Deloitte.

Confidentialité des données dans le nuage

Explorer le nouveau régime de protection de la vie privée dans l'environnement infonuagique

L’ère de l’infonuagique est arrivée! Cette innovation révolutionnaire comprend un vaste éventail de capacités d’externalisation de processus d’affaires publics et privés. Les services infonuagiques offrent une adaptabilité, une élasticité et une flexibilité inégalées. Les avantages sont si attrayants pour les entreprises que le taux d’adoption de ces services devrait continuer de connaître une croissance rapide dans tous les secteurs et sous-secteurs.

D’ici 2020, une politique de TI sans infonuagique sera aussi rare qu’une politique sans Internet peut l’être aujourd’hui.

Prédictions 2016 : l’informatique en nuage dominera le commerce numérique. (Gartner)

De nos jours, l'infonuagique offre des logiciels, des plates-formes, des infrastructures et des solutions de stockage flexibles et abordables aux organisations de tous les secteurs. Ces dernières, qui doivent composer avec des budgets limités et des demandes de croissance toujours plus pressantes, trouvent dans l'infonuagique la possibilité de réduire leurs coûts, d'accroître leur flexibilité et d'améliorer leurs capacités en matière de TI.

Types de services infonuagiques

Nuage privé
Outils qui fournissent l'adaptabilité et le libre-service pour une architecture interne.

Infrastructure-service
Capacités de calcul, de stockage et de réseautage à la demande, hébergées par un fournisseur.

Plate-forme-service
Collection d'outils qui permettent le développement d'une application hébergée par un fournisseur.

Logiciel-service
Applications hébergées par un fournisseur et utilisées par des clients sur Internet.

Nuage personnel
Capacités hébergées par un fournisseur allant du stockage à la diffusion en continu, en passant par la collaboration, accessibles par l'intermédiaire de comptes personnels.

D'ici 2019, les services infonuagiques devraient se chiffrer à 312 milliards de dollars annuellement à l'échelle mondiale et afficher une croissance de 15 % d'un exercice à l'autre[1]. Il s'agira en fait du segment qui connaîtra la plus importante croissance parmi les dépenses des TI en général, puisque les organisations commencent à tirer avantage du haut niveau de normalisation, de la fonction libre-service et du niveau d'automatisation offerts en ne payant que pour ce dont elles ont besoin, quand elles en ont besoin[2].

Toutefois, l'adoption de l'informatique en nuage soulève des questions découlant des nouveaux règlements sur la protection des renseignements personnels, qui divergent souvent d'un territoire à l'autre, et des cybermenaces en constante évolution. Par exemple, les organisations qui comptent sur plusieurs fournisseurs de services infonuagiques pourraient avoir peu ou pas de contrôle sur le transfert de leurs données au sein des différents centres de données partout dans le monde. De la même manière, il est parfois difficile de savoir qui, du gardien des données ou du fournisseur de services tiers, est responsable de la protection des données, ou encore quel est l'ensemble de lois sur la protection des données qui s'applique. Qui plus est, les fournisseurs de services infonuagiques sont souvent réticents à divulguer entièrement les mesures de sécurité qu'ils utilisent pour protéger l'information ou leur manière de traiter les données, ce qui pose problème étant donné la prolifération et l'ampleur des récentes atteintes à la confidentialité qui ont donné lieu à des recours collectifs liés à la protection de la vie privée et qui ont porté atteinte à la réputation des utilisateurs de systèmes infonuagiques.

Par conséquent, il n'est pas étonnant que les organisations qui se tournent vers la prochaine génération de services infonuagiques externalisés soient préoccupées par la confidentialité et la protection des données dans le nuage.

[1] Gartner. Forecast Analysis: Public Cloud Services, Worldwide, 2Q15 Update, 26 août 2015.
[2] Forrester. TechRadar Cloud Computing Q4 2015, 8 décembre 2015.

Principales considérations

Il n'y a pas de réponse simple aux défis liés à la réglementation, à la confidentialité et à la sécurité que pose l'informatique en nuage, mais il existe trois étapes importantes que vous pouvez suivre pour protéger vos données dans le nuage.

Comprendre les lois sur la protection de la vie privée des différents territoires et vous y conformer

Vous pouvez comprendre les risques que vous courez et vos obligations uniquement lorsque vous connaissez les exigences juridiques du territoire d'où viennent les données, et où elles sont stockées et traitées au bout du compte.

