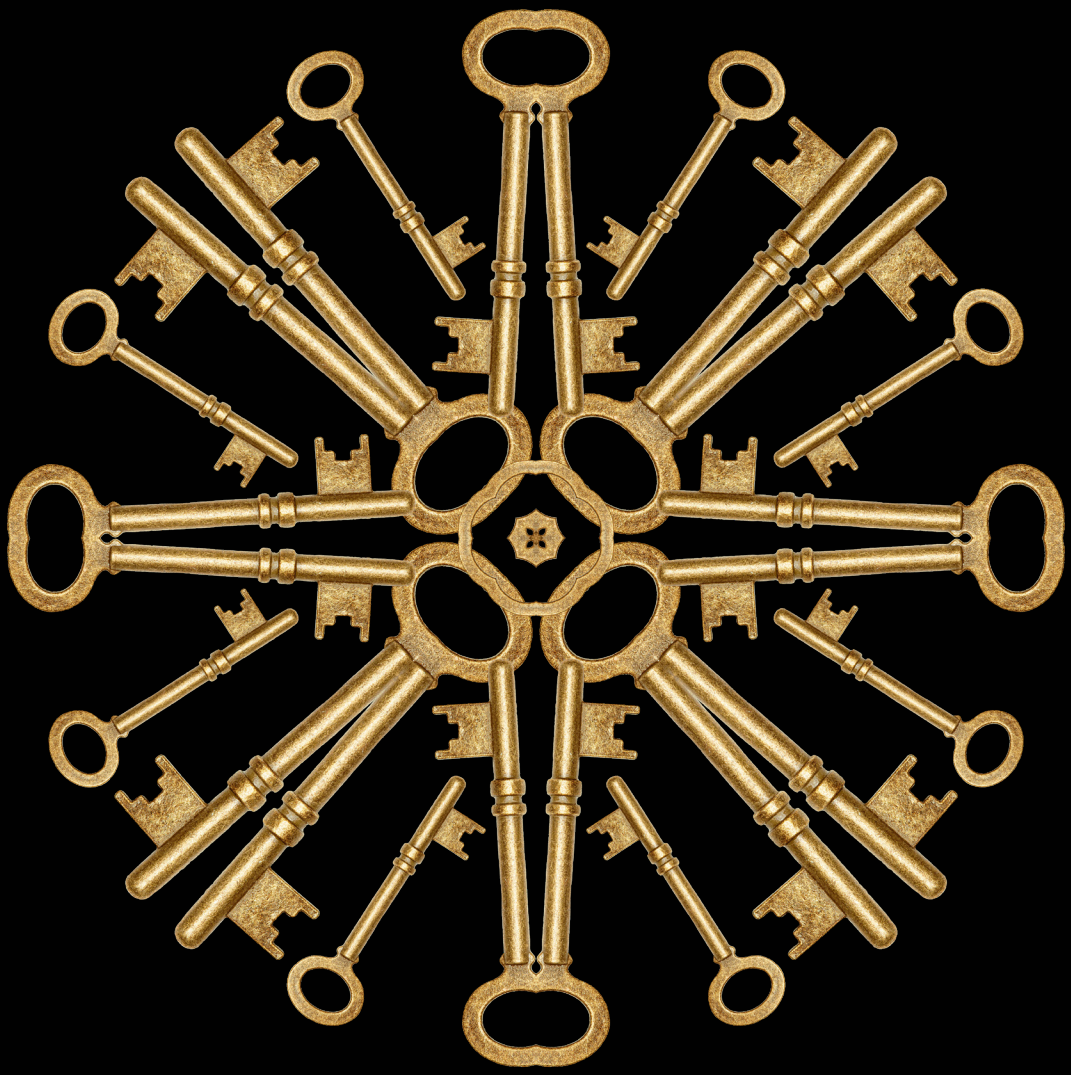
Deloitte.



# Le RGPD et les organisations canadiennes : des défis importants à relever

Cyberrisques

La réglementation sur la protection des données que l'on qualifie souvent de plus stricte au monde entrera pleinement en vigueur dans quelques mois à peine. Le Règlement général sur la protection des données (RGPD) de l'Union européenne, bien qu'il émane de l'étranger, touchera toutes les organisations canadiennes qui traitent des données à caractère personnel de personnes se trouvant dans l'Union européenne. Elles doivent par conséquent s'y préparer.

