



Le RGPD en 10 points clés

L'essentiel pour mettre votre structure en conformité

Le RGPD encadre la collecte et l'usage des données personnelles. Voici les **dix principes** à connaître pour rester en conformité et protéger vos clients comme vos patients.

1**LICÉITÉ**

Tout traitement repose sur l'une des six bases légales : consentement, contrat, obligation légale, intérêt légitime, mission d'intérêt public ou intérêts vitaux.

2**FINALITÉ**

Les données sont collectées pour un objectif précis, explicite et légitime, sans réutilisation détournée.

3**MINIMISATION**

Ne collectez que les données strictement nécessaires à la finalité poursuivie, et ne les conservez pas plus longtemps que nécessaire.

4**DONNÉES SENSIBLES**

Santé, opinions, biométrie : traitement interdit par principe, sauf exceptions prévues par la loi (soins, consentement explicite...) et avec une protection renforcée.

5**CONSENTEMENT**

Lorsqu'il est la base légale : libre, spécifique, éclairé, univoque et révocable à tout moment. Les cases pré-cochées sont interdites.

6**DROITS DES PERSONNES**

Accès, rectification, effacement, limitation, portabilité, opposition : réponse sous un mois (prolongeable de deux mois si la demande est complexe).

7**REGISTRE DES TRAITEMENTS**

Article 30 : documentez vos traitements. En pratique indispensable dès que vous traitez des données régulièrement ou des données de santé, quelle que soit votre taille.

8**SÉCURITÉ**

Mots de passe, chiffrement, accès restreints et sauvegardes : la protection technique est une obligation.

9**VIOLATION DE DONNÉES**

En cas de fuite présentant un risque : notification à la CNIL si possible sous 72 heures, et information des personnes si le risque est élevé.

10**LE DPO**

Le délégué à la protection des données pilote votre conformité et dialogue avec la CNIL. Obligatoire notamment en cas de traitement de données de santé à grande échelle ; vivement recommandé dans les autres cas.

Bon à savoir

Le RGPD n'est pas qu'un document : c'est une **démarche continue**. Une non-conformité expose à des sanctions de la CNIL pouvant atteindre 20 millions d'euros ou 4 % du chiffre d'affaires annuel mondial (le montant le plus élevé étant retenu). Se faire accompagner sécurise et simplifie la mise en conformité.