Checklist RGPD 2026 : Tout ce qu'il faut savoir

Guide complet et checklist actionnable pour la conformité au Règlement Général sur la Protection des Données

---

Table des Matières

---

1. Introduction au RGPD 2026

Qu'est-ce que le RGPD ?

Le **Règlement Général sur la Protection des Données (RGPD)** ou **General Data Protection Regulation (GDPR)** est un règlement européen entré en vigueur le 25 mai 2018. Il établit un cadre juridique unique pour la protection des données personnelles au sein de l'Union européenne.

Important 2026 : Le RGPD continue d'évoluer avec de nouvelles interprétations, jurisprudences et lignes directrices. Les organisations doivent rester à jour avec les dernières exigences.

Champ d'Application

Le RGPD s'applique à :

- **Toutes les organisations** (entreprises, associations, administrations) traitant des données personnelles
- **Quelle que soit la taille** (y compris les TPE/PME et micro-entreprises)
- **Quelle que soit la localisation** si les données concernent des résidents de l'UE

- **Tous les types de traitement** (collecte, stockage, utilisation, transmission, suppression)

Données Personnelles : Définition Élargie

Les données personnelles incluent :

- **Données d'identification** : nom, prénom, adresse, numéro de téléphone, email
- **Données numériques** : adresse IP, cookies, identifiants en ligne
- **Données sensibles** : origine ethnique, opinions politiques, convictions religieuses, données de santé, données biométriques
- **Données professionnelles** : poste, employeur, numéro de sécurité sociale
- **Données comportementales** : historique de navigation, habitudes d'achat

---

2. Principes Fondamentaux du RGPD

Les 7 Principes Clés

1. **Licéité, loyauté et transparence**
    - Les données doivent être traitées de manière licite, loyale et transparente
    - Information claire des personnes concernées
2. **Finalité**
    - Les données doivent être collectées pour des finalités déterminées, explicites et légitimes
    - Ne pas utiliser les données de manière incompatible avec la finalité déclarée
3. **Minimisation des données**
    - Ne collecter que les données strictement nécessaires
    - Limiter la durée de conservation
4. **Exactitude**
    - Mettre à jour les données inexactes
    - Supprimer ou rectifier les données erronées
5. **Limitation de la conservation**
    - Conserver les données sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire aux finalités
6. **Intégrité et confidentialité**

- Sécuriser les données contre les traitements non autorisés ou illicites
- Protéger contre la perte, la destruction ou les dégâts accidentels

7. **Responsabilité**
   - Le responsable de traitement doit pouvoir démontrer la conformité au RGPD

---

3. Checklist Complète de Conformité

☑ Étape 1 : Gouvernance et Responsabilités

- **Désigner un DPO** (Délégué à la Protection des Données) si requis
  - Obligatoire pour : organismes publics, traitements à grande échelle, données sensibles, surveillance systématique
  - Coordonnées du DPO publiées et communiquées à la CNIL
- **Nommer un responsable de traitement** pour chaque traitement de données
- **Établir un registre des activités de traitement** (obligatoire pour les organisations de plus de 250 employés ou traitements à risque)
- **Mettre en place une politique de protection des données** écrite et accessible
- **Former le personnel** sur les obligations RGPD
- **Sensibiliser la direction** aux enjeux de protection des données

☑ Étape 2 : Cartographie des Données

- **Identifier tous les traitements** de données personnelles
- **Cartographier les flux de données** (origine, destination, durée de conservation)
- **Classer les données** par niveau de sensibilité
- **Documenter la base juridique** pour chaque traitement
  - Consentement
  - Exécution d'un contrat
  - Obligation légale
  - Intérêt légitime
  - Mission d'intérêt public
  - Protection des intérêts vitaux
- **Identifier les sous-traitants** et vérifier leur conformité RGPD

☑ Étape 3 : Information des Personnes Concernées

- **Rédiger une politique de confidentialité** claire et accessible
- **Mettre à jour les mentions d'information** sur tous les supports (site web, formulaires, contrats)
- **Informer sur** :
    - Identité et coordonnées du responsable de traitement
    - Finalités du traitement
    - Base juridique du traitement
    - Destinataires des données
    - Durée de conservation
    - Droits des personnes concernées
    - Existence d'une prise de décision automatisée
    - Transfert international de données (le cas échéant)
- **Adapter le langage** selon le public cible (clients, employés, prospects)

