

RGPD : Qui est concerné ?

## Description

[Le règlement général sur la protection des données \(RGPD\)](#) vise à harmoniser les pratiques dans l'Union européenne (UE) concernant le traitement des données personnelles. Adopté par l'UE le 14 avril 2016, il vise tout acteur qui a recours à des données personnelles. Ils ont alors l'obligation de se conformer à ce règlement. Il est donc intéressant de connaître quel type d'acteur est concerné par le RGPD.

[Obtenir un devis gratuit RGPD](#)

## Qu'est-ce que le RGPD et qui est concerné ?

Le RGPD est un règlement européen qui  **vise à harmoniser les différentes législations européennes sur le traitement des données personnelles.**

Il impose des obligations aux entreprises en matière de collecte, traitement et conservation des données personnelles.

S'inscrivant dans la continuité de la [Loi informatique et libertés](#), il poursuit principalement 3 objectifs :

- Le renforcement des droits des personnes ;
- La responsabilisation des acteurs traitant des données personnelles ;
- La crédibilisation de la régulation par une coopération renforcée entre autorités de protection des données.

Ainsi, le RGPD est obligatoire dans l'ensemble des 28 États membres de l'UE depuis le 25 mai 2018. De ce fait, tous les acteurs ayant recours à des données personnelles doivent se conformer à ce règlement européen.

## Quels sont les critères d'application du RGPD pour les entités concernées ?

Le RGPD vise principalement les entités qui réalisent des traitements des données personnelles. Cependant, certains traitements de données ne sont pas concernés par le RGPD.

## Traitement des données

Le traitement des données personnelles vise tout d'abord la collecte de données personnelles.

Cela correspond à **toutes informations qui se rapportent à une personne physique** qui peut être identifiée ou identifiable.

De ce fait, le traitement de données personnelles est défini par [l'article 4 du RGPD](#) comme étant « toute opération appliquée à des données personnelles ».

Ainsi, il concerne notamment :

- La collecte ;
- La communication ;
- La conservation ;
- L'enregistrement.

L'objectif du règlement est alors **de protéger la vie privée des citoyens** en protégeant leur information personnelle. Ces informations peuvent être : le nom, le prénom, l'adresse ou encore le numéro de téléphone.

De ce fait, **ces traitements peuvent faire l'objet de collecte** par les entités qui y ont accès. Cela peut être la collecte de données sur des salariés ou encore des clients ou des fournisseurs.

**A noter** : Le règlement européen s'applique à tout traitement de données personnelles effectué par une entreprise sur le territoire français ou européen.

## Traitement non concerné par le RGPD

En principe, les traitements sur des données à caractère personnel d'individus ne résidant pas dans l'union européenne ou n'ayant pas la citoyenneté européenne ne sont pas concernés par le RGPD.

De plus, il existe également d'autres exceptions qu'il convient d'énumérer :

- Les traitements réalisés dans le cadre d'activités mises en place pour la prévention d'infraction pénale ;
- Les traitements réalisés à des fins strictement personnelles ;
- Les traitements réalisés dans le cadre de la protection des libertés et droits fondamentaux.

**Zoom** : La manipulation des données est indispensable et demande une grande rigueur pour les entreprises. Aussi, afin de vous aider dans cette tâche difficile, LegalPlace vous propose de réaliser un [devis de mise en conformité RGPD](#) : une solution simple, efficace et économique !

## Quel est le champ d'application du RGPD ?

Le RGPD s'applique à tous les organismes qui traitent des données personnelles dans l'UE depuis 2016. Ainsi, le RGPD instaure des grands principes qui doivent être respectés.

### Qui ?

En principe, le RGPD **s'applique à tous les organismes effectuant un traitement des données personnelles** indépendamment de sa taille, son pays d'implantation ou son activité.

En effet, le règlement concerne tout organisme public ou privé qui traite des données personnelles pour son propre compte ou non. Peu importe que la collecte de données ne soit pas l'activité principale ou que la collecte soit effectuée pour le compte d'une autre entreprise.

De plus, le RGPD **visé également les sous-traitants**. Si une entreprise fait appel à un sous-traitant réalisant un traitement de données personnelles, il appartient alors à l'entreprise de vérifier que le prestataire respecte bel et bien les règles du RGPD.

Cependant, ils doivent traiter des données personnelles pour le compte d'autres organismes.

Ainsi, si une entité traite des données personnelles pour son compte ou pour le compte d'autrui, **elle a l'obligation de garantir des protections des données** qui lui sont confiées.

**Bon à savoir** : En cas de non-conformité des traitements, l'entreprise ainsi que le

sous-traitant seront co-responsables.

## Où ?

Pour que le RGPD s'applique, [l'article 3 du RGPD](#) dispose que :

- L'entité doit être établie dans un pays de l'UE ;
- Son activité vise directement les habitants de l'UE.

Ainsi, toutes entités qui ne sont pas établies dans l'UE mais qui visent directement des habitants résident sur l'un des territoires de l'UE est soumis aux obligations du RGPD.

Cela s'applique également pour les sous-traitants qui doivent soit être établis dans l'un des pays de l'UE ou qui doivent expressément cibler des habitants de l'UE.

**A noter** : le règlement s'applique pour le traitement de données de tout citoyen européen, indépendamment de sa nationalité.

