



RGPD : Tous concernés !

Tout le monde en parle, mais êtes vous préparé ?

Après 20 ans de réflexion, le nouveau Règlement Général de Protection des Données (RGPD) est entré en vigueur depuis le 25 Mai 2018. Ce règlement augmente le plafond des amendes pouvant être infligées par les autorités de régulation (CNIL en France). Plusieurs changements au sein de votre entreprise sont à organiser...

→ RGPD QUEZACO ?

Le RGPD est le nouveau texte de référence européen en matière de renforcement de la protection de l'utilisation des données à caractère personnelles des citoyens européens. Il a 3 grands objectifs :

- **Mieux protéger** les personnes physiques à l'égard du traitement et la circulation de leurs données personnelles.
- **Accorder des droits** aux personnes physiques dont les données ont été collectées.
- **Imposer de nouvelles obligations** et responsabilités aux collecteurs de ces données avec des sanctions importantes en cas de manquement.



ATTENTION : Certaines entreprises peu scrupuleuses profitent du RGPD pour proposer des prestations excessivement coûteuses, faites appel avant tout à votre bon sens.

→ EN QUOI S'APPLIQUE LE RGPD ?

Le RGPD concerne le traitement de toutes les informations concernant une **personne physique identifiée ou identifiable**, y compris les données personnelles brutes ou indirectes ressorties de manière automatisée en totalité, en partie ou non.

Le traitement des données à caractère personnel est une opération (ou un ensemble d'opérations) qui porte sur la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation, la modification, l'extraction, etc... Une **donnée personnelle** correspond à toute information se rapportant à une personne physique identifiée ou identifiable, c'est-à-dire qui permet de remonter à une personne physique déterminée en se basant sur ces informations. Par ailleurs, un fichier ne contenant que des coordonnées d'entreprises n'est pas un traitement de données personnelles.

Les données personnelles vont des informations les plus communes (identité, photo, adresse mail, numéro de téléphone, numéro de sécurité sociale, etc...) au plus personnelles (caractéristiques physiques, culturelles, sociales, etc...) ou bien même digitales (adresse IP, identifiant, mot de passe, numéro client, etc...).

Le RGPD concerne donc **plusieurs domaines au sein de votre entreprise :**

- **Votre personnel :** gestion du personnel et des rémunérations, trombinoscope, registre des salariés, surveillance, etc...

- **Vos fournisseurs :** annuaires d'entreprises, fichier fournisseurs, etc...
- **Vos clients/prospects :** politique de fidélisation, collecte de coordonnées de prospects par un questionnaire, base marketing avec informations précises (localisation, âge, goûts, comportements d'achats même sans le nom, etc...) etc...

La durée de conservation de ces données doit être également limitée pendant un temps raisonnable par rapport à ce qui est nécessaire vis-à-vis des finalités de leurs utilisations. De plus, il n'est désormais plus possible de collecter ou traiter des données personnelles uniquement au cas où cela pourrait vous être utile un jour.

→ QUI EST CONCERNÉ ?

Le RGPD s'applique à toutes les entreprises traitant (ou sous traitant) des données personnelles, dès lors :

- Qu'elle est établie sur le territoire de l'Union européenne (UE).
- Que son activité cible directement des résidents européens.

Ainsi, les mêmes obligations spécifiques en matière de sécurité, confidentialité et documentation de l'activité sont imposées aux entreprises établies hors de l'UE dès lors qu'elles proposent des services ou des produits aux résidents européens. Elles sont tenues solidairement responsables.

brèves



EQUICER SUR LE TERRAIN

Retrouvez nos conseillers sur différents événements de la filière en France : au Galop Expo à Deauville (23 au 25 octobre), à Equita à Lyon (31 octobre au 4 novembre) et à EquiSeine à Rouen (15 au 18 novembre).



→ POINTS DE VIGILANCE

Certaines données ou certains types de traitements nécessitent une vigilance particulière et peuvent entraîner des actions supplémentaires :

Lorsque vous traitez certains types de données à risque comme :

- Les données révélant l'origine pré-tendument raciale ou ethnique
- Les données portant sur les opinions politiques, philosophiques ou religieuses
- Les données relatives à l'appartenance syndicale
- Les données concernant la santé ou l'orientation sexuelle.

Lorsque votre traitement a pour objet ou effet :

- La surveillance systématique des personnes (télé-surveillance, etc...)
- Le traitement de données sensibles (santé, etc...)
- Le traitement de données concernant des personnes vulnérables (mineurs, etc...)

En cas de risques de piratage des données personnelles, vous devez le signaler à la CNIL dans les 72 heures, ainsi qu'aux personnes concernées du vol de leurs informations.

→ SE CONFORMER AUX OBLIGATIONS EN 6 ÉTAPES

Toutes les entreprises doivent dès maintenant se mettre en conformité, les fichiers déjà existants aussi. Par le RGPD, l'entreprise devient actrice de sa mise en conformité et doit pouvoir en justifier à tout moment via une documentation fournie. ↓



→ LES DROITS ACCORDÉS PAR LE RGPD

Si votre structure recueille des données elle doit obtenir le consentement des personnes physiques de façon explicite. Ces dernières peuvent retirer leur consentement à tout moment et disposent des droits suivants :

Information	• Sur tous les traitements faits pour chaque donnée • Exhaustive et détaillée
Accès	• À l'ensemble des informations détenues et leur utilisation ou non • Réponse donnée dans un délai d'un mois gratuitement
Rectification	• À la demande de la personne physique • Pour toutes les données communiquées
Opposition	• Cessation de l'utilisation à la demande • Sauf s'il existe des motifs légitimes et impérieux
Limitation	• En cas de contestation • Demande la limitation de leur utilisation plutôt que l'effacement
Portabilité	• Récupération des données au près du responsable du traitement initiale automatiquement collectées • Demande de transfère des données à un tiers
Oubli	• Toutes personnes concernées à le droit d'obtenir l'effacement • Dans le respect des obligations légales en vigueur
Réparation	• Obtention du responsable du traitement réparation du préjudice subi • Obtention du sous traitant la réparation du préjudice subi

→ LES POURSUITES ET SANCTIONS ENCOURUES

Les organismes doivent être en mesure de prouver à tout moment à l'organisme de régulation (la CNIL en France) leur conformité au RGPD. Les entreprises qui manquent aux dispositions du RGPD peuvent être sanctionnées par des sanctions administratives ou des amendes qui dépendent de la catégorie de l'infraction.

SANCTIONS ADMINISTRATIVES

- Mise en demeure.
- Retrait de sa certification.
- Rectification, limitation ou effacement des données.
- Satisfaction des demandes d'exercice des droits des personnes.
- Suspension des flux pour un destinataire situé dans un pays tiers.
- Limitation du traitement temporairement ou définitivement.
- Avertissement.

AMENDES

- 10 à 20 M€.
- 2 à 4 % du chiffre d'affaires annuel mondial.

EQUICER *infos* N°26

Comité de rédaction :
Lola BEUNEICHE
Erick BOSSARD

Pour plus d'informations, contactez votre comptable ou votre conseiller EQUICER

www.equicer.fr