大成 DENTONS

Résidence des données pour les entreprises canadiennes – Le nouveau risque pour la vie privée et comment le gérer

Pleins feux sur les sociétés canadiennes

Le jeudi 8 avril 2021
De midi à 13 h HE (webinaire en anglais)
De 13 h à 14 h HE (webinaire en français)

Vos conférenciers

Chantal Bernier
Avocate-conseil
chantal.bernier@dentons.com

Chantal Bernier dirige le groupe de pratique canadien Cybersécurité et protection de la vie privée de Dentons et est membre du groupe Affaires et politiques gouvernementales du cabinet.

Elle conseille des entreprises nationales et internationales de premier plan dans le cadre de l'expansion de leurs activités au Canada et en Europe, de leur entrée sur le marché du commerce électronique, de la mise en place d'outils d'analyse des données et du déploiement d'initiatives de mise en marché fondées sur les données.

Elle compte parmi ses clients des sociétés de technologies publicitaires, des institutions financières, des sociétés de biotechnologie, des entreprises spécialisées dans l'analyse des données et des institutions gouvernementales.

Christophe Fichet
Associé
christophe.fichet@dentons.com

Christophe Fichet est associé responsable de la pratique TMT du bureau de Paris.

Christophe a développé une expertise sectorielle de pointe dans le domaine des infrastructures (actives/passives) et des services de communications électroniques en France ainsi qu'en Afrique et au Moyen-Orient, au service de groupes internationaux du secteur, de banques conseil ou d'investissement et de fonds et d'organismes prêteurs internationaux comme la Banque Mondiale.

Il conseille régulièrement des gouvernements et des autorités de régulation dans le cadre de réformes du secteur, de procédures d'attribution de licences ou de privatisations dans de nombreux pays.

Quel est le problème?

- Les autorités de réglementation et les consommateurs se concentrent de plus en plus sur les risques pour la vie privée liés au lieu de stockage des données personnelles :
  - En juillet 2020, les organisations américaines ont perdu la possibilité de recevoir, de traiter et de stocker des données personnelles soumises au RGPD via l'accord conclu entre la Commission Européenne et la Federal Trade Commission, de sorte que les responsables de traitement soumis au RGPD ne peuvent plus transférer de données personnelles directement ou indirectement (en ce compris via le Canada) à un organisme récipiendaire américain en vertu du Privacy Shield.
  - Les cyberattaques sont clairement liées à certains pays – les autorités de réglementation s'attendent à ce que les entreprises canadiennes en tiennent compte au moment de choisir des fournisseurs de services
  - La population s'oppose de plus de plus au stockage de données dans les pays qui ne respectent pas le droit fondamental à la vie privée

Quels sont les risques liés à la confidentialité des données?

- Risque réglementaire : Si vous (i) collecter et traitez directement ou (ii) recevez de partenaires ou de clients, des données personnelles soumises au RGPD et que vous les stockez aux États-Unis, vous vous exposez (i) dans le premier cas à des des risques de non-conformité au regard du RGPD et (ii) dans le second cas à des risques de responsabilité contractuelle vis-à-vis desdits partenaires qui sont et demeurent responsables du traitement des données vis-à-vis des personnes concernées.
- Risque pour la sécurité : Si vous transférez des données vers des pays qui ne se soucient guère de la sécurité des données, vous augmentez le risque de manquement aux obligations de protection des données et à l'obligation de responsabilisation qui incombent aux responsables de traitement et dans une certaine mesure aux sous-traitants
- Risque pour la réputation : Si vous stockez des données dans des pays qui ne respectent pas la vie privée, vous risquez de perdre des clients

Comment nous souhaitons aborder le sujet aujourd'hui :

1. Description des règles sur la résidence des données qui s’appliquent directement et indirectement aux entreprises canadiennes

2. Présentation de solutions concrètes

Ce dont il ne sera pas question :

Règles sur la résidence des données qui s’appliquent aux institutions publiques et à leurs fournisseurs de services

Identification du risque réglementaire

- Actuellement :
  - Le Règlement général sur la protection des données (« RGPD ») prohibe sauf dérogations spécifiques et restrictives le droit de transférer des données à carcatère personnel à l'extérieur de l'Espace Economique Européen
  - Le 16 juillet 2020, la Cour de justice de l'Union européenne a encore davantage restreint ces transferts hors EEE vers les pays n'offrant pas un degré de protection équivalent à celui applicable au sein de l'EEE
  - Selon les lignes directrices du CPVP et du BSIF, les organisations doivent accorder une attention particulière aux facteurs qui peuvent « réduire la capacité du fournisseur de services étranger » de protéger les renseignements personnels
- Dans l'avenir :
  - Le projet de loi 64 du Québec propose d'exiger une évaluation des facteurs relatifs à la vie privée avant tout transfert de données personnelles à l'extérieur du Québec
  - Le projet de loi canadien C-11 (*Loi sur la protection de la vie privée des consommateurs*) vise à officialiser l'obligation d'informer les particuliers du transfert transfrontalier
  - Le Canada négocie actuellement avec l'UE le droit des entreprises régies par la LPRPDE de recevoir des données personnelles de l'UE

