RGPD

et les PME canadiennes : votre entreprise est-elle visée?

Qu'est-ce que le RGPD?

Le Règlement général sur la protection des données (RGPD) est une nouvelle loi qui encadre la collecte et l'utilisation des données à caractère personnel des citoyens de l'Union européenne (UE). Le droit à la vie privée de ces personnes est ainsi mieux protégé.

Votre entreprise est-elle concernée par le RGPD?

Oui, si des résidents de l'Union européenne visitent votre site Web ou y font des achats, vous devez vous conformer au RGPD.

De plus, si vous recueillez les données personnelles de citoyens européens (par exemple via un formulaire d'abonnement sur votre site Web) ou que vous leur envoyez des courriels commerciaux, vous êtes assujetti au RGPD et vous devez le respecter.

Qu'entend-on par données personnelles?

Une donnée personnelle est tout renseignement qui permet d'identifier une personne :

- Âge
- Groupe ethnique
- Sexe
- Adresse postale
- Emploi
- Données biométriques : empreintes digitales, reconnaissance faciale, etc.
- Renseignements médicaux
- Identifiants uniques : adresse IP, données de localisation, adresse courriel, etc.

Les 3 acteurs du RGPD

Le RGPD fait la distinction entre 3 parties distinctes :

Personne concernée

Personne dont les données personnelles sont collectées. Il s'agit de vos utilisateurs, ainsi que des visiteurs et des acheteurs sur votre site Web.

Responsable du traitement

Entreprise qui demande des données à caractère personnel à ses utilisateurs ainsi qu'aux visiteurs et acheteurs sur son site Web. C'est le cas de votre entreprise.

Sous-traitant

Tierce partie qui traite et conserve les données au nom du responsable du traitement. Cyberimpact, par exemple, est un sous-traitant.

Ignorer le RGPD pourrait vous coûter cher

Si vous ne vous conformez pas au RGPD, cela pourrait vous valoir **jusqu'à 20 millions d'euros d'amende** ou **4 % de vos revenus de l'année précédente,** selon le montant le plus élevé. C'est sans compter la couverture de presse défavorable et la perte potentielle de confiance de vos clients. L'UE pourrait également interdire aux entreprises étrangères de faire affaire en Europe.

RGPD

Recommandations pour vous conformer

1 Identifiez et documentez toutes les données à caractère personnel qui passententreles mains de votre entreprise

Indiquez comment votre entreprise collecte et traite les données à caractère personnel, en précisant :

- Les données à caractère personnel que vous détenez et celles que vous avez l'intention de collecter (noms, adresses courriel, adresses physiques, etc.)
- La façon dont vous recueillez ces données (formulaire pour clients, formulaire d'abonnement sur votre site Web, formulaire d'adhésion, demande de soumission, etc.)
- Les raisons de collecter et de traiter des données à caractère personnel
- La durée de conservation de ces données
- Si vous partagez ces données avec d'autres organisations

2 Droits à la confidentialité des données et demandes d'accès

Expliquez clairement comment et pourquoi votre entreprise a l'intention d'utiliser les données collectées et comment vos clients peuvent voir et modifier leurs données à caractère personnel. Une bonne politique de confidentialité des données vous aidera à protéger les droits des personnes concernées. De plus, vos clients ont le droit de vous demander de supprimer leurs données à caractère personnel. Vous devez donc avoir mis en place la technologie et les processus qui vous permettent de répondre à leurs demandes dans un délai d'un mois.

3 Nommez un délégué à la protection des données

Nommez une personne qui sera responsable des questions entourant la protection des données dans votre entreprise (délégué à la protection des données*). Cette personne sera chargée de mieux faire connaître les règlements sur la protection des données, de former vos employés et de faire le suivi de la conformité.

4 Faites la révision et la mise à jour de vos mesures de sécurité

Ne faites affaire qu'avec des sous-traitants qui connaissent bien les lois sur la vie privée (RGPD, LCAP). Limitez l'accès aux fichiers contenant les données conservées dans un système informatique (mots de passe, mise à jour régulière des réglages de sécurité, etc.).

5 Obtenez le consentement de vos contacts

Organisez vos contacts de l'UE par listes ou groupes distincts (par ex. dans votre plateforme de marketing par courriel). N'ajoutez à votre liste d'envoi de courriels que les gens qui vous ont donné un consentement exprès et ne conservez pas leurs données plus longtemps que nécessaire. Votre entreprise doit garder un registre où sont consignés la manière et le moment où une personne vous a donné son consentement. Le recours à une liste d'envoi ne donne pas au propriétaire d'entreprise l'autorisation de se servir des données d'un client dans un autre but que celui clairement énoncé

6 En cas de violation des données

En cas de perte, de piratage, de modification ou de destruction des données de manière accidentelle, votre entreprise a la responsabilité de gérer la situation. Toute faille de sécurité doit être signalée à l'autorité de protection des données pertinente dans le pays pertinent de l'Union européenne dans les 72 heures suivant sa découverte. Vous devez également en notifier toutes les personnes qui en sont affectées.

7 Consultez un expert

Envisagez d'effectuer une vérification de conformité avec l'aide de professionnels.

* Il n'est pas nécessaire de nommer un délégué à la protection des données si le traitement des données à caractère personnel n'est pas l'une des activités principales de votre entreprise et que vous collectez des données à petite échelle.

Préparé pour vous par :

FCEI
FÉDÉRATION CANADIENNE DE L'ENTREPRISE INDÉPENDANTE

cyberimpact
Plateforme de marketing par courriel **pour les PME canadiennes** qui est conforme à la LCAP et au RGPD.