

# Le R.G.P.D

- Synthèse -

- Impacts et mise en œuvre -



CODE  
DU  
TRAVAIL

ACTU Info – Juin 2018

Le 25 mai est entré en vigueur **le nouveau Règlement Général sur la Protection des Données (RGPD)** - ou GDPR en Anglais -, visant à renforcer les droits des personnes. Le RGPD modifie en profondeur la réglementation applicable en matière de collecte et de traitement des données personnelles. Son objectif est double : **harmoniser la législation à l'échelle européenne** d'une part, **renforcer les droits des personnes en imposant de nouvelles obligations**, dont le non-respect expose à un risque de sanctions lourdes.

## Sommaire

1. RGPD, qui est concerné ?
2. Comment mettre en œuvre le RGPD ?
3. RGPD et notion de consentement des personnes

### 1. RGPD, qui est concerné ?



Le RGPD concerne les organismes et les sociétés sans distinction de leur caractère privé ou public. Ainsi, il concerne tout organisme qui collecte et traite des données personnelles de résidents européens.



Le saviez-vous ?

Contrairement aux directives européennes dont l'application est soumise à transposition nationale, le RGPD, en tant que règlement européen, **est d'application immédiate dans l'ensemble des Etats membres**. Concrètement, la société qui collecte et exploite des données personnelles – notamment dans le cadre de ses actions d'emailing marketing – doit se conformer au nouveau règlement général sur la protection des données depuis le 25 mai 2018, dès lors que sont concernés des résidents européens.

## 2. Comment mettre en œuvre le RGPD

1. **Sécurisation des données** : Les organismes qui collectent et traitent des données personnelles – ainsi que leurs sous-traitants – devront mettre en place les mesures de sécurité conformes aux préconisations : au moment de la conception de leur système d'exploitation, ils devront veiller à l'efficacité des dispositifs de protection associés.
2. **Etablissement et tenue à jour d'un registre des traitements** : l'entreprise qui dispose de données personnelles devra en consigner l'état dans un registre spécifique, mis à jour. Ce registre sera disponible à tout moment pour consultation par l'autorité de protection compétente (CNIL) Ce registre devrait comporter :
  - ✓ La liste des données personnelles et leur degré de sensibilité
  - ✓ La finalité de leur utilisation
  - ✓ Leur durée de conservation.
  - ✓ Les personnes ayant accès à ces données et leur niveau de sécurité
3. **Notification des fuites de données** : l'entreprise ainsi que son sous-traitant aura l'obligation de prévenir l'autorité nationale en cas de faille avérée dans son système de sécurité.
4. **Nomination d'un Délégué à la Protection des Données – en anglais Data Protection Officer- (DPO)** : les organismes privés et publics qui manipulent des données considérées comme « sensibles » devront s'adjoindre le concours d'un DPO en vue de leur protection (obligatoire ou fortement recommandé)
5. **Obtention du consentement des personnes** : Le recueil des données personnelles devra faire l'objet d'un consentement écrit de la personne concernée (voir ci-après)
6. **Droits des personnes** : le RGPD accorde 2 nouvelles prérogatives aux personnes. Le droit à l'effacement, variante du droit à l'oubli, et le droit à la portabilité. Ce dernier imposera à la société de communiquer, sur simple demande de la personne concernée, l'ensemble des données personnelles collectées sous un format lisible par machine.



Pensez à établir votre registre des activités de traitement et vos mentions d'information, des modèles sont disponibles sur le site de la CNIL : <https://www.cnil.fr/fr/les-outils-de-la-conformite>

# RGPD

## PASSER À L'ACTION

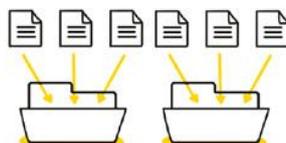
en 4 étapes

1



Constituez un registre de vos traitements de données

2



Faites le tri dans vos données

3



Respectez les droits des personnes

4



Sécurisez vos données



### POINTS DE VIGILANCE POUR LES ENTREPRISES

- ⇒ La mise à jour de vos conditions générales de vente / contrats de prestation
- ⇒ Le recueil du consentement des tiers (clients, prospects, salariés, candidats au recrutement...)
- ⇒ L'établissement du registre des données personnelles collectées
- ⇒ La désignation d'un DPO est recommandée

Les sanctions prévues en l'absence de mise en œuvre du RGPD sont lourdes :  
**Des amendes jusqu'à 20 millions d'euros ou 4 % du CA !**

### 3. RGPD et notion de consentement des personnes

Le RGPD place au cœur des débats la notion de consentement de la personne visée par la collecte et le traitement des données.

Dans un premier temps, le RGPD précise les contours de l'obligation d'information à la charge de l'organisme exploitant les données personnelles : le responsable du traitement doit fournir une information « **compréhensible et aisément accessible** » concernant les modalités et la finalité de la collecte des données.

Dans un second temps, le RGPD se focalise sur les modalités du consentement : il doit s'agir d'un « **acte positif clair par lequel la personne concernée manifeste de façon libre, spécifique, éclairée et univoque son accord au traitement des données à caractère personnel la concernant** ». Concrètement, le consentement pourrait être donné par déclaration écrite, ou au moyen d'une case à cocher, à charge pour la société qui exploite les données, en tout état de cause, de prouver le caractère licite du consentement. Le texte du règlement européen ajoute que l'inactivité ou le silence de la personne, ou la case cochée par défaut par le responsable du traitement ne sont pas constitutif d'un consentement tel que défini par le RGPD.

Modèles sur le site de la CNIL :

<https://www.cnil.fr/fr/rgpd-exemples-de-mentions-dinformation>



#### Zoom en matière RH :

Le RGPD complète les informations à fournir obligatoirement aux salariés préalablement au traitement de leurs données personnelles. Ainsi, les salariés (et les candidats) devront être informés notamment :

- des coordonnées du DPO ;
- du fondement juridique du traitement ;
- de la durée de conservation des données ;
- de leur droit d'introduire une réclamation auprès de la Cnil ;
- de leur droit de retirer leur consentement à tout moment ;
- de l'intention d'effectuer un traitement ultérieur des données à d'autres fins.

*L'équipe Paye/RH Touche Pas à La Paye*