Le RGPD renforce les droits des personnes à l'égard de leurs données personnelles, établissant un seuil plus élevé tant pour la transparence que pour le consentement. Toute organisation qui recueille, utilise, stocke, communique ou traite les données à caractère personnel de toute personne résidant dans l'Union européenne (UE) – sans égard à sa citoyenneté ou au lieu où est établi le siège social de l'organisation – sera assujettie au RGPD. Cette situation est très sérieuse : les sanctions financières en cas de non-respect du règlement vont jusqu'à 20 millions d'euros ou quatre pour cent du chiffre d'affaires mondial annuel de l'organisation, le montant le plus élevé étant retenu.

Approuvé par le Parlement européen en avril 2016, le RGPD entrera en vigueur le 25 mai 2018. La période de grâce accordée pour se préparer à la pleine conformité tire à sa fin, et les sociétés qui ne sont pas prêtes pourraient bientôt ressentir les effets de ces lourdes amendes.

# Incidence sur les entreprises canadiennes

Outre ses objectifs de renforcer les droits des personnes à l'égard de leurs données à caractère personnel et d'harmoniser les exigences liées à la protection des données dans l'ensemble de l'UE, le RGPD représente un nouvel ensemble d'exigences législatives qui touchent directement les organisations canadiennes. L'un de ses aspects les plus pertinents est le principe d'extraterritorialité : le règlement s'appliquera aux organisations du monde entier qui traitent les données à caractère personnel de personnes se trouvant dans l'UE, sans égard à la citoyenneté de la personne ou au lieu où l'organisation est établie.

Autrement dit, qu'une organisation soit physiquement présente ou non dans l'UE, elle sera tenue de respecter le RGPD si elle offre des produits ou des services à des personnes se trouvant dans l'UE. Par exemple, un détaillant canadien qui n'a pas de bureaux ni de magasins sur le territoire de l'UE, mais qui recueille quand même, par l'intermédiaire de ses sites web ou de ses applications mobiles, des données à caractère personnel de clients se trouvant dans l'UE sera tenu de respecter le RGPD.

Pour bien comprendre leurs obligations de conformité, les entreprises canadiennes visées par le RGPD devront définir les exigences qui dépassent la portée des lois canadiennes actuelles en matière de protection de la vie privée, comme la Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE), et s'y conformer. Les mesures précises devront être évaluées au cas par cas, mais nous donnons ici un aperçu des principaux aspects de la conformité et nous proposons des solutions potentielles pour surmonter les difficultés.

## 1. Responsabilisation

Les efforts de responsabilisation que les organisations canadiennes ont déployés jusqu'à maintenant pour s'assurer de respecter les lois canadiennes sur la protection de la vie privée devront dans de nombreux cas être intensifiés pour répondre aux exigences obligatoires du RGPD. Plus particulièrement, les organisations qui sont assujetties au règlement seront bientôt tenues de démontrer leur conformité et de faire preuve de transparence à cet égard. Ainsi, beaucoup devront élargir leurs pratiques actuelles de protection de la vie privée afin d'inclure clairement la protection des renseignements à caractère personnel de leurs clients et employés qui se trouvent dans l'Union européenne.

Les organisations doivent par ailleurs mettre en œuvre un cadre de responsabilisation régissant le traitement des données à caractère personnel, ou rehausser celui qu'elles possèdent déjà, afin d'instaurer une culture de protection de la vie privée dans l'ensemble de l'entreprise. Ce cadre permettra à l'organisation de s'assurer qu'elle consigne et conserve des dossiers sur les mesures techniques et organisationnelles qu'elle utilise dans le but de protéger les données à caractère personnel. Par exemple, elle doit consigner les rôles et responsabilités liés à la protection de la vie privée, élaborer et mettre en œuvre des politiques et des processus internes et externes en matière de protection de la vie privée, tenir à jour un registre des activités de traitement des données, pouvoir démontrer que des évaluations des facteurs relatifs à la protection de la vie privée sont effectuées et documentées avant l'utilisation de nouvelles technologies, et vérifier la présence des employés aux séances de formation sur la protection de la vie privée.

