question.

Partie 5 : Gestion et expiration ou résiliation de l'accord

La présente section traite de facteurs touchant la gestion et la surveillance de l'accord ainsi que l'application des exigences en matière d'accès à l'information, de protection de la vie privée et de sécurité.

Conformément aux politiques établies, votre institution doit prendre des mesures précises, et effectuer un suivi au besoin, pour surveiller le rendement des fournisseurs de services afin de s'assurer qu'ils respectent les exigences et interdictions prévues dans l'accord, et notamment :

- établir que l'accord ou le contrat est régi par les dispositions relatives à l'accès à l'information de la LAIPVP ou de la LAIMPVP, sous réserve des exceptions applicables[20];
- surveiller le rendement du fournisseur de services au regard des modalités de l'accord;
- veiller à ce que le fournisseur de services réponde aux exigences et suive les processus établis en temps utile et de manière appropriée (formation, engagements de confidentialité, établissement de rapports, interventions en cas d'atteinte à la vie privée, etc.);

20 Voir le bulletin d'interprétation **Renseignements de tiers** du CIPVP publié en 2024.

- veiller à ce que l'institution ou des parties désignées mènent les activités requises d'évaluation et de gestion de l'accord (p. ex., les audits, EIVP ou inspections) en temps utile;
- évaluer le rendement du fournisseur de services afin de déterminer si des mesures correctives ou préventives s'imposent et, le cas échéant, exiger que le fournisseur prenne ces mesures;
- s'assurer que le fournisseur de services signale en temps utile les risques liés à l'accès à l'information, à la protection de la vie privée et à la sécurité et que les plans d'intervention pertinents sont mis en œuvre;
- appliquer les modalités du contrat en prenant des mesures correctives, dont la résiliation, en cas de manquement de la part du fournisseur de services sur le plan de l'accès à l'information, de la protection de la vie privée ou de la sécurité;
- assurer une délégation appropriée des rôles et des responsabilités de l'institution, avec une formation et des ressources adéquates, pour mener à bien ces mesures de surveillance pendant la durée du contrat ou de l'accord avec le fournisseur de services.

À la fin du contrat ou après sa résiliation, l'institution doit :

- définir les modalités liées à l'expiration ou à la résiliation de l'accord (p. ex., la restitution des documents ou leur disposition en toute sécurité, y compris les copies de sauvegarde) et les documents exigés (p. ex., certificat de destruction);
- recenser et documenter les enseignements tirés relativement aux aspects de l'accord ayant trait à l'accès à l'information, à la protection de la vie privée et à la sécurité. Cette démarche peut contribuer à l'élaboration, à la mise en œuvre, à la surveillance ou à la fermeture d'accords futurs avec le même fournisseur de services ou d'autres fournisseurs.

Glossaire

Accord

Dans le présent document, s'entend d'un contrat, d'un protocole d'entente, d'un accord de niveau de services ou d'un autre instrument juridique entre une institution et un fournisseur de services qui traitent des documents ou des renseignements personnels au nom de l'institution.

Approvisionnement

Processus consistant pour une institution à trouver, à sélectionner et à acquérir des biens ou services auprès de fournisseurs externes afin de répondre à ses besoins opérationnels.

Contrôle

Avoir le contrôle d'un document ou de renseignements personnels signifie en être responsable, en assurer la protection et être en mesure de décider de leur gestion. Une institution a le contrôle d'un document ou de renseignements personnels lorsqu'elle a l'obligation et le pouvoir de les gérer, et notamment de limiter, de régir et d'assurer leur utilisation, divulgation ou disposition, sans égard à l'entité qui en a la garde.

Document

Document qui reproduit des renseignements sans égard à leur mode de transcription, que ce soit sous forme imprimée, sur film, au moyen de dispositifs électroniques ou autrement [par. 2 (1) de la LAIPVP ou de la LAIMPVP].