## Comment ?

Différents principes ont été instaurés afin que le RGPD puisse s'appliquer de la manière la plus efficace possible. En voici quelques-uns :

- [Le private accountability](#) : c'est un principe qui énonce que le responsable de traitement voit sa responsabilité engagée en cas de non-conformité du RGPD ;
- [Le principe de privacy by design](#) : dès la conception du produit, les entités doivent veiller à prendre en compte la protection des données personnelles au sens du RGPD ;
- Le principe de la minimisation des données : la collecte de données doit être limitée à ceux strictement nécessaire par les responsables de traitement ;
- Le principe de la licéité de traitement : il existe 6 conditions dans lesquelles le traitement des données personnelles est permis, listées à [l'article 6-1 du RGPD](#).

De plus, Le RGPD est également **venu attribuer des droits aux personnes dont les données sont collectées**, à savoir :

- Le droit d'accès aux données ;
- Le [droit à la portabilité](#) ;
- Le droit de rectification.

Voici un schéma récapitulatif du champ d'application du RGPD :

Qui ?	Où ?	Comment ?
Tous organismes qui collectent des données personnelles	Au sein de l'UE ou dont l'activité vise des résidents de l'UE.	En instaurant des principes comme le principe de la minimisation  En attribuant des droits aux personnes dont les données sont collectées.

## Quelles sont les actions pour être en conformité avec le RGPD ?

Plusieurs actions sont possibles pour être en conformité avec le RGPD. En voici quelques exemples.

### Trier les données

Il est important **de collecter et de trier les données personnelles pertinentes**.

En pratique, cela passe par la création d'un registre qui permet d'avoir une vue d'ensemble sur toutes les données qui sont collectées.

Ce registre permet, en effet, d'être en [conformité avec le RGPD](#) en recensant les données nécessaires et essentielles.

### Respecter les droits des personnes

Ce respect permet d'être en conformité avec le RGPD puisque **des droits ont été attribués aux personnes dont les données sont collectées**.

Il faut donc s'assurer d'une certaine transparence avec les données collectées. Mais aussi en informant clairement les personnes concernées que leurs données sont collectées.

### Sécuriser les données

Il faut également **sécuriser les données traitées** pour éviter toutes fuites ou des collectes illégales.

Pour cela, il faut impérativement identifier les risques et maîtriser l'utilisation des données collectées.

## Quelles sont les sanctions en cas de non-respect du RGPD pour les entités concernées ?

Il existe plusieurs types de sanctions en cas de non-respect du RGPD. Ces sanctions sont principalement administratives et pénales. Cependant, il existe également d'autres sanctions.

### Sanctions administratives

Des sanctions administratives peuvent être prononcées par la Commission nationale de l'informatique et des libertés (CNIL).

Elle est chargée de **veiller à la protection des données personnelles**.

Plusieurs types de sanctions peuvent être prononcés par la formation restreinte de la CNIL :

- Un rappel à l'ordre qui est un avertissement avant de prononcer une réelle sanction ;
- Une injonction concrète de cesser la violation des données personnelles ;
- La limitation ou suspension temporaire du traitement des données ;
- Une amende administrative dont le montant est fixé selon la gravité de la violation : Ce montant peut être compris entre 2 et 4% du chiffre d'affaires annuel d'un organisme et peut aller jusqu'à 20 millions d'euros.

### Sanctions pénales

Des sanctions pénales peuvent également être prononcées.

Selon [l'article 226-18 du code pénal](#), le fait de collecter des données personnelles de manière illégale, par un moyen frauduleux ou de manière déloyale **est puni de 5 ans d'emprisonnement et de 300 000 euros d'amende**.

De plus, ces sanctions pénales sont inscrites dans [le RGPD à l'article 84](#).

Cet article prévoit que les États membres détiennent la possibilité d'instaurer des sanctions à l'échelle nationale et sur le plan pénal.

Ainsi, chaque État membre de l'UE peut établir des sanctions pénales pour non-respect du RGPD.

## Autres sanctions

D'autres sanctions administratives et pénales sont également prononcées en cas de non-respect du RGPD.

La formation restreinte de la CNIL peut décider **de rendre public la décision qu'elle adopte**.

Cette publication peut impacter fortement la réputation de l'entité qui n'a pas respecté les obligations du RGPD.

De plus, l'entité qui ne respecte pas les obligations du RGPD **s'expose à devoir verser des dommages et intérêts ainsi qu'un déficit à l'image**.

Les dommages et intérêts sont versés directement à la personne qui a été victime d'un dommage personnel ou matériel à cause de la fuite de données.

**Attention** : ce sont des sanctions supplémentaires. De ce fait, elles s'ajoutent aux sanctions administratives et aux sanctions pénales.

## FAQ

### Quels sont les 3 principes du RGPD du droit aux personnes ?

Les 3 principes du RGPD du droit aux personnes sont : le droit d'accéder à leurs données et d'en obtenir une copie, le droit de les rectifier et le droit de s'opposer à leur utilisation.

## **Quel est le but du RGPD ?**

Le but du RGPD est de permettre aux citoyens européens de vérifier et de faire valoir leurs droits et leurs données personnelles quand celles-ci sont collectées de manière illégale. Le RGPD offre alors un cadre pour que la collecte des données personnelles n'entrave pas leur droit à une vie privée.

## **Est-ce que le RGPD est obligatoire ?**

Le respect du RGPD est obligatoire pour toutes les entreprises résident dans l'UE ou dont leur activité vise directement les habitants de l'UE.