NORTON ROSE FULBRIGHT

Actualité juridique

Ce que les entreprises canadiennes devraient savoir au sujet du RGPD

Avril 2018
Protection de la vie privée et accès à l'information

Le *Règlement général sur la protection des données* (RGPD) de l'Union européenne (UE) entre en vigueur le 25 mai 2018 et aura des répercussions pour de nombreuses organisations canadiennes, notamment celles qui traitent des données à caractère personnel dans l'Union européenne à titre de responsables du traitement ou de sous-traitants, ou qui traitent des données relatives à des personnes concernées de l'Union européenne.

Le RGPD est l'aboutissement d'une refonte des lois de l'Union européenne en matière de protection des données et remplace la Directive 95/46CE sur la protection des données de même que la législation de mise en œuvre de ses États membres.

Le RGPD impose des obligations de responsabilité contraignantes aux responsables du traitement (les organisations qui déterminent les finalités et les moyens du traitement des données) ainsi qu'aux sous-traitants (les organisations appelées à traiter les données à caractère personnel pour le compte des responsables du traitement).

Un aperçu des principaux aspects du RGPD est présenté ci-dessous.

Application du RGPD aux organisations canadiennes

Ayant une portée territoriale étendue, le RGPD s'appliquera à de nombreuses organisations qui ne sont pas actuellement assujetties aux lois européennes en matière de protection des données. Le RGPD s'appliquera au traitement de données à caractère personnel par des organisations (y compris des organisations canadiennes) qui ont un établissement dans l'UE, indépendamment du lieu où sont traitées ces données. Le RGPD s'appliquera également au traitement de données à caractère personnel par des organisations (y compris des organisations canadiennes) qui sont responsables du traitement des données ou qui agissent comme sous-traitants relativement 1) à l'offre de biens ou de services (même sans frais) à des personnes dans l'UE ou 2) à la surveillance du comportement de personnes dans l'UE.

La portée du RGPD est vaste et pourrait s'appliquer à bon nombre d'organisations canadiennes. Le traitement s'entend de toute opération appliquée à des données à caractère personnel, dont la collecte, l'utilisation, la communication et la conservation. À titre d'exemple, le RGPD s'appliquerait vraisemblablement aux sites Web canadiens en anglais offrant la possibilité d'acheter des biens en euros et leur livraison à des citoyens européens ainsi qu'aux sites Web canadiens assurant un suivi du comportement de citoyens européens au moyen de l'installation de témoins persistants.

Il est possible que les organisations canadiennes qui ne prévoient pas offrir des biens et services dans l'UE échappent à l'application du RGPD.

Représentant dans l'UE

Tout responsable du traitement ou sous-traitant qui n'a pas d'établissement dans l'UE, mais qui entre dans le champ d'application du RGPD, devra désigner un représentant dans l'UE qui agira pour son compte. Une exception s'applique si le traitement est occasionnel, s'il n'implique pas un traitement à grande échelle de catégories particulières de données (comme les données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale ou les données concernant la santé) et si le traitement des données n'est pas susceptible d'engendrer un risque pour les droits et les libertés des personnes concernées.

Consentement

Aux termes du RGPD, les données à caractère personnel ne peuvent être traitées que dans certaines circonstances bien définies (pour exécuter un contrat ou respecter une obligation légale, par exemple) ou moyennant l'obtention d'un consentement. Pour être valable, le consentement doit respecter certaines exigences particulières. Le RGPD précise que le consentement s'entend de toute manifestation de volonté, libre, spécifique, éclairée et univoque faite par une déclaration ou par un acte positif clair. Le consentement doit être aussi facile à retirer qu'à donner. Les enfants de moins de 16 ans devront obtenir le consentement d'un parent.

Gouvernance et principe de responsabilité

Les organisations ont l'obligation positive de mettre en œuvre des moyens de protection des données dès la conception et par défaut. Elles doivent démontrer qu'elles se conforment au RGPD et prouver que la protection des données est prise au sérieux et que leur traitement reçoit le niveau de protection voulu au sein de l'organisation.

Les organisations devront désigner un délégué à la protection des données si : 1) le traitement des données est effectué par une autorité publique ou un organisme public; 2) les activités de base de l'organisation consistent en des opérations de traitement de données qui exigent un suivi régulier et systématique à grande échelle des personnes concernées; ou 3) les activités de base consistent en un traitement à grande échelle de catégories particulières de données (par exemple des données relatives à des condamnations pénales ou révélant l'origine ethnique). Les délégués à la protection des données doivent recevoir l'aide voulue aux fins de l'exercice de leurs missions, devraient faire rapport au niveau le plus élevé de la direction et devraient posséder des connaissances spécialisées du droit et des pratiques en matière de protection des données.

Le RGPD officialise également l'obligation de réaliser des analyses d'impact relatives à la protection des données pour les types de traitement susceptibles d'engendrer un risque élevé pour les droits et libertés d'une personne physique, par exemple dans un cas de profilage, lorsque les décisions fondées sur les profils en question produisent des effets juridiques.