Résidence des données en vertu du RGPD

- L'article 44 interdit à tout responsable de traitement ou sous-traitant, au sens du RGPD, tout transfert de données à caractère personnel à l'extérieur de l'Espace Economique Européen, y compris les transferts ultérieurs de données du pays destinataire vers un pays tiers, **sauf** si des « garanties appropriées » sont en place, telles que :
  - Le « pays importateur » a reçu le statut « Adéquat » de la Commission européenne pour son régime de confidentialité (seuls 12 pays possèdent ce statut); **OU**
  - Le transfert entre organisations est soumis à des clauses contractuelles types (CCT) approuvées par la Commission européenne; **OU**
  - Le transfert au sein d'une société et des membres de son groupe est assujetti à des « règles d'entreprise contraignantes » (REC) approuvées; **OU**
  - L'individu a expressément consenti au transfert de données transfrontalier (cas ultime extrêmement contraignant pour le faire admettre)

Ce que cela signifie pour les entreprises canadiennes

1. Les entreprises régies par la LPRPDE du Canada (loi fédérale) peuvent recevoir des données personnelles de responsable de traitement (ou sous traitant) soumis au RGPD sans autre autorisation parce que l'UE a reconnu que la LPRPDE offrait un niveau de protection adéquat
2. Les entreprises qui relèvent exclusivement d'une loi provinciale sur la protection de la vie privée – la PIPA de la C.-B., la PIPA de l'Alberta ou la *Loi sur la protection des renseignements personnels* du Québec – ne peuvent pas recevoir de données personnelles de l'UE sauf exception (CCT, REC ou consentement) parce que ces lois n'ont pas été reconnues par l'UE comme offrant un niveau de protection adéquat
3. Les États-Unis n'ont pas le statut de pays adéquat

Qu’en est-il du bouclier de protection des données UE-États-Unis?

- Le « Bouclier de protection des données » a été invalidé par la décision de la Cour de justice de l’UE (CJUE) du 16 juillet 2020, communément appelée Schrems II
- La CJUE a jugé que le cadre légal en vigueur aux Etats-Unis permettait la surveillance de masse sans offrir de protection adéquate

PAR CONSÉQUENT

- Les entreprises américaines ne peuvent plus utiliser la certification en vertu du bouclier de protection des données UE-États-Unis pour recevoir des données personnelles soumises au RGPD
- Les responsables de traitement et les sous-traitants de données personnelles au sens du RGPD ne peuvent plus transférer les données personnelles à des organisations soumises au droit américain en se fondant sur le bouclier de protection des données
- Les organisations canadiennes recipiendaires de données personnelles tombant dans le champ d’application du RGPD doivent respecter les obligations contractuelles que leur imposent les responsables de traitement (voire les sous traitants) de données personnelles

L’argument décisif

- En plus d’invalider le bouclier de protection des données UE-États-Unis, la CJUE
  - Reconnaît la validité des Clauses Contractuelles Types (« CCT »); **mais**
  - Oblige les organisations concernées à renforcer les CCT pour s’assurer que leur mise en œuvre n’est pas compromise dans le pays de destination

- La responsabilité d’évaluer la protection des données personnelles dans le pays de destination incombe ainsi aux organisations, responsables du traitement de données personnelles concerné (ou sous-traitant) –au sens du RGPD, qui les transfèrent

Qu’en est-il du Brexit?

- 19 février 2021 : projet de décision de la Commission de l’UE d’accorder le statut « Adéquat » au Royaume-Uni

- Quel est l’avenir de la protection des données au Royaume-Uni?
  - Probablement une application de plus en plus pragmatique du RGPD
  - Pour en savoir plus, consultez notre webinaire sur le RGPD à l’intention des avocats-conseils nord-américains : https://www.dentons.com/en/whats-different-about-dentons/connecting-you-to-talented-lawyers-around-the-globe/events/2021/january/21/gdpr-in-practice-for-north-american-companies

Si ce n’est pas possible…

- D’autres garanties et dérogations alternativement disponibles, sous conditions, pour transférer des données hors de l’UE

5 options envisageables

Option 1 : Trouver des fournisseurs de services qui stockent des données au Canada

