

## les 5 recommandations pour le respect du RGPD

**Les actions principales à mener pour entamer et maintenir sa mise en conformité avec les règles de protection des données :**

### **1- Désigner un pilote:**

- ❖ Pour piloter la gouvernance des données personnelles et protéger les droits fondamentaux des personnes concernées ;vous aurez besoin d'un véritable chef d'orchestre : le délégué à la protection des données personnelles. Le DPO doit connaître les caractéristiques-clés de son établissement pour pouvoir adapter ses actions
- ❖ Le DPO peut être interne ou externe à l'établissement et mutualisé entre plusieurs établissements. Pour réunir l'ensemble des compétences attendues et soutenir le DPO
- ❖ Le DPO pilote la mise en conformité au RGPD de votre entreprise, et met en œuvre les actions d'amélioration. Il sensibilise les équipes et gère la coordination et l'animation de la conformité, dont il assure le respect.

### **2- Constituez un registre de vos traitements de données:**

- ❖ En constituant votre registre, vous aurez une vision d'ensemble sur vos traitements de données.
- ❖ Identifiez les activités principales de votre entreprise qui utilisent des données personnelles.
- ❖ Dans votre registre, créez une fiche pour chaque activité recensée, en précisant :
  - L'objectif poursuivi.
  - Les catégories de données utilisées.
  - Qui a accès aux données.
  - La durée de conservation de ces données (durée durant laquelle les données sont utiles d'un point de vue opérationnel, et durée de conservation en archive).
- ❖ Le registre est placé sous la responsabilité du dirigeant de l'entreprise.

- ❖ Pour avoir un registre exhaustif et à jour, il faut en discuter et être en contact avec toutes les personnes de l'entreprise susceptibles de traiter des données personnelles.

### 3- Faites le tri dans vos données:

Pour chaque fiche de registre créée, vérifiez que :

- ❖ les données que vous traitez sont nécessaires à vos activités.
- ❖ vous ne traitez aucune donnée dite « sensible ».
- ❖ seules les personnes habilitées ont accès aux données dont elles ont besoin.
- ❖ vous ne conservez pas vos données au-delà de ce qui est nécessaire.

### 4-Respectez les droits des personnes:

Le RGPD renforce l'obligation d'information et de transparence à l'égard des personnes dont vous traitez les données (clients, collaborateurs, etc.).

**Informez les personnes:** Les personnes doivent être informées de l'utilisation des données les concernant et de la manière dont ils peuvent exercer leurs droits.

**Permettez aux personnes d'exercer facilement leurs droits:** les personnes dont vous traitez les données (clients, collaborateurs, prestataires, etc.) ont des droits sur leurs données : droit d'accès, de rectification, d'opposition, d'effacement, à la portabilité et à la limitation du traitement.

### 5-Sécurisez vos données:

Si le risque zéro n'existe pas en informatique, vous devez prendre les mesures nécessaires pour sécuriser les données.

Cela vous permet aussi de protéger votre patrimoine de données en réduisant les risques de pertes de données ou de piratage.

Les mesures à prendre, informatiques ou physiques, dépendent de la sensibilité des données que vous traitez et des risques qui pèsent sur les personnes en cas de d'incident.

**Des réflexes doivent être mis en place :** mettre à jour de vos antivirus et logiciels, bien choisir ses mots de passe, chiffrer vos données dans certaines situations et faire des sauvegardes.

Les failles de sécurité ont également des conséquences pour ceux qui vous ont confié des données personnelles : Ayez à l'esprit les conséquences pour les personnes et pour votre entreprise.