1 Principes de la protection des données

: Niveau 1
: Réglementation
: Tout service

Bonnes pratiques

- Respecter les grands principes du RGPD :

→ Licéité, loyauté et transparence.
→ Limitation des finalités.
→ Minimisation des données.
→ Exactitude des données.
→ Limites de la conservation des données.
→ Garantir la sécurité des données.

- Démontrer sa conformité à la règlementation : à l'autorité de contrôle, à des partenaires ou à des clients.
- Intégrer la protection des données dès la conception.
- Informer les personnes concernées.

Réglementation

- Article 5 du RGPD sur les principes du RGPD.
- Article 6 du RGPD sur le principe de licéité du traitement.
- Articles 13 et 14 du RGPD sur l'information des personnes concernées.
- Articles 32 du RGPD sur la sécurité des données.

Risques

Ne pas respecter les principes du RGPD fait peser plusieurs risques sur le Responsable de Traitement (ou l'entreprise) :

- Risques juridiques :

→ Sanction administrative de niveau 1 de 2% du CA mondial ou 10M€.
→ Sanction administrative de niveau 2 de 4% du CA mondial ou 20M€.
→ Sanction pénale de 300000€ et 5 ans de prison pour non-respect de la sécurité des données.

- Risques réputationnel :

→ Atteinte à l'image de l'entreprise
→ Perte d'opportunités, (notamment, commerciales).

- Risque de sécurité des données et de l'entreprise.

- **Licéité, loyauté et transparence**

→ Les données à caractère personnel doivent être traitées de manière licite, loyale et transparente au regard de la personne concernée.

- **Limitation des finalités**

→ Les données à caractère personnel doivent être collectées pour des finalités déterminées, explicites et légitimes.

→ Ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités.

- **Minimisation des données**

→ Les données à caractère personnel doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées

→ Si non nécessaire au traitement, la donnée ne doit pas être collectée, ou de façon facultative.

- **Exactitude**

→ Les données à caractère personnel doivent être exactes et, si nécessaire, tenues à jour.

→ Toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel qui sont inexactes soient effacées ou rectifiées sans tarder.

- **Limite de la conservation des données dans le temps**

→ Les données à caractère personnel doivent être conservées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées.

- **Sécurité**

→ Garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées.

- **Accountability**

→ Être conforme à la règlementation.

À voir à la suite du chapitre 1 :

→ Les durées de conservation

→ Les 12 régles d'or de la sécurité

→ Les droits des personnes