

# RGPD

4 January 2026 • 7 min de lecture

Insights

RGPD

## Décryptage du RGPD : Le guide complet article par article

Entré en vigueur en **mai 2018**, le RGPD (GDPR en anglais) est le texte de référence mondial pour la protection des données personnelles. Il ne s'agit pas d'interdire la collecte de données, mais de **responsabiliser** les acteurs et de redonner le **contrôle** aux citoyens.

Voici le résumé structuré de l'intégralité du texte pour comprendre vos obligations et les droits des utilisateurs.

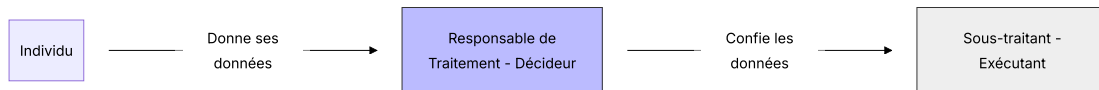
### Dispositions Générales (Art. 1 - 4)

*De quoi parle-t-on et qui est concerné ?*

**Ce qu'il faut retenir** : Le RGPD s'applique à toute organisation (entreprise, asso, administration) qui traite des données de résidents européens, **même si l'organisation est basée hors de l'UE**.

- **Art. 2 (Champ d'application)** : Concerne tout traitement automatisé (informatique) ou fichier papier structuré.
- **Art. 4 (Définitions clés)** :
  - **Donnée personnelle** : Toute info identifiant une personne directement (Nom) ou indirectement (IP, cookie, numéro de téléphone).
  - **Traitement** : Collecte, stockage, modification, suppression, etc.

- **Responsable de traitement (Controller)** : Celui qui décide du "pourquoi" et du "comment" (ex: l'entreprise qui vend le produit).
- **Sous-traitant (Processor)** : Celui qui traite les données pour le compte du responsable (ex: l'hébergeur cloud, le logiciel de paie).



## Les Grands Principes (Art. 5 - 11)

*Les règles d'or à respecter avant même de collecter.*

C'est la boussole éthique et légale du RGPD. Si vous ne respectez pas ces principes, tout le reste est illégal.

### Les 6 Principes de l'Article 5

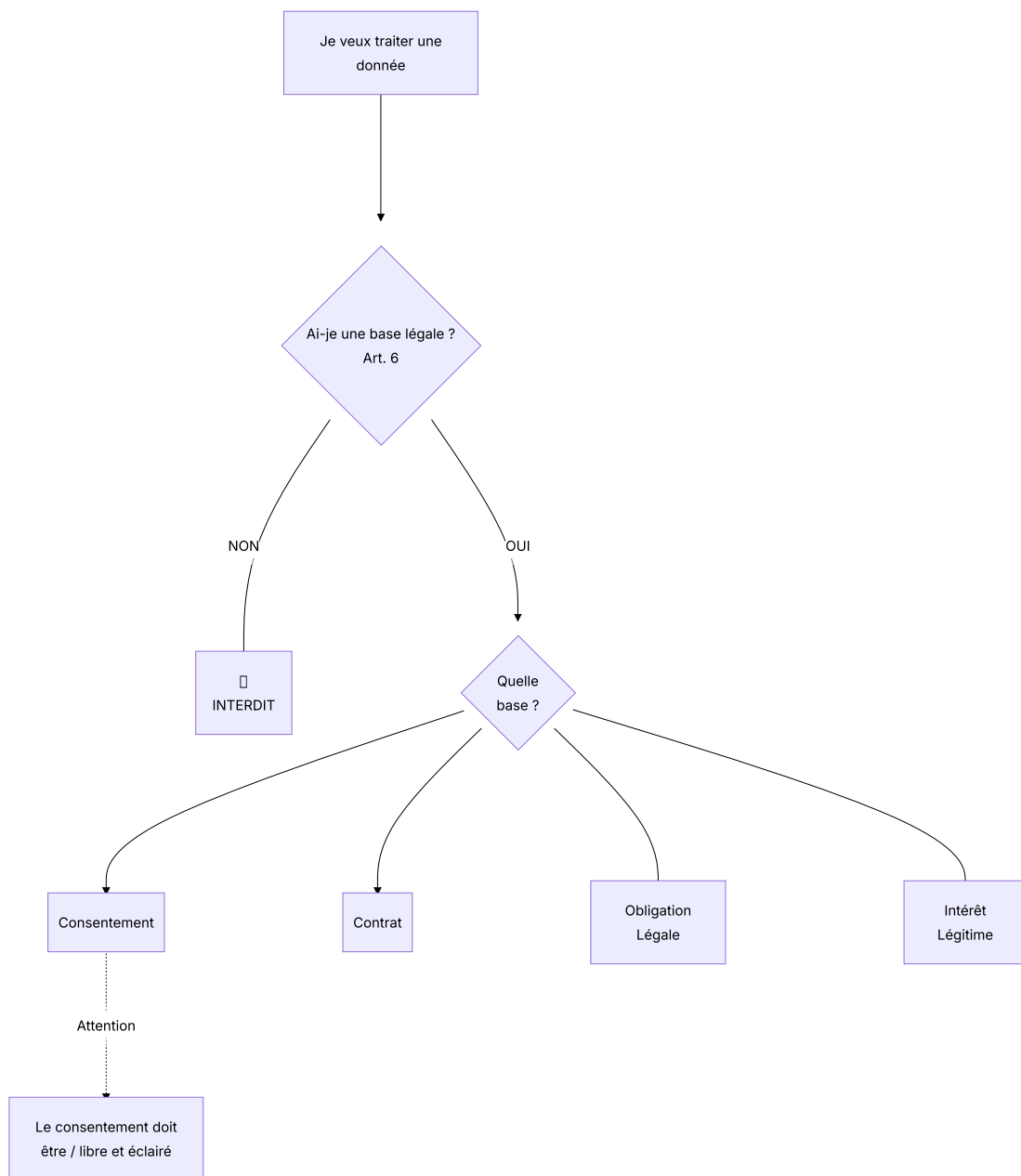
1. **Licéité, loyauté, transparence** : Ne rien faire dans le dos de l'utilisateur.
2. **Limitation des finalités** : On ne collecte pas des données "au cas où". Si on collecte pour livrer un colis, on ne s'en sert pas pour faire de la pub sans le dire.
3. **Minimisation** : Collecter le strict nécessaire (pas besoin de la date de naissance pour une newsletter).
4. **Exactitude** : Les données doivent être à jour.
5. **Limitation de la conservation** : On ne garde pas les données éternellement (ex: suppression des CV après 2 ans).
6. **Intégrité et confidentialité** : Sécuriser les données (contre le piratage ou la perte).