Les principales mesures de protection de la vie privée que les organisations canadiennes n'étaient tenues de respecter qu'en vertu de la législation sectorielle canadienne ou qui étaient généralement recommandées comme meilleures pratiques constitueront désormais des obligations juridiques au titre du RGPD. C'est le cas des mesures suivantes :

- **Nommer un délégué à la protection des données :** les organisations dont les activités de base comprennent le suivi régulier ou systématique de données à caractère personnel ou le traitement de données à grande échelle doivent embaucher un délégué à la protection des données. Celles qui ne sont pas physiquement présentes dans l'UE, mais qui traitent quand même les données de personnes concernées de l'UE doivent désigner un représentant qui agira en leur nom au sein de l'UE.

- Effectuer des évaluations des facteurs relatifs à la protection de la vie privée (EFVP) : les organisations canadiennes doivent effectuer une EFVP avant d'exécuter toute opération de traitement de données susceptible d'occasionner un risque élevé pour les droits et libertés des personnes concernées de l'UE, comme le transfert d'information dans le nuage ou des activités d'analytique des données. Elles doivent également consigner la façon dont les recommandations de l'EFVP seront intégrées dans la mise en œuvre du projet. De plus, si l'EFVP indique qu'il existe un risque élevé, l'organisation doit consulter l'autorité de contrôle correspondante de l'UE et intégrer ses recommandations dans la solution ou le projet final avant de procéder au lancement.
- Tenir un registre des activités de traitement des données : bien qu'il existe des exemptions légales, les organisations canadiennes doivent, en règle générale, créer et tenir à jour un registre de certaines activités de traitement de données, en consignant notamment l'objectif du traitement, les catégories de données, les catégories de destinataires des données ainsi que les périodes de conservation. Elles peuvent à cette fin créer des inventaires des données et effectuer des exercices de mise en correspondance qui leur fourniront une bonne visibilité de leurs données. Savoir exactement où les données sont stockées dans l'organisation et où elles seront conservées après avoir été communiquées à des tiers constitue la première étape de la conception et de la mise en œuvre de stratégies appropriées de protection des données.
- Protéger les données à caractère personnel par défaut et dès la conception : les entreprises ne peuvent recueillir, partager et stocker que la quantité minimale d'information requise pour les fins prévues, et elles doivent utiliser des techniques de pseudonymisation dès que possible. Elles doivent par ailleurs pouvoir démontrer que la « protection des données par défaut » se situe au cœur de la conception de leurs produits, services ou applications. La « protection intégrée de la vie privée » est démontrée lorsqu'une solution est configurée de manière à ce que les paramètres par défaut protègent la vie privée de l'utilisateur, ou lorsque les documents architecturaux ou techniques indiquent que la confidentialité constituait une condition préalable à l'étape de la conception.

Le RGPD élargit plusieurs des exigences déjà imposées par la LPRPDE, notamment les suivantes :

- Sécurité : les organisations canadiennes doivent mettre en place des mesures de sécurité appropriées selon le risque, la nature, la portée, le contexte et les objectifs du traitement des données. Au-delà de cette obligation générale, quatre solutions sont expressément mentionnées :
  - pseudonymisation et cryptage;
  - confidentialité, intégrité, disponibilité et résilience continues des systèmes et des services;
  - capacité de rétablir rapidement la disponibilité des données à caractère personnel et l'accès à celles-ci en cas d'incident physique ou technique;
  - évaluations et tests réguliers de l'efficacité des mesures.
- Responsabilité de tiers : tout tiers qui traite des données à caractère personnel de personnes concernées de l'UE pour le compte d'une autre organisation est également tenu de respecter le RGPD. Dans le cas des organisations canadiennes, cela signifie qu'elles devront évaluer les tiers qui traitent en leur nom les données de personnes concernées de l'UE et s'assurer qu'ils respectent le règlement. De plus, les organisations qui n'exercent pas d'activités dans l'UE ou n'offrent pas de produits ou de services à des personnes concernées de l'UE, mais qui traitent quand même des données de personnes concernées pour le compte d'une autre organisation, relèveraient du champ d'application du RGPD.