Évaluation de l'incidence sur la vie privée (EIVP)

Analyse comportant plusieurs activités et livrables; il ne s'agit pas d'un seul document ou produit final. Cette évaluation peut contribuer à relever, analyser et atténuer des risques importants pour la vie privée associés à la création ou à la modification de programmes ou de systèmes, y compris ceux qui font intervenir des fournisseurs de services. Comprendre les risques pour la vie privée peut vous aider à prendre des mesures appropriées en temps opportun afin que vous et votre fournisseur de services respectiez la LAIMPVP ou la LAIMPVP ainsi que d'autres exigences, et à prendre des décisions éclairées en matière de politiques, d'activités, d'approvisionnement, d'architecture et de sécurité. (Voir **Planifier pour réussir : Guide d'évaluation de l'incidence sur la vie privée** du CIPVP, publié en 2015.)

Évaluation de la menace et des risques

Outil de gestion des risques pour la sécurité et d'élaboration de plans de sécurité. Cette évaluation est effectuée pour : évaluer la nature sensible des biens et des renseignements; identifier et analyser les menaces et les vulnérabilités éventuelles; évaluer le niveau de risque, en tenant compte de l'efficacité des mesures de sécurité actuelles; recommander des mesures appropriées pour protéger les biens et les renseignements contre la perte, le vol, la destruction, la modification ou l'utilisation abusive.

Externalisation

Délégation de tâches ou d'activités (y compris le traitement de documents ou de renseignements personnels) qu'une institution pourrait être en mesure d'accomplir, mais que des fournisseurs externes pourraient faire mieux ou à moindre coût. L'externalisation peut avoir pour objectif de réduire les coûts, d'augmenter l'efficacité ou d'améliorer la qualité.

Fournisseur de services

Entité qui fournit des services à l'institution. Il peut s'agir d'une organisation, d'une entreprise ou d'un particulier de l'extérieur ou d'un autre secteur de programme de la même institution. Les services peuvent être fournis contre rémunération ou non.

Garde

Possession matérielle d'un document ou de renseignements personnels. Cette notion se distingue de celle du contrôle; un fournisseur de services peut avoir la garde mais non le contrôle d'un document ou de renseignements personnels. Dans le contexte d'un accord avec un fournisseur de services, l'institution doit conserver le contrôle et la responsabilité d'un document ou de renseignements personnels recueillis en son nom, même si un fournisseur de services les traite ou les conserve.

Institution

En vertu de la LAIPVP, ministère ou organisme, conseil, commission, personne morale ou autre entité désignés comme institution dans les règlements [par. 2 (1) de la LAIPVP].

En vertu de la LAIMPVP, municipalité, école, service de police ou organisme, conseil, commission, personne morale ou autre entité désignés comme institution dans les règlements [par. 2 (1) de la LAIMPVP].

Personne responsable

Directeur de programme ou l'équivalent que la loi, un règlement, une politique ou un autre instrument autorise à exercer des fonctions particulières au sein de l'institution, à gérer les documents qui les concernent et à en rendre compte. La personne responsable doit se conformer à la LAIPVP ou à la LAIMPVP.

Renseignements personnels

Renseignements consignés ayant trait à un particulier qui peut être identifié, par exemple, le nom, l'adresse, le numéro de téléphone, le sexe, l'état matrimonial, l'éducation, les antécédents professionnels ou criminels et les renseignements médicaux. Il peut également s'agir « d'un numéro d'identification, d'un symbole ou d'un autre signe individuel » qui est attribué au particulier, s'il est raisonnable de s'attendre à ce que ce particulier puisse être identifié à partir des renseignements, seuls ou combinés à d'autres renseignements. (Voir le par. 2 (1) de la LAIPVP ou de la LAIMPVP, et la feuille-info **Que sont les renseignements personnels?** de 2016 de même que le bulletin d'interprétation **Renseignements personnels** de 2024 du CIPVP.)

Traitement

S'entend de la collecte, de l'utilisation, de la divulgation, de la conservation, du stockage, de la protection ou de la disposition de documents ou de renseignements personnels.

Document d'orientation du CIPVP :

La protection de la vie privée et l'accès à l'information dans les contrats du secteur public avec des fournisseurs de services externes

Information and Privacy Commissioner of Ontario

Commissaire à l'information et à la protection de la vie privée de l'Ontario

2, rue Bloor Est,
Bureau 1400
Toronto, Ontario
Canada M4W 1A8

www.ipc.on.ca/fr
416-326-3333
info-fr@ipc.on.ca

Mai 2024