Comprendre comment votre fournisseur de services infonuagiques protégera vos données

La tendance juridique est de diviser la chaîne d'approvisionnement des services d'informatique en nuage en rendant chacune des parties responsable de la confidentialité des données, au lieu du seul gardien ou contrôleur des données.

Explorer différents outils et technologies de chiffrement

Une grande variété d'outils et de capacités, qui fournissent notamment des mécanismes de chiffrement et d'anonymisation afin de sécuriser vos renseignements, continuent d'arriver sur le marché.

Étape 1 :

Où vos données sont-elles stockées?

Comprendre les lois sur la protection de la vie privée des différents territoires et s'y conformer

Selon les modèles d'informatique en nuage, les données sont souvent traitées ou stockées dans plusieurs territoires, créant des chevauchements de territoires pour les entreprises canadiennes et les multinationales. Ces organisations doivent donc se conformer aux lois canadiennes en matière de protection de la vie privée de même qu'aux lois des autres territoires.

Les lois canadiennes

Au Canada, les sociétés sous réglementation fédérale et les entreprises du secteur privé visées par la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) sont autorisées à traiter ou à stocker des renseignements personnels à l'extérieur du Canada, à condition que des garanties contractuelles et des mesures de sécurité adéquates aient été mises en place et que les clients en aient été avisés. En Alberta, les entités du secteur privé visées par la législation provinciale de protection de la vie privée doivent aller encore plus loin et fournir un avis (habituellement par l'intermédiaire d'une politique de confidentialité affichée publiquement) sur la manière d'obtenir de l'information au sujet des politiques, garanties et pratiques du fournisseur de services.

Il n'en va pas de même pour le secteur public. Parmi les obstacles importants à l'utilisation des services infonuagiques figurent certaines des lois provinciales canadiennes sur la localisation des données, plus précisément pour les organismes du secteur public exerçant leurs activités en Nouvelle-Écosse et en Colombie-Britannique, qui peuvent restreindre la manière dont les données personnelles peuvent être stockées à l'extérieur du pays et la façon d'y accéder. La *Loi sur l'accès à l'information et la protection de la vie privée* de la Colombie-Britannique et la loi sur la protection des renseignements personnels (*Personal Information International Disclosure Protection Act*) de la Nouvelle-Écosse interdisent toutes deux l'accès aux données ainsi que leur divulgation et leur stockage à l'extérieur du Canada sans consentement. D'autres restrictions dans la législation canadienne peuvent également nécessiter que certains dossiers soient conservés au Canada (p. ex., les dossiers fiscaux).

Cela s'explique en grande partie par la capacité des organismes étrangers d'application de la loi d'accéder aux données des citoyens canadiens, sans avis ni consentement, en vertu de la *USA Patriot Act*. Par conséquent, par mesures administratives, les entités du secteur public canadien ont hésité à adopter les solutions infonuagiques, même lorsqu'il n'y a aucune restriction dans d'autres provinces. Dans de nombreux cas, des technologies additionnelles, telles que le chiffrement et la segmentation en unités, devraient être envisagées pour permettre aux entités du secteur public d'utiliser l'infonuagique tout en se conformant à la législation.

Les lois européennes

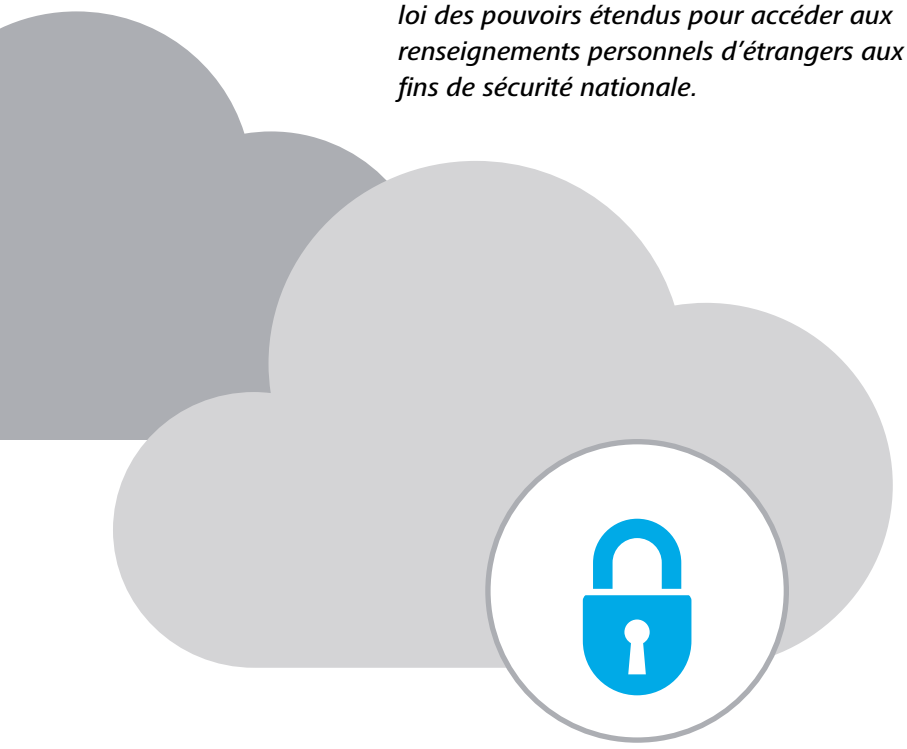
Les multinationales canadiennes exerçant des activités dans l'Union européenne (UE) doivent porter une attention particulière à deux changements réglementaires additionnels : l'invalidation de l'accord Safe Harbor entre l'UE et les États-Unis[3], et le nouveau règlement général sur la protection des données (RGPD) qui doit entrer en vigueur d'ici 2018.

