

RGPD · le cadre européen

Règlement Général sur la Protection des Données · européen · entré en application le 25 mai 2018.
S'impose à tout organisme (public ou privé) qui traite des données de personnes situées dans l'UE · portée extraterritoriale.

La CNIL (loi Informatique & Libertés, 1978) contrôle en France · sanctions jusqu'à 20 M€ ou 4 % du CA mondial.

Qu'est-ce qu'une donnée perso ?

Catégorie	Exemples
Identification directe	Nom · prénom · n° SS · photo
Identification indirecte	IP · cookie · téléphone · GPS
Données sensibles (renforcé)	origine ethnique · opinion · santé · orientation sexuelle · biométrie
Traitement	toute opération · collecte · enregistrement · conservation · communication · suppression.

Les 6 principes fondamentaux

- 1 Licéité & transparence · base légale + information claire
- 2 Finalités · déterminées, explicites, légitimes
- 3 Minimisation · seulement ce qui est nécessaire
- 4 Exactitude · données à jour, rectifiables
- 5 Limitation conservation · pas plus que nécessaire
- 6 Intégrité · confidentialité · chiffrement, accès

Principe transversal · accountability · pouvoir démontrer à tout moment qu'on respecte le RGPD.

Les acteurs

Acteur	Rôle
Responsable de traitement	Définit finalités & moyens · porte la responsabilité
Sous-traitant	Traite pour le compte du responsable · contrat écrit obligatoire
DPO · Data Protection officer	Conseille · contrôle · coopère avec la CNIL · indépendant
CNIL	Autorité de contrôle française
CEPD	Cohérence à l'échelle UE

DPO obligatoire · organismes publics · suivi à grande échelle · données sensibles à grande échelle.

Les 8 droits des personnes

- Information · au moment de la collecte
- Accès · obtenir ses données (réponse en 1 mois)
- Rectification · corriger les inexactitudes
- Effacement · « droit à l'oubli »
- Limitation · gel temporaire du traitement
- Portabilité · format structuré (JSON, CSV)
- Opposition · prospection commerciale
- Décision automatisée · droit à l'intervention humaine

Conformité · démarche pratique

- 1 Registre des traitements · obligatoire dès 250 salariés
- 2 Choisir une base légale · consentement, contrat, obligation légale, etc.
- 3 Contrats sous-traitants (DPA) · cloud, CRM, analytics
- 4 AIPD · analyse d'impact si risque élevé
- 5 Sécuriser · chiffrement · pseudonymisation · accès
- violation de données · notification à la CNIL sous 72 heures.

PI vs RGPD & IA

Critère	PI · droit d'auteur	RGPD
Protégé	Création	Données perso
Titulaire	Créateur	Personne physique
Durée	70 ans post mortem	Limitée à la nécessité
Régulateur	INPI · tribunaux	CNIL

Privacy by Design & by Default · AI Act (UE, 2024) · responsabilité humaine pour les IA.