Droits des personnes concernées

Le RGPD confère aux personnes concernées divers droits relativement à leurs données à caractère personnel, y compris les suivants :

- le droit d'obtenir que les données à caractère personnel soient transmises à la personne concernée ou à un autre responsable du traitement dans un format couramment utilisé et lisible par machine (le droit à la portabilité des données);

- le droit d'exiger du responsable du traitement qu'il efface les données à caractère personnel dans certaines circonstances et, s'il les a rendues publiques, qu'il prenne des mesures raisonnables pour informer d'autres responsables du traitement qui traitent ces données de la demande d'effacement (le droit à l'oubli);

- le droit de recevoir des informations complémentaires au sujet du traitement de données par un responsable du traitement (solution d'exportation, limites de stockage) suivant une demande faite par la personne concernée et la transmission de ces informations sous une forme électronique d'usage courant;

- les interdictions et les restrictions concernant la prise de décision automatisée, y compris le profilage (ce qui peut avoir une incidence sur les applications fondées sur l'intelligence artificielle);

- le droit à la transparence, qui exige des responsables du traitement qu'ils fournissent des précisions au sujet des pratiques de traitement des données à caractère personnel de l'organisation; et

- le droit de s'opposer à l'utilisation des données à caractère personnel à des fins de prospection.

Notification de violation

Le RGPD prévoit la mise en place d'un nouveau régime de signalement des violations. Lorsque se produit une violation :

- l'autorité de contrôle compétente doit être informée « dans les meilleurs délais » et, si possible, 72 heures au plus tard après que le responsable du traitement a pris connaissance de la violation. Aucune notification n'est exigée si la violation n'est pas susceptible d'engendrer un risque pour les droits et libertés des personnes concernées;

- les personnes concernées doivent être informées « dans les meilleurs délais » lorsque la violation est susceptible d'engendrer un risque élevé pour leurs droits et libertés.

Les responsables du traitement devront tenir un registre où seront consignées les violations.

Conséquences liées au non-respect des dispositions

Les sociétés déclarées coupables d'avoir violé des droits en matière de traitement de données et manqué à leurs obligations connexes pourraient se voir imposer de lourdes pénalités aux termes du RGPD. Deux niveaux de pénalités sont prévus :

- les infractions graves seront passibles d'une amende pouvant atteindre 20 000 000 d'euros (soit environ 30 000 000 $ CA) ou, s'il est plus élevé, 4 % du chiffre d'affaires annuel mondial du groupe de l'entité; et

- les infractions mineures seront passibles d'une amende pouvant atteindre 10 000 000 d'euros ou, s'il est plus élevé, 2 % du chiffre d'affaires annuel mondial du groupe de l'entité.

Le RGPD permettra également aux particuliers ayant subi un dommage matériel ou moral du fait d'une violation du RGPD d'intenter une poursuite privée et d'être représentés par des organismes d'intérêt public.

Quelques suggestions à l'intention des organisations canadiennes

Bien qu'il y ait un certain chevauchement entre le RGPD et diverses lois canadiennes régissant la protection des renseignements personnels (notamment les obligations en vertu de la LPRPDE, de la PIPA en Alberta et en Colombie-Britannique et de la *Loi sur la protection des renseignements personnels dans le secteur privé* du Québec), les organisations canadiennes pourraient devoir prendre des mesures supplémentaires si elles agissent à titre de responsables du traitement ou de sous-traitants à l'égard des données à caractère personnel de personnes concernées se trouvant dans l'UE conformément au RGPD. Le bureau du commissaire à l'information et à la protection de la vie privée de la Colombie-Britannique a également publié des directives (en anglais seulement) sur le RGPD et dressé des similitudes entre la PIPA en vigueur dans cette province et le RGPD.

Les organisations canadiennes ont tout intérêt à revoir leurs activités afin de déterminer si elles sont assujetties au RGPD et si elles saisissent les obligations légales qui en découlent. Compte tenu des nouvelles exigences fédérales canadiennes en matière de déclaration obligatoire des atteintes à la protection des données et de celles qui sont prévues par le RGPD à cet égard, il pourrait s'avérer judicieux de revoir ces processus quoi qu'il en soit. Les organisations canadiennes devraient envisager des stratégies qui leur permettraient de gérer leur exposition aux risques associés au RGPD.

Ryan Berger
Caroline Deschênes
Amanda Ferriss

Pour plus de renseignements sur le sujet abordé dans ce bulletin, veuillez communiquer avec l'un des avocats mentionnés ci-dessous :

> Julie Himo	Montréal	+1 514.847.6017	julie.himo@nortonrosefulbright.com
> Robert L. Percival	Toronto	+1 416.216.4075	robert.percival@nortonrosefulbright.com
> Tony A. Morris	Calgary	+1 403.267.8187	tony.morris@nortonrosefulbright.com
> Ryan Berger	Vancouver	+1 604.641.4956	ryan.berger@nortonrosefulbright.com