En octobre 2015, la Cour de justice de l'Union européenne a déclaré invalide l'accord Safe Harbor entre l'UE et les États-Unis, lequel permettait l'échange de données outre-Atlantique, invoquant le fait qu'il ne protégeait pas adéquatement les données des citoyens de l'Union européenne de l'accès qu'y avaient les organismes américains d'application de la loi. En effet, les entreprises de l'UE peuvent transférer des renseignements personnels uniquement dans les pays dont les lois fournissent une protection « adéquate »; les lois américaines en matière de protection de la vie privée ne sont pas considérées comme adéquates. Bien que cette décision n'interdise pas le transfert de données à des fournisseurs de services infonuagiques se trouvant aux États-Unis, elle annule les règles d'exonération desquelles les entreprises pouvaient se réclamer lorsqu'elles transféraient des données personnelles de l'UE vers les États-Unis aux fins de stockage ou de traitement. Cela pose problème étant donné que les quatre principaux fournisseurs de services infonuagiques, soit Amazon Web Services, Microsoft Azure, Google et IBM SoftLayer, ainsi que la plupart des principaux acteurs du secteur des logiciels-services, tels que ServiceNow, Salesforce et Microsoft Office 365, ont leur siège social aux États-Unis; la plupart de leurs centres de données sont aussi situés aux États-Unis.

[3] L'accord Safe Harbor avait été négocié entre le département du Commerce américain et la Commission européenne pour permettre aux entreprises de transférer des données de l'UE vers les États-Unis en conformité avec la directive sur la protection des données de l'UE (maintenant remplacée par le RGPD). Seules les organisations autocertifiées qui adhéraient aux principes de l'accord Safe Harbor relatifs à la protection de la vie privée étaient légalement autorisées à transférer des données de l'UE vers les États-Unis. La décision de la Cour de justice de l'Union européenne a été rendue dans une affaire présentée par Max Schrems, un utilisateur autrichien de Facebook qui a déposé une poursuite en vertu de la loi de protection des données irlandaise après que les révélations d'Edward Snowden ont montré que ses données, de même que celles d'autres citoyens de l'UE, avaient fait l'objet d'un accès par les services secrets américains.

Afin de fournir aux entreprises un système d'autocertification fondé sur des principes à long terme en vue du transfert sécurisé des données personnelles de citoyens européens vers les États-Unis, la Commission européenne et le département du Commerce américain ont récemment conclu un nouvel accord appelé « Bouclier vie privée UE-États-Unis » (EU-US Privacy Shield). Cet accord comprend des principes tels que la sécurité, la responsabilité des transferts ultérieurs, la publication d'avis, le choix, l'intégrité des données, la limitation de la finalité, l'accès, les recours, l'application de la loi et la responsabilité. En vertu du nouveau cadre, les entreprises qui transfèrent des données de citoyens de l'UE doivent s'engager à respecter des obligations encore plus strictes à l'égard de la confidentialité des données et à les publier. Ces engagements à l'égard de la protection de la vie privée doivent être supervisés par le département du Commerce américain et mis en application par la Federal Trade Commission (FTC). En outre, les entreprises qui traitent des données des RH de l'UE seront liées par les décisions des Autorités de protection des données (APD) européennes.