### La Base Légale (Art. 6)

Pour traiter une donnée, il faut **une** justification parmi les 6 suivantes :

- **Consentement** : L'utilisateur a dit "Oui" (ex: Newsletter).

- **Contrat** : Nécessaire pour fournir le service (ex: Adresse pour livraison).
- **Obligation légale** : La loi l'impose (ex: Factures pour les impôts).
- **Intérêt vital** : Sauver une vie (ex: Urgence médicale).
- **Mission d'intérêt public** : Pour les impôts, la sécu, etc.
- **Intérêt légitime** : Nécessaire pour l'entreprise sans nuire à la personne (ex: Prévention de la fraude).



# Droits des Personnes (Art. 12 - 23)

*Le pouvoir aux utilisateurs.*

Les citoyens disposent de droits qu'ils peuvent exercer à tout moment.

L'entreprise a **1 mois** pour répondre.

- **Art. 13-14 (Information)** : Droit de savoir ce qu'on fait de mes données (Politique de confidentialité).
- **Art. 15 (Accès)** : "Montrez-moi tout ce que vous avez sur moi."
- **Art. 16 (Rectification)** : "Corrigez mon adresse, elle est fausse."
- **Art. 17 (Oubli / Effacement)** : "Supprimez-moi de vos bases" (sauf si une loi oblige à garder la donnée).
- **Art. 20 (Portabilité)** : "Rendez-moi mes données dans un fichier Excel/CSV pour que j'aille chez un concurrent."
- **Art. 21 (Opposition)** : "Arrêtez de m'envoyer de la pub."

**Exemple** : Un utilisateur quitte Spotify pour Deezer. Il peut demander la **portabilité** de ses playlists (Art. 20) pour ne pas tout refaire manuellement.