Tout tiers qui traite des données à caractère personnel de personnes concernées de l'UE pour le compte d'une autre organisation est également tenu de respecter le RGPD.

## 2. Transparence

Les récentes modifications imposées à la LPRPDE par la Loi sur la protection des renseignements personnels numériques exigent une norme de transparence plus élevée de la part des organisations canadiennes, notamment l'utilisation d'un langage clair et simple pour communiquer les demandes de consentement. Les exigences de notification aux personnes touchées par une violation sont élargies. Elles imposent d'aviser également le Commissariat à la protection de la vie privée et prévoient l'obligation de tenir à jour un registre des atteintes à la protection des données.

Les organisations canadiennes qui ont récemment révisé leurs énoncés de confidentialité et leurs programmes d'intervention en cas d'atteinte à la sécurité des données pour s'assurer de respecter la Loi sur la protection des renseignements personnels numériques devront mettre à jour ces énoncés et programmes afin de se conformer au RGPD, de deux façons en particulier :

- Transparence des opérations de traitement des données : les organisations devront expliquer, dans un langage concis, transparent et clair, les renseignements à caractère personnel qu'elles recueillent, utilisent et communiquent, les pays dans lesquels leur traitement est effectué, les mesures qui sont prises pour les protéger ainsi que les droits des clients et des employés à l'égard de leurs renseignements. Elles peuvent utiliser des vidéos, des tutoriels, des blogues et des schémas pour assurer ce niveau de transparence.
- Notification en cas de violation : lorsqu'une atteinte à la protection des données est susceptible d'occasionner un risque pour les droits et libertés des personnes, les organisations sont tenues de la signaler à l'autorité de contrôle appropriée dans un délai de 72 heures, de même qu'aux personnes qui sont concernées dans les meilleurs délais. Elles doivent par ailleurs consigner toute atteinte à la sécurité des données à caractère personnel, notamment les faits, les répercussions et les mesures correctives qui ont été prises.

### 3. Consentement et autres motivations juridiques

En vertu de la LPRPDE, les organisations canadiennes peuvent demander le consentement exprès ou implicite, selon le degré de confidentialité des renseignements personnels et les attentes raisonnables de la personne. De même, le RGPD exige l'obtention du consentement exprès pour effectuer le traitement de renseignements à caractère personnel lorsque l'organisation n'a pas d'autres motifs valables de les traiter.

Plus particulièrement, le règlement exige que les organisations évaluent leurs activités liées à la protection des données et s'assurent que ces activités reposent sur l'une des motivations juridiques suivantes :

- Consentement univoque par un acte positif clair : les organisations doivent obtenir le consentement des personnes concernées de l'UE, qui doit être manifesté de façon libre, spécifique, éclairée et univoque (comme cocher une case sur un site web). Le système ou l'application de l'organisation doit par ailleurs pouvoir consigner les options de consentement, et un consentement parental vérifiable est exigé si le traitement vise les données de personnes mineures.
- Autres motivations juridiques du traitement : il arrive que des données puissent être recueillies et traitées sans consentement en cas de conformité à un ensemble limité de critères (p. ex., exécution d'un contrat, obligation légale, intérêt vital de la personne concernée, ou intérêt public).

Il est essentiel que les organisations évaluent et consignent les motivations juridiques qui rendent légitime l'ensemble de leurs activités actuelles de traitement des données. Cet exercice leur permettra de déterminer les finalités de traitement qui s'appuient uniquement sur le consentement de la personne (comme l'utilisation des données à caractère personnel aux fins d'activités de profilage) et qui créent par conséquent la nécessité d'obtenir et de gérer le consentement univoque et positif de la personne concernée.