Bien que la LPRPDE du Canada soit actuellement considérée comme adéquate pour la protection des données des citoyens de l'UE, cela pourrait être remis en question si le projet de loi C-51, la nouvelle Loi antiterroriste du Canada, n'est pas modifié dans sa version actuelle, qui donne aux organismes canadiens d'application de la loi des pouvoirs étendus pour accéder aux renseignements personnels d'étrangers aux fins de sécurité nationale.



De plus, le nouveau RGPD imposera de nouvelles exigences en matière de sécurité et de confidentialité à toute organisation qui fait appel à un fournisseur de services infonuagiques pour traiter ou stocker des données de citoyens de l'Union européenne. Une fois entériné, le RGPD remplacera la directive de protection des données européenne, qui fournissait la base pour chaque loi sur la protection des données dans chaque État membre, et accroîtra les responsabilités tant pour les utilisateurs que pour les fournisseurs de services infonuagiques :

- Toute entreprise (contrôleur des données) qui choisit de traiter des données dans le nuage devra s'assurer que le fournisseur de services infonuagiques (agent de traitement des données) offre des garanties suffisantes pour mettre en œuvre des mesures de protection techniques et organisationnelles appropriées qui respectent la nouvelle réglementation de l'UE.
- Le contrat de service entre le contrôleur des données et l'agent de traitement des données devra interdire le recours à des sous-traitants sans consentement.
- Le contrat de service oblige le contrôleur des données à retirer les données du nuage à la fin du contrat, et à rendre toute information disponible aux ADP du pays pour en assurer la conformité.
- Le contrôleur des données et l'agent de traitement des données devront tous deux effectuer des évaluations des risques afin de s'assurer que l'utilisation des mesures de sécurité est appropriée compte tenu des risques identifiés.
- Le contrôleur des données aura le devoir de signaler les atteintes à la sécurité, et le contrôleur des données et l'agent de traitement des données seront tous deux responsables conjointement de tout dommage résultant d'un incident de sécurité.

Il est important de noter que ces changements ont déjà une incidence sur le marché. Microsoft et Amazon ont annoncé qu'elles ouvriront des centres de services infonuagiques au Canada afin de se conformer à la demande quant aux données qui doivent être conservées au pays. Microsoft a aussi annoncé l'ajout de capacités de stockage de données en Allemagne grâce à un nouveau système de contrôle du chiffrement dont une entreprise locale détient des clés de sécurité pour les serveurs allemands dans son nuage Azure. Seule une cour d'Allemagne sera en mesure d'ordonner que celles-ci soient cédées. Il est prévu que cette pratique deviendra la norme pour les sites à l'extérieur des États-Unis.

Étape 2 :

De quelle manière vos données sont-elles protégées?

Comprendre comment votre fournisseur de services infonuagiques protégera vos données

À la lumière de ces tendances réglementaires, les entreprises canadiennes qui font affaire avec des fournisseurs de services infonuagiques doivent porter une attention particulière aux territoires dans lesquels leurs données seront stockées.

Pour se conformer à la réglementation sur la confidentialité à l'échelle mondiale, les organisations doivent s'assurer que leurs fournisseurs de services infonuagiques mettent en place des contrôles techniques et administratifs afin de protéger leurs données. Cela est particulièrement important pour les organisations qui traitent des données de l'UE, car les autorités de l'UE peuvent évaluer chaque transfert de données si une plainte concernant la protection de la vie privée est portée à leur attention. Afin d'éviter les problèmes de non-conformité, les contrats avec les fournisseurs de services infonuagiques devraient définir des normes de protection des données et établir des ententes de niveau de service (ENS) qui décrivent les mesures de sécurité et de confidentialité. Ces mesures devraient inclure des contrôles techniques adéquats, tels que le chiffrement de bout en bout ou la segmentation en unités. Des outils de prévention de pertes de données peuvent aussi contribuer à appliquer les politiques visant le transfert des données.

Pour que ces ententes juridiques aient un effet concret, les organisations doivent aussi les gérer activement. En d'autres mots, elles devraient exiger des rapports réguliers sur la pertinence des mesures de confidentialité et de sécurité et sur les activités liées aux bases de données de leurs fournisseurs de services infonuagiques, ainsi que la divulgation de tout incident ou question qui pourrait présenter un risque pour les données.