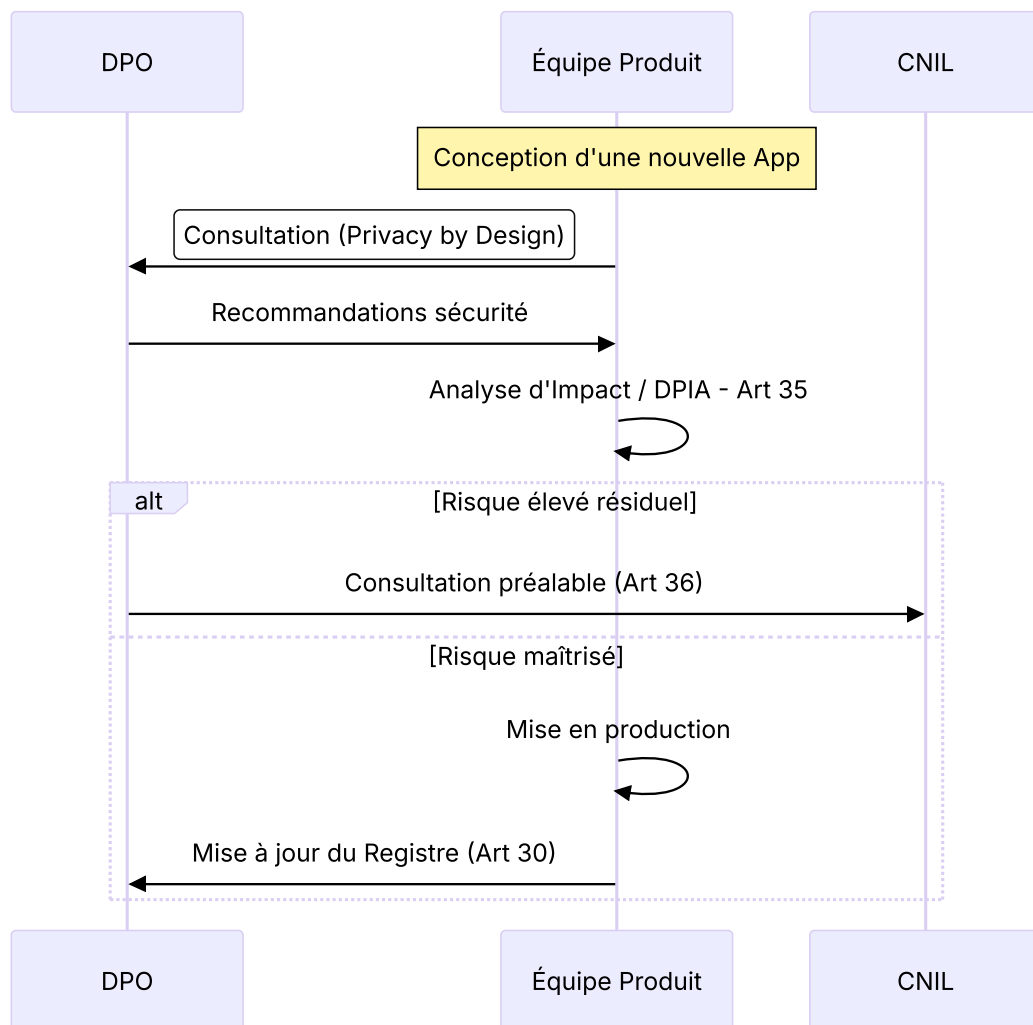
# Responsabilité et Conformité (Art. 24 - 43)

*Les devoirs des entreprises (Accountability).*

Il ne suffit pas de respecter la loi, il faut pouvoir **prouver** qu'on la respecte.

- **Art. 25 (Privacy by Design & Default)** : La protection des données doit être intégrée dès la conception du produit (ex: case décochée par défaut).
- **Art. 28 (Sous-traitance)** : Un contrat écrit est obligatoire entre le Responsable et le Sous-traitant pour définir les responsabilités.
- **Art. 30 (Registre)** : Tenir un registre des activités de traitement (obligatoire pour les organismes > 250 employés ou si traitement sensible).
- **Art. 32 (Sécurité)** : Chiffrement, pseudonymisation, sauvegardes.
- **Art. 33-34 (Fuite de données)** : En cas de piratage, prévenir la CNIL sous **72h** et les utilisateurs si le risque est élevé.

- **Art. 35 (DPIA - Analyse d'impact)** : Obligatoire pour les traitements à haut risque (ex: vidéosurveillance à grande échelle, données de santé).
- **Art. 37 (DPO - Délégué à la protection des données)** : Obligatoire pour les organismes publics et ceux qui traitent des données sensibles à grande échelle.