☑ Étape 4 : Droits des Personnes

- **Mettre en place des procédures** pour exercer les droits :
    - Droit d'accès
    - Droit de rectification
    - Droit à l'effacement (droit à l'oubli)
    - Droit à la limitation du traitement
    - Droit à la portabilité des données
    - Droit d'opposition
- **Répondre aux demandes** dans un délai d'1 mois (prorogeable de 2 mois pour les demandes complexes)
- **Ne pas facturer** l'exercice des droits (sauf cas exceptionnels)
- **Vérifier l'identité** de la personne faisant la demande
- **Documenter** toutes les demandes et réponses

☑ Étape 5 : Sécurité des Données

- **Mettre en œuvre des mesures techniques et organisationnelles** adaptées aux risques

- **Chiffrer les données sensibles** (au repos et en transit)
- **Pseudonymiser ou anonymiser** les données lorsque possible
- **Limiter l'accès** aux données (principe du moindre privilège)
- **Mettre en place des sauvegardes** régulières et sécurisées
- **Protéger contre les cyberattaques** (pare-feu, antivirus, détection d'intrusion)
- **Sécuriser les accès distants** (VPN, authentification forte)
- **Gérer les mots de passe** selon les bonnes pratiques (complexité, rotation)

☑ **Étape 6 : Analyse d'Impact (PIA)**

- **Identifier les traitements à risque** (évaluation des risques pour les droits et libertés)
- **Réaliser une Analyse d'Impact (PIA)** pour les traitements à haut risque :
  - Utilisation de nouvelles technologies
  - Surveillance systématique de zones accessibles au public
  - Traitement de données sensibles à grande échelle
  - Profilage automatisé avec effets juridiques ou significatifs
- **Consulter la CNIL** si le PIA indique un risque résiduel élevé
- **Documenter et archiver** les PIA réalisés

☑ **Étape 7 : Gestion des Violations de Données**

- **Mettre en place un processus de détection** des violations de données
- **Définir des procédures de réponse** aux violations
- **Notifier la CNIL** sous 72 heures en cas de violation présentant un risque pour les droits et libertés
- **Informer les personnes concernées** sans délai indu si risque élevé
- **Documenter** toutes les violations et les mesures correctives mises en place

☑ **Étape 8 : Contrats et Sous-Traitance**

- **Vérifier que tous les contrats** avec les sous-traitants incluent les clauses RGPD requises
- **Exiger des garanties** de conformité RGPD des sous-traitants
- **Mettre en place des Accords de Traitement des Données (DPA)** avec chaque sous-traitant
- **Vérifier les sous-traitants des sous-traitants** (chaîne de sous-traitance)

- **Conserver une liste à jour** de tous les sous-traitants

☑ **Étape 9 : Transfert International de Données**

- **Identifier les transferts** de données en dehors de l'UE/EEE
- **Vérifier les mécanismes de transfert** :
    - Décision d'adéquation de la Commission européenne
    - Clauses contractuelles types (SCC)
    - Règles d'entreprise contraignantes (BCR)
    - Dérogations spécifiques
- **Mettre à jour les contrats** avec les mécanismes de transfert appropriés
- **Documenter les évaluations** de transfert
- **Surveiller les évolutions** juridiques (ex: Schrems II, nouvelles décisions d'adéquation)

☑ **Étape 10 : Documentation et Preuves de Conformité**

- **Conserver tous les documents** prouvant la conformité :
    - Registre des activités de traitement
    - Politiques et procédures
    - PIA réalisés
    - Contrats avec les sous-traitants
    - Preuves de formation du personnel
    - Registre des violations de données
    - Registre des demandes d'exercice des droits
- **Mettre à jour régulièrement** la documentation
- **Archiver** les anciennes versions pour preuve d'évolution

---

4. Nouvelles Exigences 2026

Évolutions Récentes

Renforcement des Obligations pour les Cookies

- **Vérifier la conformité** des bannières de cookies
- **Obtenir un consentement explicite** (pas de cases pré-cochées)
- **Permettre le refus aussi facile que l'acceptation**

