



# LE RGPD

RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES

## ▶ 25 mai 2018

Date d'entrée en application du **RGPD**, qui encadre le traitement des données personnelles sur le territoire de l'Union Européenne

## ▶ QUI EST CONCERNÉ

Le **RGPD** s'applique à toute organisation, publique et privée, qui traite des données personnelles pour son compte ou non, dès lors qu'elle est établie sur le territoire de l'Union Européenne et que son activité cible directement des résidents européens

## ▶ LES 8 RÈGLES D'OR

permettant la collecte, l'utilisation et la conservation des données personnelles par le RGPD

- ❖ Licéité du traitement
- ❖ Finalité du traitement
- ❖ Minimisation des données
- ❖ Protection particulière des données sensibles
- ❖ Conservation limitée des données
- ❖ Obligation de sécurité
- ❖ Transparence
- ❖ Droits des personnes

## ▶ DROITS DES PERSONNES

- ❖ Droit d'accès
- ❖ Droit de rectification
- ❖ Droit d'opposition
- ❖ Droit à l'effacement
- ❖ Droit à la portabilité
- ❖ Droit à la limitation du traitement
- ❖ Droit de ne pas faire l'objet d'une décision individuelle automatisée

## ▶ OBLIGATIONS DES RESPONSABLES DE TRAITEMENTS

- Informer les personnes concernées de leurs droits
- Obtenir le consentement
- Collecter uniquement les données nécessaires
- Sécuriser les données : restreindre l'accès
- Ne pas divulguer n'importe quelles données, à n'importe qui
- Supprimer les données en accord avec les durées légales
- Informer le DPO de tout nouveau traitement de données
- Notifier toute violation de données

## ▶ LES OBLIGATIONS DES ENTREPRISES

- Désigner un DPO (Data Protection Officer)
- Tenir un registre de traitement de données
- Informer les personnes concernées
- Assurer la sécurité des données
- Réaliser une analyse d'impact sur la vie privée (PIA)
- Respecter le principe de protection des données personnelles et de la vie privée en devenant « Accountable » (responsable)
- Respecter les notions de « *privacy by design* » et « *privacy by default* »
- Revoir les contrats de sous-traitants et valider la conformité avec les exigences du RGPD

## ▶ DE QUOI PARLE-T-ON ?

Une **donnée personnelle** :  
est toute information se rapportant à une personne physique identifiée ou identifiable

Un **traitement de données personnelles** :  
est une opération, ou ensemble d'opérations, portant sur des données personnelles, quel que soit le procédé utilisé (collecte, enregistrement, organisation, conservation, modification...)

### Données personnelles

Données directement identifiantes:

- Nom
- Prénom
- Email nominatif
- Photo

Données indirectement identifiantes:

- Pseudo
- Matricule
- Numéro de sécurité sociale
- Données biométriques
- Date et lieu de naissance
- Lieu de résidence
- Nom de l'employeur
- Centres d'intérêt

### Données sensibles

- Origines raciale ou ethnique
- Convictions religieuses ou philosophiques
- Opinions politiques
- Appartenance syndicale
- Données génétiques ou biométriques
- Orientations sexuelles
- Etat de santé

LE TRAITEMENT EST INTERDIT

### Les pays concernés ?

Tous les pays de l'UE et pays hors UE traitant les données des personnes situées dans l'UE

En cas de non respect du RGPD l'amende peut s'élever à :

## 20 M €

ou 4% du CA annuel global  
(Le plus élevé des deux)



La **CNIL** est le « Gendarme » du RGPD en France avec pouvoir de sanctions administratives