LawellMcMiller

News.

Pourquoi le RGPD constitue-t'il une opportunité de business pour votre entreprise ?

Le « RGPD », on en mange à toutes les sauces depuis 2018 mais il y a un aspect dont on n'a pas assez parlé : **les opportunités économiques et commerciales qu'il crée**.

Les données constituent la matière première des entreprises. Elles ont, de nos jours, une valeur inestimable. Le développement d'affaires et les prises de décisions des entreprises résident en effet en grande partie sur l'exploitation de ces données.

Si ces données constituent des *données à caractère personnel* et que vous effectuez un *traitement* de ces données, il y a des principes à respecter.

Ces principes ont été posés par le **Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (RGPD)**.

Avant d'expliquer en quoi ce Règlement constitue une réelle opportunité économique pour votre entreprise (TPE, PME ou multinationale), il nous semble important de revenir rapidement sur **quelques concepts de base**.

1. Qu'est-ce qu'une donnée à caractère personnel ?

Une *donnée à caractère personnel* est toute information se rapportant à une **personne physique**, **vivante**, **identifiée ou identifiable [art. 4, 1) RGPD]**.

Une personne physique peut en effet être identifiée **directement** (via son nom et son prénom) mais également **indirectement** (par exemple, via son numéro de téléphone, sa plaque d'immatriculation, un numéro de sécurité sociale, une adresse postale, une adresse email, sa voix, son image, etc).

Relevons que cette identification peut se faire à partir d'une seule donnée (son nom) mais également à partir d'un croisement de plusieurs données (exemple : une femme, née en 1981, vivant dans telle ville et membre de telle entreprise).

> **Exemples de données à caractère personnel** :
>
> nom, prénom, adresse personnelle, adresse e-mail (telle que prénom.nom@entreprise.com) **d'un client, d'un prospect ou d'un employé**, un numéro de carte d'identité, la composition familiale d'une personne, des données de localisation (ex : fonction localisation d'un téléphone portable, d'un véhicule, etc), une adresse de protocole internet (IP), un cookie, un identifiant en ligne, etc.

2. Qu'est-ce qu'un traitement ?

Le *traitement* couvre une large gamme d'opérations effectuées, de manière automatisée ou non (il peut donc aussi s'agir d'un fichier papier), sur des données à caractère personnel **[art. 4, 2) RGPD]**.

Cela comprend la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction de données à caractère personnel.

> **Plus concrètement - exemples de traitement** :
>
> Gestion du personnel et administration des salaires, gestion d'un site Internet récoltant des données à caractère personnel (via un formulaire de contact, un compte client, une newsletter, etc), accès à/consultation d'une base de données de contacts contenant des données à caractère personnel, envoi d'e-mails promotionnels, publication/affichage d'une personne sur un site Internet, conservation d'adresses IP, utilisation d'un système de paiement, enregistrement de vidéosurveillance, etc

3. Conclusion

Toute entreprise, quelle que soit sa taille, traite dans le cadre de ses activités des *données à caractère personnel*.

4. Conséquence(s)

Chaque entreprise est responsable des données qu'elle traite et doit pouvoir démontrer qu'elle respecte les obligations prévues par le RGPD et les lois nationales (principe d'accountability) (obligation d'information des personnes concernées, protection des données dès la conception des projets, protection des données par défaut, tenue d'un registre des traitements de données, conclusion de contrats avec les sous-traitants, rédaction d'une « data protection policy », analyse d'impact, etc). Ces obligations seront détaillées dans un prochain post.

Les autorités de contrôle nationales (l'APD en Belgique, la CNIL en France, etc) veillent au grain.

Elles peuvent agir d'initiative ou être saisies d'une plainte.

Il faudra dans ce cadre démontrer les mesures qui ont été mises en place au sein de l'entreprise.

Il convient de noter qu'en plus de **l'amende administrative qui peut aller jusqu'à 4 % du chiffre d'affaires annuel mondial** (ce qui peut faire très mal dans le contexte actuel), des **sanctions pénales** supplémentaires peuvent désormais également être infligées pour toute violation à la législation vie privée. Une modification du Code pénal a permis de garantir que la société et les personnes physiques ayant commis les mêmes faits puissent être responsables pénalement côte à côte. Ainsi, une personne physique peut être condamnée au même titre que sa société, dans la mesure où tous les éléments de l'infraction sont réunis. **Les *administrateurs* ne peuvent donc désormais plus se retrancher derrière la personne morale et peuvent ainsi voir leur responsabilité également être engagée**.