Les organisations devraient aussi disposer de personnes-ressources désignées en matière de confidentialité et de sécurité chez leur fournisseur de services infonuagiques afin que les problèmes, questions et incidents puissent être traités sans délai. Cela est particulièrement important compte tenu des règlements qui obligent les entreprises à signaler les atteintes à la protection de données. Ce type de déclaration d'atteinte à la vie privée est obligatoire dans 47 États américains, ainsi qu'au Canada et maintenant dans l'Union européenne en vertu du nouveau RGPD. Par exemple, presque toutes les provinces exigent la déclaration obligatoire d'atteinte à la vie privée auprès d'un dépositaire de renseignements sur la santé, et la *Loi sur la protection des renseignements personnels numériques* exige maintenant la déclaration des atteintes à la vie privée de la part de toutes les entreprises privées et des entités sous réglementation fédérale (p. ex., les banques). De surcroît, le RGPD tiendra conjointement responsables les utilisateurs de services infonuagiques et leurs fournisseurs des atteintes à la vie privée, celles-ci devant être signalées aux autorités compétentes dans les 72 heures suivant la découverte de l'incident. Il devient donc essentiel que les contrats entre les utilisateurs de services infonuagiques et les fournisseurs traitent des exigences de déclaration des incidents.

Finalement, les organisations devraient utiliser les examens, les évaluations des risques ou les audits pour confirmer que leur fournisseur de services infonuagiques respecte les normes de protection des données énoncées dans leurs contrats. Le RGPD recommande qu'une approche de protection intégrée de la vie privée[4] soit utilisée en incorporant cette protection à toute nouvelle technologie ou à tout nouveau service offerts et en menant des évaluations des risques pour les bases de données à haut risque. Ces évaluations peuvent prendre la forme d'audits exécutés par des tiers et offerts par le fournisseur à ses clients ou d'une évaluation du risque d'un élément de protection intégrée de la vie privée que le fournisseur effectue lui-même. Dans tous les cas, les organisations devront collaborer plus étroitement avec leurs fournisseurs de services infonuagiques afin de préciser les responsabilités de chacun à l'égard de la protection des données et de mettre en place des mécanismes pertinents pour surveiller les activités de leurs fournisseurs, ce qui devrait être décrit dans leurs ententes de service.

[4] La protection intégrée de la vie privée est un cadre qui se fonde sur l'intégration proactive de la protection de la vie privée dans la conception et le fonctionnement des systèmes informatiques, de l'infrastructure des réseaux et des pratiques d'affaires.

www2.deloitte.com/content/dam/Deloitte/ca/Documents/risk/ca-fr-ers-privacy-by-design-brochure.PDF

Étape 3 :

Vos données sont-elles bien protégées?

Explorez différents outils et technologies de chiffrement

Lorsque vous chiffrez des données, vous les rendez illisibles sans la clé de déchiffrement et si elles sont illisibles, les cybercriminels ne se donneront pas la peine de les voler, car elles n'auront aucune valeur sur le marché noir ni pour un tiers[5]

Le chiffrement est un ensemble de technologies matures qui peut être appliqué à une solution infonuagique afin de renforcer les contrôles de sécurité et de confidentialité des données. Les méthodes de chiffrement varient et peuvent être intégrées à des dossiers, à des bases de données et à des applications, selon les besoins. Dans certains cas, le chiffrement peut être effectué directement par le système d'exploitation pour tous les volumes du système. Le chiffrement des données est une caractéristique explicite que votre fournisseur de services infonuagiques peut soutenir au moyen d'un ensemble de services et de mécanismes.

Le chiffrement peut être exploité à de nombreux niveaux, selon vos exigences, vos applications et la méthode que vous souhaitez. Structurellement, vous devrez examiner les mécanismes que vous voulez utiliser pour chiffrer vos données et définir votre stratégie de gestion des clés.

Mécanismes de chiffrement. Ces mécanismes mettent en œuvre l'algorithme de chiffrement réel utilisé pour cacher ou obscurcir les données. La majorité d'entre eux sont fondés sur des algorithmes basés sur des clés, utilisant soit une clé partagée ou une paire de clés publique-privée. Sinon, il est aussi possible d'utiliser la segmentation en unités, un processus qui consiste à substituer aux champs de valeurs précises des valeurs de données anonymes (ce qui peut permettre ou non la récupération des données originales). Ce modèle est utilisé couramment pour les applications telles que CRM (p. ex., Salesforce ou Dynamix) ainsi que pour d'autres applications d'affaires (p. ex., les données de cartes de crédit ou les renseignements liés à la gestion de la main-d'œuvre). La plupart des bases de données permettent maintenant de chiffrer les données qu'elles contiennent, et le déchiffrement sera alors possible uniquement grâce à une application approuvée et aux identifiants d'utilisateurs autorisés. Les appareils de chiffrement offrent aussi une autre méthode, soit le chiffrement des données lors de la déconnexion d'un réseau privé et leur déchiffrement lorsqu'un utilisateur approuvé y accédera.