- **Conserver les preuves de consentement** (qui, quand, comment)
- **Respecter la durée de conservation** des cookies (13 mois maximum pour les cookies de mesure d'audience)

Protection des Données des Enfants

- **Vérifier l'âge** des utilisateurs pour les services en ligne
- **Obtenir le consentement parental** pour les enfants de moins de 15 ans (16 ans dans certains pays)
- **Adapter les informations** de protection des données pour les enfants
- **Limiter la collecte** de données pour les services destinés aux enfants

Intelligence Artificielle et RGPD

- **Évaluer l'impact** des systèmes d'IA sur la protection des données
- **Garantir la transparence** des décisions automatisées
- **Permettre l'intervention humaine** dans les décisions automatisées ayant des effets juridiques ou significatifs
- **Respecter les droits** des personnes concernées par les traitements automatisés

Données Biométriques et de Santé

- **Renforcer la protection** des données biométriques (visage, empreintes, iris)
- **Sécuriser les données de santé** avec des mesures supplémentaires
- **Limiter l'accès** aux données sensibles
- **Obtenir un consentement explicite** pour le traitement des données sensibles

Jurisprudence Récente

- **Amendes record** pour non-conformité (ex: Meta 1,2 milliard d'euros en 2023)
- **Interprétation stricte** du consentement
- **Responsabilité accrue** des responsables de traitement
- **Obligation de transparence renforcée**

---

5. Droits des Personnes Concernées

Droit d'Accès (Article 15)

Ce que cela implique :

- Fournir une copie des données personnelles traitées

- Informer sur les finalités du traitement
- Indiquer les catégories de données concernées
- Communiquer les destinataires ou catégories de destinataires
- Préciser la durée de conservation

Délai : 1 mois (prorogeable de 2 mois)

Droit de Rectification (Article 16)

Ce que cela implique :

- Corriger les données inexactes
- Compléter les données incomplètes
- Informer les tiers ayant reçu les données de la rectification

Délai : 1 mois

Droit à l'Effacement (Droit à l'Oubli) (Article 17)

Cas où il s'applique :

- Les données ne sont plus nécessaires aux finalités
- La personne retire son consentement
- La personne s'oppose au traitement
- Les données ont été traitées illégalement
- Effacement requis par une obligation légale

Exceptions :

- Exercice du droit à la liberté d'expression
- Respect d'une obligation légale
- Motifs d'intérêt public
- Établissement, exercice ou défense de droits en justice

Droit à la Limitation du Traitement (Article 18)

Cas où il s'applique :

- La personne conteste l'exactitude des données
- Le traitement est illicite mais la personne s'oppose à l'effacement
- Les données ne sont plus nécessaires mais la personne en a besoin pour des droits en justice

Droit à la Portabilité (Article 20)

Ce que cela implique :

- Fournir les données dans un format structuré, couramment utilisé et lisible par machine
- Transmettre directement à un autre responsable si techniquement possible

Conditions :

- Traitement basé sur le consentement ou un contrat
- Traitement automatisé

Droit d'Opposition (Article 21)

Ce que cela implique :

- Permettre à la personne de s'opposer au traitement pour des raisons tenant à sa situation particulière
- Cesser le traitement sauf motifs légitimes impérieux

Opposition au marketing direct :

- Doit être respectée sans condition
- Doit être facile à exercer (lien de désabonnement visible)

---

6. Obligations par Type d'Organisation

Entreprises Privées

Taille	Obligations Spécifiques
Micro-entreprise	Désignation DPO si traitement à risque, registre si traitement régulier, respect des droits
TPE/PME	Désignation DPO si traitement à risque, registre obligatoire, PIA si traitement à risque
Grande entreprise	DPO obligatoire, registre obligatoire, PIA obligatoire pour traitements à risque, documentation complète

Organismes Publics

- **DPO obligatoire** dans tous les cas
- **Registre des activités de traitement obligatoire**
- **Publication des informations** sur le traitement des données
- **Respect strict** des finalités d'intérêt public

Associations

- **DPO obligatoire** si traitement régulier et systématique de données sensibles
- **Registre obligatoire** si plus de 250 membres ou traitement à risque
- **Information claire** des adhérents sur l'utilisation de leurs données

Professionnels de Santé

- **Protection renforcée** des données de santé
- **Chiffrement obligatoire** des données médicales
- **Désignation d'un DPO** obligatoire
- **Respect du secret médical** en plus du RGPD

---

7. Gestion des Violations de Données

Définition d'une Violation de Données

Une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière.