Il est donc important d'avoir une **attitude proactive en *cartographiant* au sein des différents départements les différents traitements réalisés, en *identifiant la base légale* justifiant ces traitements, en *minimisant la collecte* des données, en mettant en place des *procédures* permettant le respect des droits des personnes concernées** et **des *mesures de protection* des données traitées** [protection physique des données, mise en place de politiques relatives à l'utilisation des ordinateurs, des smartphones, à la gestion des mots de passe, sensibilisation du personnel, etc].

Remarque importante si votre entreprise soumissionne régulièrement à des **marchés publics** :

Les autorités publiques sont à la fois *pouvoirs adjudicateurs*, contraints de respecter la réglementation des marchés publics, mais aussi des *responsables de traitement*, contraints de respecter les règles du RGPD.

Le pouvoir adjudicateur ne peut donc pas choisir un adjudicataire qui ne présente pas les garanties suffisantes en termes de protection des données.

Sous l'angle de la réglementation des marchés publics, cette exigence de conformité au RGPD peut donc très certainement relever d'une condition d'exécution du marché public (soit d'une condition dont le respect est imposé à l'adjudicataire durant l'exécution du marché). Si le pouvoir adjudicateur entend « cadenasser » cette exigence d'exécution, il pourrait en outre ériger certains éléments du RGPD au titre de critère de sélection.

Il est donc important, si vous avez l'habitude de soumissionner à des marchés publics, de d'ores et déjà réfléchir à mettre votre entreprise en conformité.

5. Pourquoi, au-delà de l'aspect réglementaire, le RGPD constitue-t'il surtout une source d'opportunités commerciales non négligeable pour votre entreprise ?

Parce que les mesures techniques et organisationnelles à mettre en place permettront :

- **de renforcer votre image de marque en vous démarquant de la concurrence** : être RGPD « compliant » constitue un gage de sécurité, de transparence et de fiabilité vis-à-vis de vos clients, partenaires, prospects, salariés, etc quant au traitement de leurs données. Favoriser la transparence et permettre aux personnes concernées d'avoir un droit de regard, de contrôle et d'effacement sur leurs données permet en effet d'établir une *relation de confiance durable* ;
- **d'améliorer votre efficacité commerciale** : avoir des fichiers de données à jour qui ne reprennent que les informations *strictement nécessaires* à votre activité vous permet de répondre efficacement aux *besoins de l'entreprise*, que ce soit pour des actions commerciales ou de communication (interne ou externe). Votre client ou prospect ne recevra dans ce cadre que les informations qu'il a choisi de recevoir. Ce qui vous permet de mieux le connaitre, d'identifier ce qui peut poser problème, d'améliorer la relation, de suivre son parcours client, etc (personnalisation de la relation client);
- **de développer votre activité et vos produits ou services** : être RGPD « compliant » implique de cartographier les données et traitements réalisés. Par ce biais, vous pouvez mettre en place une *stratégie autour des données* afin de développer votre activité en renforcant des services existant ou en en créant de nouveaux ;

Le RGPD doit être considéré comme un « *label* » dont les entreprises peuvent être fières. Il ne s'agit pas d'une limitation mais d'une possibilité de faire plus et mieux.

Notre cabinet se tient à votre disposition pour réaliser un **diagnostic des traitements de données**, vous **recommander un plan d'actions sur mesure et pragmatique** afin de mettre votre entreprise en conformité avec la règlementation européenne et nationale de protection de la vie privée et des données à caractère personnel et **rédiger les documents nécessaires** (Privacy/Data Protection Policy, Car/Smartphone/Laptop Policy, etc). Nous pouvons également mettre en place **des ateliers afin de sensibiliser vos équipes à la protection des données.**

Julie Lodomez
Avocate – Associée
Médiatrice agréée

LAWELLMCMILLER

Brussels - Paris
28, avenue Marnix, 1000 Bruxelles
Belgique
02/736.40.90
www.lawell-lawyers.be