La méthode de chiffrement que vous choisissez doit s'harmoniser avec les capacités de l'application particulière que vous utilisez ainsi qu'avec le fournisseur de services infonuagiques auquel vous faites appel. L'incidence sur le rendement de l'utilisateur final doit aussi être prise en compte, puisque les différents mécanismes peuvent avoir des répercussions considérables sur l'expérience utilisateur. Les solutions avec appareils, par exemple, requièrent que toutes les données des utilisateurs soient acheminées par l'intermédiaire de l'appareil, ce qui pourrait ne pas convenir à de très grands volumes d'utilisateurs. Le chiffrement du dispositif de l'utilisateur peut entraîner des ralentissements, car la capacité de traitement pourrait être insuffisante.

Stratégie de gestion des clés. Elle porte sur la manière dont vous contrôlez vos clés de chiffrement. Aujourd'hui, de nombreux fournisseurs de services infonuagiques offrent des solutions de gestion des clés, souvent comme partie intégrante d'une gamme plus vaste de services infonuagiques. Le risque que présentent ces solutions, c'est que vous permettez encore à quelqu'un d'autre de contrôler l'accès à l'information. Une approche qui permet de garder le contrôle des clés au sein de votre organisation, que ce soit grâce à une solution de gestion des clés ou à un appareil de chiffrement, peut offrir une meilleure atténuation des risques, en particulier dans les territoires où les lois en matière de localisation des données sont plus strictes.

[5] Forrester. Welcome to the New Era of Encryption, 10 septembre 2015.

Le travail ne s’arrête pas là.

À titre de gardien ou de contrôleur des données, vous devez vous tenir informé de ce qui se passe dans le milieu en constante évolution des règlements et des exigences en matière de confidentialité et de sécurité. Votre stratégie devra évoluer au même rythme que ceux-ci. Il est important d’intégrer des revues régulières à vos cycles de planification en ce qui a trait aux risques et aux TI. La technologie utilisée seule ne suffit pas à vous protéger; vos processus et vos méthodes doivent y être jumelés et évoluer à mesure que les exigences et les menaces se transforment.

Personnes-ressources

Si vous souhaitez discuter des répercussions de la confidentialté des données sur l'informatique en nuage et de la manière dont nous pouvons aider votre organisation, veuillez communiquer avec nous.

À l'échelle nationale

Sylvia Kingsmill
Leader nationale, Protection des données et de la vie privée
skingsmill@deloitte.ca
416-985-1080

Région de l'Est

Amir Belkhelladi
Associé
Services liés aux cyberrisques
abelkhelladi@deloitte.ca
514-393-7035

Robert Masse
Associé
Services liés aux cyberrisques
rmasse@deloitte.ca
514-393-7003

Région de l'Ouest

Jamie Ross
Associé
Services liés aux cyberrisques
jaross@deloitte.ca
250-978-4412

Tejinder Basi
Associé
Services liés aux cyberrisques
tbasi@deloitte.ca
604-640-3255

Pour obtenir plus d'information sur les solutions d'informatique en nuage, veuillez communiquer avec l'une des personnes suivantes :

David Brassor
Directeur de pratique, Consultation
dbrassor@deloitte.ca
416-874-3150

David Woelfle
Leader principal, Consultation
dwoelfle@deloitte.ca
416-601-6023

Notes

www.deloitte.ca

Deloitte, l'un des cabinets de services professionnels les plus importants au Canada, offre des services dans les domaines de la certification, de la fiscalité, de la consultation et des conseils financiers. Deloitte S.E.N.C.R.L./s.r.l., société à responsabilité limitée constituée en vertu des lois de l'Ontario, est le cabinet membre canadien de Deloitte Touche Tohmatsu Limited.

Deloitte désigne une ou plusieurs entités parmi Deloitte Touche Tohmatsu Limited, société fermée à responsabilité limitée par garanties du Royaume-Uni, ainsi que son réseau de cabinets membres dont chacun constitue une entité juridique distincte et indépendante. Pour obtenir une description détaillée de la structure juridique de Deloitte Touche Tohmatsu Limited et de ses sociétés membres, voir www.deloitte.com/ca/apropos.

Conçu et produit par le Service de conception graphique de Deloitte, Canada. 16-3723V