« *La question est la suivante, en tant qu'entreprise, dois-je transférer des données vers des pays tiers si la Commission européenne n'a pas rendu de décision relativement au niveau de protection qu'offrent les lois des pays en question? Oui ou non? C'est la question fondamentale*. »
(traduction libre)

Juge von Danwitz, CJUE

Mais le stockage au Canada n'est peut-être pas pratique…

Si ce n’est pas possible, se tourner vers les « autres garanties » prévues par le RGPD

« L'invalidation du bouclier de protection des données UE-États-Unis ne crée pas de vide juridique, car les garanties de l'article 46 et les dérogations de l'article 49 s’appliquent en l'absence d’une décision sur le niveau de protection qu’offrent les lois américaines. » (traduction libre)

Juge von Danwitz, CJEU, discours prononcé lors de la Journée de la protection des renseignements personnels, 28 janvier 2021

- Le responsable de traitement (ou le sous-traitant, si applicable) reste responsable de tout re-transfert (du Canada par exemple) des données initialement collectées.
- Des conditions contractuelles commerciales sont à envisager, si l’entreprise canadienne récipiendaire des données compte les re-transférer aux États-Unis notamment.

Option 2 : CCT – Négociation d'addenda pour les accords de services (AS) déjà conclus – Article 46

- De nouvelles CCT sont sur le point de sortir (notamment pour le cas sous-traitant canadien à sous-traitant américain)
- D'ici là, les CCT actuelles constituent une garantie valable si elles comprennent des clauses supplémentaires pour répondre aux préoccupations de l'UE concernant l'accès des États aux données de l'UE, telles que :
  - Mesures technologiques :
    - Cryptage pour protéger les données de la surveillance de l'État
    - Chiffrement de bout en bout pour faire valoir que les données ne sont pas « sous le contrôle » de l'organisation, de sorte que ladite organisation ne peut être contrainte de les produire
    - Possibilité d'alerter l'organisme qui effectue le transfert de la demande d'accès de l'État sans violer l'interdiction de de communication
  - Mesures organisationnelles :
    - Politique interne pour contester toutes les demandes d'accès des États aux données couvertes par le RGPD
    - Cartographie des données pour évaluer et atténuer les risques particuliers
    - Réalisation d'une AIPD ou d'une EFVP avant un transfert transfrontalier
  - Surveillance de la conformité :
    - Politique et lignes directrices en matière de diligence raisonnable pour choisir des fournisseurs de services
    - Renforcement des audits
    - Obligation de consulter la société qui effectue le transfert sur réception de la demande d'accès de l'État en l'absence d'une interdiction de communication

Option 3 : Intégrer le consentement au transfert de données transfrontalier dans le consentement à recevoir des services (article 49)

- Le consentement explicite des individus dont les données personnelles sont traitées peu permettre ultimement et dans des conditions très restrictives - qu'il faut pouvoir dument justifier - le transfert transfrontalier de données à caractère personnel
- Le consentement doit être explicite, exprès et éclairé, et ne peut conditionner la fourniture du service ou du produit concerné
- Les garanties nécessaires dans le pays de destination devront être fournies et justifiées à tout moment

Option 4 : Dérogations au titre de l'article 49

- L'article 49 apporte des dérogations à l'interdiction du transfert transfrontalier de données personnelles lorsque ledit transfert est :
  - Nécessaire à l'exécution du contrat avec l'individu concerné
  - Dans l'intérêt de la personne ou nécessaire à la sauvegarde des intérêts vitaux de la personne
  - Dans l'intérêt public
  - Nécessaire à la défense de droits en justice
  - A lieu au départ d'un registre qui est ouvert à la consultation du public
- Toutes ces dérogations s'appliquent à des situations particulières, limitées et très restrictives :
  - Si le transfert transfrontalier est « vraiment essentiel » au respect du contrat avec le particulier, encore faut-il que :
    - Il ne soit pas « répétitif »
    - Il s'applique à un nombre limité de personnes
    - Il est accompagné de garanties appropriées

Option 5 : Autres garanties en vertu de l’article 46

- **Règles d’entreprise contraignantes** :
  - Utilisées principalement par les multinationales possédant des filiales dans le monde entier e.g. Amex
  - « Règles d’entreprise contraignantes » (REC) approuvées par l’Autorité de protection des données compétente
- **En voie de développement** :
  - Code de conduite approuvé par des associations industrielles comportant des engagements exécutoires en matière de protection des données
  - Mécanismes de certification de la protection des données comportant des engagements exécutoires en matière de protection des données

Comment choisir entre les options : Rationaliser le transfert transfrontalier de données de l'UE

