MANUEL UNIVERSITAIRE

RGPD

Règlement Général sur la Protection des Données

Fondamentaux & Sanctions CNIL

2025 : Année record des sanctions CNIL

487 millions d'euros d'amendes

83 sanctions prononcées

Rémy JUSTON-COUMAT

Édition 2025-2026

Sommaire

1. Introduction au RGPD

Le Règlement Général sur la Protection des Données (RGPD) est entré en application le 25 mai 2018 dans l'ensemble de l'Union européenne. Ce texte fondateur constitue le cadre juridique de référence pour la protection des données personnelles des citoyens européens.

> 📚 **Définition clé**
>
> Données personnelles : toute information se rapportant à une personne physique identifiée ou identifiable, directement (nom, prénom) ou indirectement (adresse IP, cookies, géolocalisation).

Le RGPD s'applique à toute organisation, publique ou privée, qui traite des données personnelles de résidents européens, y compris les entreprises situées hors de l'UE qui proposent des biens ou services aux Européens.

1.1 Pourquoi le RGPD ?

Avant le RGPD, la directive 95/46/CE de 1995 régissait la protection des données. Face à l'explosion du numérique, ce texte était devenu obsolète. Le RGPD apporte plusieurs avancées majeures :

- Harmonisation des règles au niveau européen
- Renforcement des droits des personnes
- Responsabilisation des entreprises (accountability)
- Sanctions dissuasives (jusqu'à 4% du CA mondial)

> 📊 **Chiffres clés en France**
>
> 16 433 plaintes reçues par la CNIL en 2024 (+8%)
> 487 millions d'euros d'amendes prononcées en 2025 (record historique)
> 83 sanctions en 2025, contre 87 en 2024

2. Les principes fondamentaux du RGPD

L'article 5 du RGPD définit six principes essentiels que tout traitement de données personnelles doit respecter. Ces principes constituent le socle de la conformité RGPD.

2.1 Licéité, loyauté et transparence

Le traitement doit être licite (fondé sur une base légale), loyal (pas de collecte à l'insu des personnes) et transparent (information claire des personnes).

> ⚖️ **Les 6 bases légales du traitement**
>
> 1. Consentement de la personne concernée
> 2. Exécution d'un contrat
> 3. Obligation légale
> 4. Sauvegarde des intérêts vitaux
> 5. Mission d'intérêt public
> 6. Intérêts légitimes du responsable de traitement

2.2 Limitation des finalités

Les données doivent être collectées pour des finalités déterminées, explicites et légitimes. Elles ne peuvent pas être traitées ultérieurement de manière incompatible avec ces finalités.

2.3 Minimisation des données

Seules les données adéquates, pertinentes et limitées à ce qui est nécessaire doivent être collectées. C'est le principe du « data minimization ».

> 🚨 **Exemple de manquement sanctionné**
>
> Une société pharmaceutique et un hôpital ont été sanctionnés en 2025 pour avoir filmé l'accès à un local syndical via vidéosurveillance : collecte excessive non nécessaire à l'objectif de sécurité.

2.4 Exactitude

Les données doivent être exactes et tenues à jour. Les données inexactes doivent être effacées ou rectifiées sans tarder.

2.5 Limitation de la conservation

Les données ne doivent pas être conservées au-delà de la durée nécessaire aux finalités du traitement. Des durées de conservation doivent être définies.

2.6 Intégrité et confidentialité

Le responsable de traitement doit garantir une sécurité appropriée des données, notamment contre les traitements non autorisés, la perte ou la destruction.

> 🔒 **Attention : Sécurité insuffisante**
>
> La sécurité des données est le premier motif de sanction en procédure simplifiée.
> 14 organismes sanctionnés en 2025 pour ce seul motif.

France Travail : 5 M€ d'amende (janvier 2026) pour défaut de sécurité.

