# RGPD – Règlement général de protection des données

FICHE PRATIQUE

**Le 25 mai 2018, le RGPD entre en application et vient fixer les nouvelles règles en matière de recueil, traitement et conservation des données personnelles par toute entreprise ou association.**
Le RGPD repose sur le *principe d'Accountability* : pas de formalités préalable mais l'obligation pour les entreprises et associations de mettre en place des procédures internes démontrant le respect des règles issues du RGPD

Se conformer aux exigences du RGPD en 9 étapes :

1. **Désigner une personne référente** : le **délégué à la protection des données** (DPO), membre ou non du personnel.
La désignation d'un DPO est obligatoire dans deux cas : lorsque vos activités de base vous amènent à réaliser un **suivi à grande échelle, régulier et systématique**, ou à traiter à grande échelle des **données dites sensibles** ou relatives à des **condamnations pénales et infractions**.

2. **Etablir un registre des données personnelles** qui permettra de recenser les données collectées et la manière dont elles le sont et dont elles sont traitées.

3. **Analyser les données** du registre afin d'en vérifier leur conformité au RGPD. Il faudra alors vérifier les **circonstances de collecte** des données (consentement obtenu? Sinon obligation liée au contrat?), **l'information délivrée** aux personnes faisant l'objet de la collecte des données (ont-elles été informées de la finalité du traitement et de leurs droits?), et enfin la **nature des données** collectées (seules les données strictement nécessaires au traitement et à la finalité recherchée peuvent être collectées et traitées).

4. Mettre en place des **mesures pour sécuriser les données collectées**. Pour ce faire :
- **Sensibiliser et informer les salariés** de l'entreprise
- Dans les outils de collecte, indiquer la **finalité de la collecte**, le **traitement prévu** et les **droits des personnes** (Cf. www.cnil.fr)
- Laisser à la personne la **possibilité de s'opposer au traitement** indiqué
- Indiquer les **contacts du DPO** pour que la personne puisse faire modifier ou supprimer ses données personnelles
- Prévoir un **lien de désinscription** à chaque newsletter envoyée
- **Sécuriser les locaux** contenant les données personnelles (en cas de sous-traitance, un contrat doit lier l'entreprise et le sous-traitant

5. Permettre le **droit à la portabilité** afin que les personnes puissent **récupérer leurs données transmises** à des fins personnelles.
Ce droit à la portabilité ne se limite qu'aux données traitées de manière automatisée et transmises par la personne. Il ne doit pas porter atteinte aux droits et libertés de tiers.

# RGPD – Règlement général de protection des données

FICHE PRATIQUE

**6. Informer** les bénéficiaires **du droit à la portabilité.** Il s'agit là d'expliquer clairement la différence entre le droit à la portabilité (uniquement les données personnelles fournies par le demandeur et traitées sur la base de son consentement) et le **droit d'accès** (toutes données personnelles concernant le demandeur).

*=> Exemple de courrier d'information en annexe, extrait du guide « Données personnelles et RGPD : comment faire? » de la CPME*

**7. Mener une analyse d'impact** lorsqu'il y a **combinaison de deux des critères** suivants :

- Evaluation ou notation
- Décision automatisée avec effet juridique ou effet similaire significatif
- Surveillance systématique
- Données sensibles ou données à caractère hautement personnel
- Données personnelles traitées à grande échelle
- Croisement d'ensembles de données
- Données concernant des personnes vulnérables
- Usage innovant ou application de nouvelles solutions technologiques ou organisationnelles
- Exclusion du bénéfice d'un droit, d'un service ou contrat

**8. Programmer la suppression des données** qui doit intervenir dès lors qu'elles ne sont plus nécessaires au regard de la finalité.
Il existe également un **droit à l'oubli et à l'effacement** dans le cas de collecte ou traitement illégal ou dans le cadre du **droit d'opposition** sans qu'aucun motif légitime n'y fasse obstacle.

**9. Réagir en cas d'atteinte** aux données personnelles. Dans ce cas (perte des données, accès à un fichier par une personne non autorisée, attaque informatique, etc.) l'entreprise doit en **informer la CNIL dans les 72h** suivant la découverte de l'incident. Téléservice disponible sur www.cnil.fr
En cas de risque élevé d'atteinte pour les personnes, l'entreprise doit les informer de la violation, des conséquences probables et des mesures qu'il convient d'adopter.

Sources:
https://www.cnil.fr/fr/principes-cles/rgpd-se-preparer-en-6-etapes
https://www.cpme.fr/economies/voir/2346/donnees-personnelles-preparez-l-application-du-rgpd