- Passer en revue les lieux de stockage des données de tous les fournisseurs de services
- Effectuer une évaluation de l'impact du transfert
- Selon le lieu de stockage des données, classer les fournisseurs de services en fonction du risque :
  - Aucun impact à considérer (p. ex., le fournisseur de services stocke toutes les données au Canada ou en Europe) : aucune autre mesure contractuelle nécessaire
  - Impact à prendre en compte (p. ex., le fournisseur de services stocke des données aux États-Unis) : négocier un addenda à l'AS pour inclure des CCT renforcées
  - Impact significatif (p. ex. le fournisseur de services stocke des données dans un pays qui n'a pas adopté de lois sur la protection de la vie privée et la sécurité des données ou dont les lois en matière ne sont pas efficaces) : réévaluer les contrats, négocier un addenda à l'AS, accepter le risque ou choisir un autre fournisseur de services

Guide de Dentons pour les transferts de données internationaux - L'outil d'évaluation de l'impact du transfert

https://www.dentons.com/en/insights/articles/2021/february/2/the-dentons-transfer-impact-assessment-tool

1. Orientation
   - Phase de préparation - évaluation de la sensibilité au risque interne et établissement des priorités
2. Solutions immédiates
   - Protections et garanties contractuelles à court terme pour les « projets à mi-parcours » et les « urgences »
3. Cartes de flux / transfert de données
   - Cartographie des flux de données, y compris les types de transfert, les lieux et les outils de transfert en place
   - Évaluation des autres outils de transfert de données / dérogations
4. Évaluation de la législation locale
   - Évaluation standard du risque lié au niveau de protection offert par les lois locales par rapport aux normes de l'UE et du Royaume-Uni
   - Questionnaires destinés aux fournisseurs pour confirmer la validité de l'évaluation et/ou confirmer les mesures supplémentaires prises par le fournisseur
5. Phase d'évaluation
   - Évaluation des risques identifiés au niveau des lois locales/des fournisseurs et détermination des mesures supplémentaires requises
   - Enregistrement de l'évaluation de l'impact du transfert, enregistrement de la cartographie, évaluation des outils de transfert et résultats en tant qu'outil de responsabilisation
   - Conception des mesures techniques, organisationnelles et contractuelles supplémentaires requises
6. Exigences procédurales
   - Mise à jour des garanties contractuelles et mise en œuvre de solutions politiques et techniques supplémentaires
7. Réévaluation
   - Processus régulier de réévaluation de l'efficacité des outils de transfert et des mesures supplémentaires
8. Processus d'approvisionnement courant
   - Processus et procédures de diligence des fournisseurs standards pour l'intégration de nouveaux fournisseurs / le renouvellement de contrats avec des fournisseurs et création de modèles de mises à jour contractuelles

Conclusion pour les entreprises canadiennes

- Si vous avez le choix de stocker des données de l'UE au Canada, votre vie sera plus simple
- Si vous n'avez pas ce choix :
  - Passez en revue les lieux de stockage des données de l'UE utilisés par vos fournisseurs de services
  - Évaluez le risque pour chaque lieu / fournisseur de services
  - Protégez-vous avec les clauses contractuelles appropriées
  - Adoptez des politiques d'approvisionnement pour gérer les risques liés au transfert transfrontalier

Qui peut vous aider?

Paris
- Christophe Fichet
  christophe.fichet@dentons.com

Calgary
- Elizabeth Allum
  elizabeth.allum@dentons.com
- Kelly Osaka
  kelly.osaka@dentons.com

Edmonton
- Jaclin Cassios
  jaclin.cassios@dentons.com
- Tom Sides
  tom.sides@dentons.com

Montréal
- Alexandra Quigley
  alexandra.quigley@dentons.com
- Guillaume Savard-Fouquette
  guillaume.savard@dentons.com

Ottawa
- Chantal Bernier
  chantal.bernier@dentons.com
- Charmaine Borg
  Charmaine.borg@dentons.com
- Julia Dales
  julia.dales@dentons.com
- Anca Sattler
  anca.sattler@dentons.com

Toronto
- Luca Lucarini
  luca.lucarini@dentons.com
- Tracy Molino
  tracy.molino@dentons.com
- Karl Schober
  karl.schober@dentons.com
- Chloé Snider
  chloe.snider@dentons.com
- Kirsten Thompson
  kirsten.thompson@dentons.com

Vancouver
- Arik Broadbent
  arik.broadbent@dentons.com
- Taylor Buckley
  taylor.buckley@dentons.com
- Facchin, Julie
  julie.facchin@dentons.com
- David Wotherspoon
  david.wotherspoon@dentons.com

Merci.

Chantal Bernier
Avocate-conseil
chantal.bernier@dentons.com

Christophe Fichet
Associé
christophe.fichet@dentons.com