3. Les sanctions CNIL : panorama 2024-2026

La Commission Nationale de l'Informatique et des Libertés (CNIL) dispose d'un pouvoir de sanction considérable. L'année 2025 marque un tournant historique avec près de 487 millions d'euros d'amendes, soit 9 fois plus qu'en 2024.

3.1 Évolution des sanctions

Année	Nb sanctions	Montant total	Tendance
2022	21	**101 M€**	-
2023	42	**89 M€**	↑ +100%
2024	87	**55 M€**	↑ +107%
2025	83	**487 M€**	↑ x9

3.2 Les sanctions majeures 2024-2026

Voici les sanctions les plus significatives prononcées récemment, illustrant les priorités de contrôle de la CNIL :

Entreprise	Amende	Motif principal
Google	**325 M€**	Cookies déposés sans consentement valable
Shein	**150 M€**	Non-respect de la législation cookies
Orange	**50 M€**	Publicités dans les boîtes mail sans consentement
Free Mobile + Free	**42 M€**	Défaut de sécurité des données clients
France Travail	**5 M€**	Sécurité insuffisante des données demandeurs d'emploi
Programme fidélité (anonyme)	**3,5 M€**	Transmission de données à un réseau social
Nexpublica	**1,7 M€**	Sécurité insuffisante du logiciel PCRM
Mobius (sous-traitant Deezer)	**1 M€**	Violation de données utilisateurs

3.3 Les trois axes de contrôle prioritaires

A. Cookies et traceurs publicitaires

21 sanctions en 2025 pour non-respect des règles cookies. La CNIL cible particulièrement les pratiques suivantes :

- Dépôt de cookies sans consentement préalable
- Bouton « Refuser » moins visible que « Accepter »
- Information insuffisante sur les finalités des cookies

> 🔴 **Cas Google (325 M€) - Septembre 2025**
>
> Motif : dépôt de cookies publicitaires sur les utilisateurs Google sans recueil d'un consentement valable.
>
> La CNIL a considéré que Google « ne pouvait ignorer les règles applicables » compte tenu de la communication de l'autorité depuis plusieurs années.

B. Vidéosurveillance des salariés

16 organismes sanctionnés en 2025. La surveillance vidéo permanente des salariés est considérée comme une atteinte disproportionnée, sauf circonstances exceptionnelles (sécurité, lutte contre le vol).

> ✓ **Bonnes pratiques vidéosurveillance**
>
> Ne pas filmer les salariés en continu à leur poste de travail
>
> Informer les salariés et les représentants du personnel
>
> Limiter la durée de conservation des images (30 jours max)
>
> Ne jamais filmer les espaces de pause, vestiaires ou locaux syndicaux

C. Sécurité des données

Premier motif de sanction en procédure simplifiée. Les manquements les plus fréquents :

- Mots de passe insuffisamment robustes
- Absence de chiffrement des données sensibles
- Contrôle d'accès défaillant
- Sous-traitants non encadrés contractuellement

4. Les procédures de sanction

La CNIL dispose de deux procédures pour prononcer des sanctions, adaptées à la gravité et à la complexité des dossiers.

4.1 La procédure ordinaire

Pour les affaires complexes ou les sanctions élevées. La formation restreinte de la CNIL (5 membres) se prononce après instruction contradictoire. Pas de plafond d'amende.

En 2025 : 16 sanctions par la formation restreinte, représentant l'essentiel des montants (Google, Shein, Free...).

4.2 La procédure simplifiée

Créée en 2022 pour les dossiers « ne présentant pas de difficulté particulière ». Le président de la formation restreinte statue seul. Amende plafonnée à 20 000 €.

En 2025 : 67 sanctions via procédure simplifiée (81% du total). Cette procédure accélère considérablement le traitement des dossiers.

