ÊTES-VOUS CONCERNÉ PAR LE *RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES* (RGPD) DE L'UNION EUROPÉENNE?

PIERRE ANTOINE VAILLANCOURT ET MARCEL NAUD*
ROBIC, S.E.N.C.R.L.
AVOCATS, AGENTS DE BREVETS ET DE MARQUES DE COMMERCE

Avec les récents scandales de gestion des données à caractère personnel, le nouveau *Règlement général sur la protection des données* (RGPD), dont la date d'entrée en vigueur est le 25 mai 2018, tombe à point nommé, du moins pour les résidents de l'UE. Or, les entreprises canadiennes devraient s'intéresser au RGPD puisque son champ d'action dépassera les frontières du vieux continent.

1) Qu'est-ce que le RGPD?

Le RGPD, comme son nom l'indique, « établit des règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et des règles relatives à la libre circulation de ces données[1] ». Il impose de nombreuses obligations aux entreprises (tant celles responsables du traitement que leurs sous-traitants) quant aux données à caractère personnel, plus onéreuses que celles actuellement en vigueur.

De plus, les amendes que peuvent dorénavant imposer les autorités nationales de contrôle, organismes chargés du respect du RGPD au niveau national, pourront atteindre le montant le plus élevé entre 20 millions d'euros et 4% du chiffre d'affaires mondial de l'entreprise prise en défaut[2]. D'où l'importance de s'assurer de la conformité de son entreprise, si nécessaire.

2) Est-ce que les entreprises canadiennes sont visées par le RGPD?

Le nouveau règlement produit des effets à l'extérieur de l'UE. Ainsi, est visée par le RGPD toute entreprise (établie ou non en UE) qui traite des données à caractère personnel de résidents européens lorsque ce traitement survient dans le cadre d'activités visant à :

* Pierre Antoine Vaillancourt est avocat et Marcel Naud est avocat et agent de marques chez ROBIC, S.E.N.C.R.L., un cabinet multidisciplinaire d'avocats et d'agents de brevets et de marques de commerce.
[1] Article premier RGPD.
[2] Art. 83 RGPD.

a. proposer des produits ou services (même à titre gratuit) à des résidents européens; ou
b. suivre le comportement de résidents de l'UE par le profilage.

Si une entreprise canadienne s'adonne à l'une ou l'autre de ces activités, elle est ainsi assujettie au RGPD et confrontée à un choix: soit elle limite ses activités de façon à ce les données de résidents de l'UE ne soient plus traitées par l'entreprise, soit elle se conforme aux obligations imposées par le RGPD, risquant autrement de lourdes amendes.

3) En quoi consistent les obligations découlant du RGPD?

Le RGPD renforce des obligations existantes et en impose de nouvelles. Voici un aperçu des obligations susceptibles de demander le plus d'adaptation.

- **Nomination d'un représentant[3] :** Les entreprises situées hors de l'UE doivent nommer un représentant en sol européen qui peut servir de lien entre les autorités européennes concernées et l'entreprise étrangère. Certaines exceptions sont prévues, mais elles apparaissent si restrictives qu'une entreprise préférera pécher par excès de prudence et nommer un représentant.

- **Utilisation détaillée[4]** : Selon une pratique actuelle assez répandue, une entreprise énumère les utilisations faites des données dans des énoncés plutôt vagues tels que « pour assurer le bon fonctionnement des services ». Cette approche n'est plus suffisante sous le RGPD; les entreprises doivent expliciter les finalités du traitement auquel sont destinées les données à caractère personnel ainsi que la base juridique de ce traitement.

- **Consentement manifeste, libre, éclairé et donné à des fins spécifiques[5]** : Le RGPD requiert que l'entreprise responsable du traitement puisse démontrer que la personne concernée a donné son consentement, et ce, sous une forme qui distingue clairement la demande de consentement de toute autre question lorsque le consentement est donné dans le cadre d'une déclaration écrite qui concerne également d'autres questions. Entre autres, les entreprises ne peuvent utiliser un simple avis au bas de l'écran et présumer du consentement ou offrir une case préalablement cochée. De plus, il doit être aussi simple de retirer que de donner son consentement. La personne concernée doit également pouvoir accepter ou refuser séparément les différentes opérations de traitement de ses données, et ce, sans que l'exécution d'un contrat soit subordonnée au consentement qui ne serait pas nécessaire à cette exécution.

[3] Art. 27 RGPD.
[4] Art. 13 c) RGPD.
[5] Art. 7 RGPD.

- **Protection des données dès la conception et par défaut**[6] : Les principes relatifs à la protection des données dès la conception veulent que cette protection soit prise en compte non seulement au moment du traitement lui-même, mais aussi lors de la détermination des moyens de ce traitement, par des mesures techniques et organisationnelles appropriées, telles que la « pseudonymisation ». Cela implique également la minimisation des données, pour que seules soient recueillies les données adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées. Un mécanisme de certification peut servir à démontrer le respect de ces exigences, ce qui peut être d'intérêt dans certaines circonstances.

- **Responsabilité de l'entreprise**[7] : Le principe de responsabilité des entreprises les contraint à mettre en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer que leur traitement des données soit réalisé conformément au RGPD et qu'elles soient en mesure de le démontrer, compte tenu de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques (dont le degré de probabilité et de gravité varie) pour les droits et libertés des personnes physiques. Les entreprises ne peuvent donc adopter une attitude passive ou nonchalante face à la protection de ces données.

- **Délégué à la protection des données**[8] **:** Certaines entreprises sont obligées de désigner un délégué à la protection des données (DPD). Le DPD est un individu dont les missions comprennent celle d'informer et de conseiller les personnes responsables du traitement des données sur les obligations qui leur incombent et de contrôler le respect du RGPD. Un peu comme un ombudsman, il doit être indépendant, c'est-à-dire qu'il ne reçoit d'instructions de personne relativement à ses missions et ne peut être relevé de ses fonctions ou pénalisé en raison de l'exercice de ses fonctions.

Des pratiques à ajuster

Cet aperçu des obligations de la nouvelle réglementation européenne illustre la volonté de l'UE de hausser significativement la protection des données à caractère personnel. Pour les entreprises qui ne seraient pas visées par le RGDP, elles ont, malgré tout, intérêt à ajuster leurs pratiques en la matière, puisqu'il ne faudra pas être surpris de voir d'autres juridictions, dont le Canada, emboiter le pas à l'UE.

[6] Ar. 25 RGPD.
[7] Art. 24 RGPD.
[8] Art. 37 et suivants RGPD.