L'article 25 du RGPD impose d'intégrer la protection des données personnelles dès la conception d'un traitement, en mettant en place des mesures techniques et organisationnelles appropriées. Ce faisant, le **Privacy By Design** permet de répondre de manière structurée à cette obligation.

Objectifs : éviter que la conformité RGPD ne soit un ajout tardif mais une brique native du projet.

Les 7 principes clés du Privacy By Design :

Prendre des mesures préventives pour anticiper les risques :
Exemple : implémenter un audit de sécurité dès le début.

Protéger par défaut les données personnelles sans action de l'utilisateur :
Exemple : une application ne doit pas activer la géolocalisation sans consentement explicite.

Intégrer la protection dès la conception :
Exemple : prévoir des logs anonymisés dans l'architecture technique d'une appli.

Sécuriser sans dégrader l'expérience utilisateur :
Exemple : authentification forte sans rendre l'accès au service trop lourd.

Sécuriser les données pendant toute la durée de conservation :
Exemple : chiffrement des backups jusqu'à leur destruction.

Assurer la transparence des traitements effectués :
Exemple : interface utilisateur expliquant quelles données sont collectées, pourquoi, et comment elles sont utilisées.

Respecter les droits des personnes :
Exemple : portail utilisateur pour gérer ses préférences et supprimer son compte.

Mise en œuvre du Privacy By Design

Mesures techniques :

- Chiffrement des données
- Pseudonymisation des données
- Utilisation de mots de passe…

Mesures organisationnelles :

- Formations RGPD à destination des collaborateurs
- Gestion des accès aux données personnelles
- Obligations contractuelles pour les sous-traitants…

Astuce projet : intégrer une Analyse d'Impact (AIPD) dans votre roadmap pour identifier les risques dès la phase de cadrage.

Pourquoi appliquer le Privacy by Design ?

- Assurer la sécurité des données traitées ;
- Garantir la transparence envers les personnes concernées ;
- Réduire les risques liés à la perte ou à l'altération des données ;
- Réduire les coûts liés à un incident de sécurité ;
- Limiter les risques de sanctions de la CNIL ;
- Améliorer l'expérience des personnes concernées.

Ce qu'il faut retenir

Le Privacy By Design

Pour aller plus loin...

contact@pragma9.fr