### 4. Octroi de droits nouveaux et renforcés

Les organisations canadiennes qui, conformément à la LPRPDE, accordent aux particuliers les droits d'accéder à leurs renseignements personnels et de les corriger doivent tenir compte des nouveaux droits intégrés dans le RGPD, droits qui visent à permettre aux personnes concernées de l'UE de mieux comprendre et de contrôler leurs renseignements à caractère personnel, et qui comprennent les suivants :

- Droit à l'effacement ou « droit à l'oubli » : les personnes concernées peuvent demander aux organisations d'effacer leurs données personnelles.
- Droit d'opposition au traitement des données : les personnes concernées peuvent s'opposer au traitement de leurs données personnelles, notamment le traitement automatisé et le profilage.
- Droit à la portabilité des données : les entreprises doivent fournir aux personnes concernées les données personnelles qu'elles détiennent à leur sujet, dans un format couramment utilisé et lisible par machine, et les transmettre à une autre organisation sur demande.

Le RGPD comprend également des dérogations légales qui empêcheraient les organisations d'accorder des droits individuels. Par conséquent, il est essentiel que les organisations canadiennes développent des processus pour accorder ces droits en tenant compte des cas où les dérogations légales s'appliquent. Elles doivent ensuite examiner les fonctionnalités des systèmes, des outils et des logiciels utilisés pour traiter les données des personnes concernées de l'UE afin de s'assurer qu'ils permettent la mise en œuvre des droits susmentionnés. Ces fonctionnalités pourraient inclure l'épuration des données, des capacités d'anonymisation ainsi que des mécanismes d'extraction et d'exportation de données.

### 5. Transferts transfrontaliers de données

Les organisations canadiennes qui transfèrent en dehors de l'UE les données des personnes concernées de l'UE doivent s'assurer que le transfert se fait vers l'un des pays ayant fait l'objet d'une décision de la Commission européenne constatant qu'il assure un niveau de protection adéquat, comme le Canada. Autrement, un mécanisme de protection des données adéquat doit être en place (p. ex., clauses contractuelles types, règles d'entreprise contraignantes, bouclier de protection des données, consentement).

En pratique, les organisations canadiennes qui ont recours à des tiers spécialistes en traitement des données (comme des solutions CRM ou des fournisseurs d'infonuagique) situés aux États-Unis constituent un exemple courant. En plus de s'assurer que les tiers respectent le RGPD et que les ententes touchant la prestation de services renferment des dispositions adéquates en matière de confidentialité et de sécurité, elles doivent déterminer dans quels cas il n'existe pas de mécanismes validés de transfert de données, puisque cela signifierait que le traitement de données à caractère personnel de personnes concernées de l'UE est illicite.

Il convient par ailleurs de souligner que la décision de la Commission européenne relative au niveau adéquat de protection du Canada n'est que partielle, étant donné que la LPRPDE s'applique uniquement aux employeurs qui sont des « entreprises fédérales » et n'offre donc pas de protection équivalente pour les données personnelles des employés. Par conséquent, les organisations du secteur privé qui sont assujetties à la LPRPDE doivent toujours examiner les clauses types et les règles d'entreprise contraignantes avant de transférer vers le Canada les renseignements à caractère personnel de leurs employés établis dans l'UE.

Le RGPD comprend également des dérogations légales qui empêcheraient les organisations d'accorder des droits individuels. Par conséquent, il est essentiel que les organisations canadiennes développent des processus pour accorder ces droits en tenant compte des cas où les dérogations légales s'appliquent.

### 6. Instabilité du contexte de réglementation lié à la protection de la vie privée

Le RGPD vise principalement à harmoniser les exigences de confidentialité et de protection des données dans l'ensemble de l'UE, mais il contient quand même des clauses ouvertes qui permettent aux États membres de l'UE d'ajouter des variations locales à leurs lois nationales sur la protection des données relativement à des sujets préétablis, comme l'âge requis pour consentir et le traitement des données à caractère personnel des employés. Les États membres de l'UE s'emploient actuellement à présenter et à adopter des projets de loi qui visent à modifier leurs lois nationales sur la protection des données de façon à les harmoniser avec le RGPD. Dans de nombreux cas, les différences entre les pays qui résultent des clauses ouvertes sont encore floues.

Les organisations canadiennes devront par ailleurs prêter attention à un autre règlement de l'UE qui aura des répercussions extraterritoriales : le règlement à venir sur le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques. Ce nouveau règlement devrait remplacer la directive actuelle de l'Union européenne relative à la vie privée et aux communications électroniques dont l'objet est de réglementer la protection de la vie privée dans les réseaux électroniques. Il servira de complément et de supplément au RGPD.