> ⚖️ **Comparaison des procédures**
>
> Procédure ordinaire : formation restreinte, pas de plafond, publicité possible
>
> Procédure simplifiée : président seul, max 20 000 €, généralement anonymisée

4.3 Les mesures correctives

Outre les amendes, la CNIL dispose d'un arsenal de mesures progressives :

1. Rappel aux obligations légales : simple avertissement sans sanction (64 en 2024)
2. Mise en demeure : ordre de se conformer dans un délai fixé (180 en 2024)
3. Injonction sous astreinte : obligation assortie d'une pénalité journalière
4. Amende administrative : jusqu'à 20 M€ ou 4% du CA mondial

> ⚠️ **Attention : Non-coopération**
>
> 27 organismes sanctionnés en 2024 pour défaut de coopération avec la CNIL.
>
> Le simple fait de ne pas répondre aux sollicitations de l'autorité constitue un manquement à l'article 18 de la loi Informatique et Libertés.

5. Se mettre en conformité : les essentiels

La conformité RGPD n'est pas une option mais une obligation légale. Voici les étapes clés pour une mise en conformité efficace.

5.1 Cartographier ses traitements

Le registre des traitements est obligatoire pour toute organisation de plus de 250 salariés (et pour certains traitements sensibles en dessous). Il doit recenser :

- Les finalités de chaque traitement
- Les catégories de données et de personnes concernées
- Les destinataires des données
- Les durées de conservation et mesures de sécurité

5.2 Sécuriser les données

🔐 Mesures de sécurité minimales

Politique de mots de passe robustes (12 caractères min, complexité)
Chiffrement des données sensibles (en transit et au repos)
Gestion des habilitations et contrôle d'accès
Sauvegardes régulières et testées
Journalisation des accès aux données sensibles
Procédure de gestion des violations de données

5.3 Informer et respecter les droits

Les personnes doivent être informées de manière claire et accessible. Une politique de confidentialité complète doit mentionner :

- L'identité du responsable de traitement
- Les finalités et bases légales des traitements
- Les droits des personnes et comment les exercer
- Les transferts hors UE éventuels

👤 Les droits des personnes

Droit d'accès : obtenir une copie de ses données
Droit de rectification : corriger des données inexactes
Droit à l'effacement (« droit à l'oubli ») : supprimer ses données
Droit à la portabilité : récupérer ses données dans un format réutilisable
Droit d'opposition : refuser un traitement (notamment prospection)
Droit à la limitation : geler temporairement un traitement

6. Conclusion : les enjeux pour le e-commerce

Le secteur du e-commerce et du marketing digital est particulièrement exposé aux contrôles de la CNIL. Les cookies publicitaires, la prospection commerciale et la gestion des comptes clients sont autant de zones de risque.

> 🛒 **Points de vigilance e-commerce**
>
> Bandeau cookies conforme : bouton Refuser aussi visible qu'Accepter
> Consentement opt-in pour la newsletter (case non pré-cochée)
> Durée de conservation des comptes clients inactifs (3 ans max recommandé)
> Sécurisation des paiements et données bancaires
> Contrats sous-traitants (hébergeur, paiement, livraison)

Le RGPD n'est pas seulement une contrainte juridique : c'est aussi un argument commercial. 87% des consommateurs européens déclarent se soucier de la protection de leurs données. Une conformité RGPD visible renforce la confiance et peut devenir un avantage concurrentiel.

> 📌 **À retenir**
>
> Le RGPD s'applique à toute organisation traitant des données de résidents européens
> Les sanctions CNIL sont en forte hausse : 487 M€ en 2025 (record historique)
> Cookies et sécurité sont les deux priorités de contrôle
> La conformité est un processus continu, pas un projet ponctuel
> Documenter ses actions est essentiel (accountability)

Sources et références

- CNIL - Bilan des sanctions 2024 et 2025
- Règlement (UE) 2016/679 (RGPD)
- Loi n°78-17 du 6 janvier 1978 modifiée (Loi Informatique et Libertés)
- Décisions de sanctions CNIL (cnil.fr)