## Transferts Internationaux (Art. 44 - 50)

*Faire sortir les données de l'UE.*

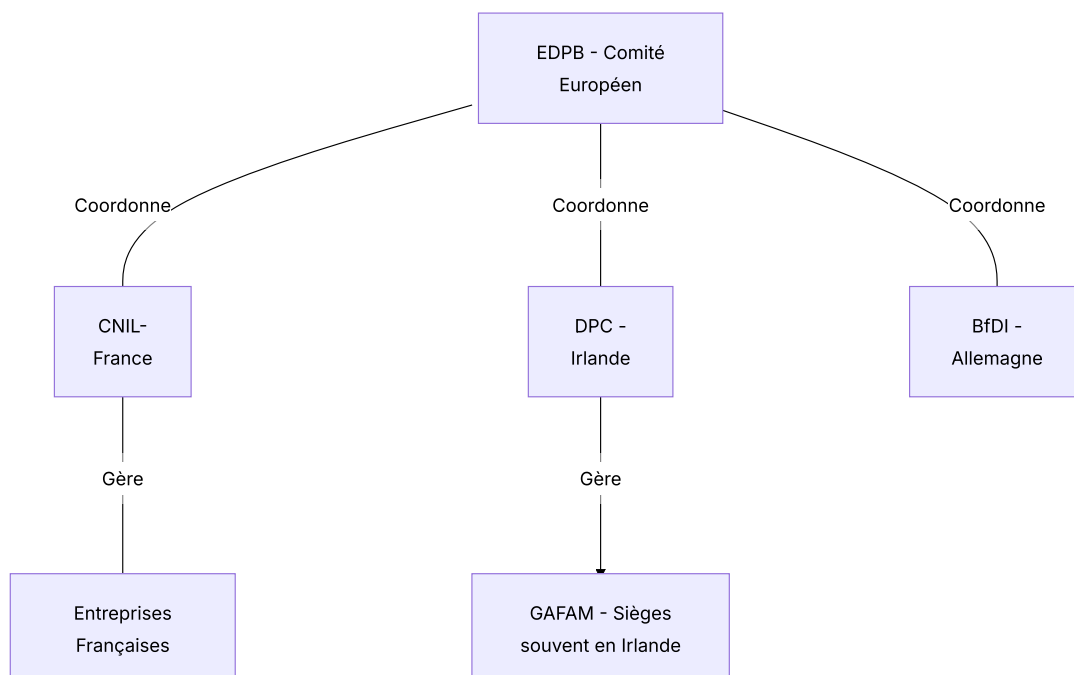
**Principe** : Les données doivent rester dans l'Espace Économique Européen (EEE). **Exceptions pour transférer dehors (ex: USA, Inde)** :

1. **Décision d'adéquation (Art. 45)** : L'UE dit "Ce pays est sûr" (ex: Suisse, Japon, Royaume-Uni, et récemment USA sous le *Data Privacy Framework*).
2. **Clauses Contractuelles Types (CCT - Art. 46)** : Modèles de contrats rédigés par l'UE à faire signer au partenaire étranger.
3. **BCR (Règles d'entreprise contraignantes)** : Pour les grands groupes internationaux.

## Autorités et Coopération (Art. 51 - 76)

*Les gendarmes de la donnée.*

- **Art. 51 (Autorité de contrôle)** : Chaque pays a son gendarme (France = CNIL).
- **Art. 56 (Guichet unique)** : Si une entreprise agit dans toute l'Europe (ex: Amazon), elle n'a affaire qu'à une seule autorité principale (celle de son siège social européen, souvent l'Irlande ou le Luxembourg).
- **EDPB (Comité Européen)** : Réunit toutes les CNIL d'Europe pour harmoniser les règles et trancher les conflits.



## Sanctions et Recours (Art. 77 - 84)

*Le bâton.*

Les citoyens peuvent porter plainte auprès de la CNIL (Art. 77) ou attaquer en justice pour obtenir réparation (dommages et intérêts - Art. 82).

**Les Amendes Administratives (Art. 83) :** Il existe deux niveaux de plafonds selon la gravité de l'infraction :

Type d'infraction	Amende Max	% du CA Mondial
<b>Niveau 1</b> (Manque de sécurité, registre mal tenu, etc.)	<b>10 Millions €</b>	<b>2 %</b>
<b>Niveau 2</b> (Non-respect des droits, consentement, principes de base)	<b>20 Millions €</b>	<b>4 %</b>

*Note : Pour les GAFAM, 4% du chiffre d'affaires mondial représente des milliards d'euros (ex: Amazon a été condamné à 746 M€).*

## Dispositions spécifiques (Art. 85 - 91)

*Les ajustements nationaux.*

Le RGPD laisse une marge de manœuvre aux États pour certains sujets :

- **Droit du travail :** Les RH peuvent traiter des données spécifiques selon le droit local.
- **Liberté d'expression :** Les journalistes bénéficient d'exceptions pour pouvoir informer.
- **Recherche et Statistique :** Régimes dérogatoires pour la science.

---

© 2026 Eric Blaudez. All rights reserved.

[LinkedIn](#)

---

Les opinions exprimées sur ce site sont strictement personnelles et ne reflètent pas nécessairement celles de mon employeur. Les contenus sont fournis à titre informatif et ne constituent pas un conseil juridique.