**En prévision de la mise en application du Règlement général sur la protection des données en mai 2018, nous encourageons toutes les organisations canadiennes concernées à prendre les mesures suivantes :**

- Déterminer dans quelle mesure le règlement s'applique à leurs activités.
- Établir un registre des activités de traitement des données qui leur fournira de l'information sur les données à caractère personnel qu'elles sont tenues de protéger, comme les motivations juridiques et les mesures de sécurité qui soutiennent chaque activité de traitement.
- Passer en revue les politiques de confidentialité existantes et s'assurer que les principaux aspects de la conformité au RGPD y sont inclus (p. ex., la base juridique du traitement, les transferts vers des pays tiers, l'existence de la prise de décision automatisée).
- Effectuer une évaluation des lacunes afin de déterminer les pratiques de confidentialité existantes qui peuvent être mises à profit pour assurer la conformité au RGPD.
- Passer en revue les contrats existants afin de déterminer si les tiers fournisseurs respectent le RGPD et, le cas échéant, si des mécanismes validés de transferts transfrontaliers de données sont en place.
- Offrir aux employés une formation sur tous les aspects pertinents de la protection de la vie privée qui touchent leurs fonctions, (p. ex., protection intégrée de la vie privée, évaluation des facteurs relatifs à la vie privée (EFVP), protocole d'intervention en cas d'atteinte à la sécurité des données, pratiques de conservation et de destruction des données).
- Évaluer les processus et les fonctionnalités des TI, de même que les contrôles de sécurité des TI afin de déterminer la meilleure façon d'intégrer les exigences du RGPD dans les technologies.
- Hiérarchiser et ordonner les modifications nécessaires en effectuant une analyse des risques et des coûts-avantages.
- Planifier et effectuer régulièrement des audits ou des examens de la conformité.

# Le côté positif

Il est important que les organisations canadiennes assujetties au Règlement général sur la protection des données comprennent bien de quelle façon le règlement s'appliquera à leurs activités ainsi que les mesures qu'elles doivent prendre pour maintenir le niveau de conformité approprié

Il importe par ailleurs qu'elles voient le côté positif : le RGPD leur offre des occasions d'améliorer leur situation globale quant au risque lié à la protection de la vie privée et à la sécurité, de même que de créer une marque bien différenciée et de gagner la confiance des consommateurs à long terme.

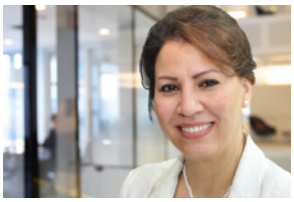
Il serait dans l'intérêt des organisations canadiennes de considérer ces avancées en matière de protection des données comme des tremplins potentiels pour l'acquisition d'un avantage concurrentiel, plutôt que de simples questions de conformité qui entravent la croissance.

# Personnes-ressources

## Auteur

**Irene Reverte Sanchez**
416-874-4228
irevertesanchez@deloitte.ca

## Personnes-ressources



**Est**
**Mariama Zhouri**
514-393-7317
mzhouri@deloitte.ca

**Ouest**
**Don MacPherson**
604-640-3120
donmacpherson@deloitte.ca

**Toronto**
**Beth Dewitt**
416-643-8223
bdewitt@deloitte.ca

Deloitte.

**www.deloitte.ca**

**À propos de Deloitte**

Deloitte offre des services dans les domaines de l'audit, de la certification, de la consultation, des conseils financiers, des conseils en gestion des risques et de la fiscalité, et des services connexes, à de nombreuses entreprises du secteur privé et public. Deloitte sert quatre entreprises sur cinq du palmarès Fortune Global 500® par l'intermédiaire de son réseau mondial de cabinets membres dans plus de 150 pays et territoires, qui offre les compétences, le savoir et les services de renommée mondiale dont les clients ont besoin pour surmonter les défis d'entreprise les plus complexes. Pour en apprendre davantage sur la façon dont les quelque 264 000 professionnels de Deloitte, dont 9 400 au Canada, ont une influence marquante, veuillez nous suivre sur LinkedIn, Twitter ou Facebook.

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. 18-5535H