**Fiche 2 : Mesures de sécurité des données personnelles**

**Principes du RGPD :**
Conformément à l'**Art. 32 du RGPD**, les mesures de sécurité doivent être adaptées au risque encouru. Voici des exemples de mesures techniques et organisationnelles :

**1. Chiffrement**

* **Ce que c’est :** Technique rendant les données illisibles sans une clé de décryptage.
* **Quand l’appliquer :** Pour les données sensibles ou critiques (exemple : données de paiement).
* **Exemple :** Une PME utilise un logiciel de chiffrement pour protéger les fichiers contenant les informations bancaires de ses clients.

**2. Gestion des mots de passe**

* **Ce que c’est :** Mise en place de mots de passe forts et renouvelés régulièrement.
* **Quand l’appliquer :** Pour protéger l’accès aux systèmes et aux données.
* **Exemple :** Utiliser des mots de passe contenant au moins 12 caractères, avec majuscules, chiffres et caractères spéciaux.

**3. Contrôle des accès**

* **Ce que c’est :** Limiter l’accès aux données aux seules personnes autorisées.
* **Quand l’appliquer :** Toujours, pour réduire le risque d’accès non autorisé.
* **Exemple :** Les informations RH d’une PME ne sont accessibles qu’au directeur et au responsable administratif.

**4. Sauvegarde régulière**

* **Ce que c’est :** Copies régulières des données pour éviter leur perte.
* **Quand l’appliquer :** Pour toutes les données critiques.
* **Exemple :** Une sauvegarde hebdomadaire est réalisée sur un disque dur externe sécurisé.

**5. Authentification multi-facteurs**

* **Ce que c’est :** Double vérification pour accéder à un système (exemple : mot de passe + code SMS).
* **Quand l’appliquer :** Pour sécuriser les accès sensibles (exemple : tableau de bord client).
* **Exemple :** Un commerçant active une double authentification pour accéder à son logiciel de gestion.
	1. **La pseudonymisation**
	2. **La confidentialité, l'intégrité, la disponibilité des systèmes.**
	3. **Une procédure pour restaurer la disponibilité des données en cas d’incident.**

**Actions pratiques :**

* **Évaluez les risques liés aux données :** Identifiez les types de données traitées et leur sensibilité (exemple : données bancaires, dossiers clients).
* **Adoptez des mesures de sécurité :**
* Mettez en place des mots de passe robustes et changez-les régulièrement.
* Limitez les accès aux données sensibles aux seules personnes autorisées.
* Sauvegardez régulièrement les données (exemple : sauvegarde hebdomadaire sur un disque externe sécurisé).
* **Exemple concret :** Une boutique en ligne : utilisez un protocole HTTPS pour sécuriser les paiements en ligne et activez l’authentification à deux facteurs pour l’accès au tableau de bord administratif.