Procédure de Gestion

Étape 1 : Détection

- Mettre en place des systèmes de détection (SIEM, monitoring)
- Former le personnel à reconnaître les signes de violation
- Établir des canaux de signalement interne

Étape 2 : Évaluation

- Évaluer la nature et l'étendue de la violation
- Identifier les catégories de données concernées
- Déterminer le nombre de personnes affectées
- Évaluer le risque pour les droits et libertés

Étape 3 : Containment

- Prendre des mesures immédiates pour limiter l'impact
- Isoler les systèmes affectés si nécessaire
- Empêcher l'accès non autorisé

Étape 4 : Notification

À la CNIL (sous 72 heures) :

- Décrivez la nature de la violation
- Indiquez les catégories de données concernées
- Fournissez le nombre approximatif de personnes concernées
- Décrivez les conséquences probables
- Décrivez les mesures prises ou proposées

Aux personnes concernées (sans délai indu si risque élevé) :

- Langage clair et compréhensible
- Description de la nature de la violation
- Conseils sur les mesures à prendre
- Coordonnées du DPO

Étape 5 : Documentation

- Documenter tous les aspects de la violation
- Conserver les preuves des actions entreprises
- Mettre à jour les procédures en fonction des leçons apprises

Exemples de Violations

Type de Violation	Exemple	Risque	Notification CNIL	Notification Personnes
Accès non autorisé	Piratage de base de données	Élevé	Oui	Oui
Perte de données	Vol de laptop non chiffré	Moyen	Oui	Selon évaluation
Divulgation accidentelle	Email envoyé à mauvais destinataire	Faible	Non	Non
Ransomware	Chiffrement des données	Élevé	Oui	Oui

---

8. Transfert International de Données

Mécanismes de Transfert Valides

1. Décision d'Adéquation

- Pays reconnu par la Commission européenne comme offrant un niveau de protection adéquat

- **Exemples 2026** : Japon, Canada, Royaume-Uni, Corée du Sud, etc.
- Vérifier la liste à jour sur le site de la Commission européenne

2. Clauses Contractuelles Types (SCC)

- Clauses standard adoptées par la Commission européenne
- Utiliser la version la plus récente (2021)
- Adapter les clauses au contexte spécifique
- Conserver une copie signée des clauses

3. Règles d'Entreprise Contraignantes (BCR)

- Règles internes approuvées par une autorité de protection des données
- Applicable aux groupes multinationaux
- Processus d'approbation long et complexe

4. Dérogations Spécifiques

- Consentement explicite de la personne concernée
- Exécution d'un contrat
- Intérêt public
- Protection des intérêts vitaux
- Documenter la base juridique de la dérogation

Schrems II et Conséquences

- **Évaluer le niveau de protection** dans le pays destinataire
- **Mettre en place des mesures supplémentaires** si nécessaire
- **Documenter l'évaluation** des risques
- **Surveiller les évolutions** juridiques

Checklist Transfert International

- Identifier tous les transferts de données hors UE/EEE
- Vérifier le mécanisme de transfert utilisé
- Mettre à jour les contrats avec les clauses appropriées
- Réaliser une évaluation des risques pour chaque transfert
- Documenter les décisions et évaluations
- Surveiller les changements réglementaires

9. Sanctions et Risques

Montant des Amendes

Type de Violation	Amende Maximale
Infractions liées aux obligations (articles 83.4)	Jusqu'à **10M€ ou 2% du CA mondial** (le montant le plus élevé)
Infractions liées aux droits (articles 83.5)	Jusqu'à **20M€ ou 4% du CA mondial**
Infractions liées aux transferts internationaux	Jusqu'à **20M€ ou 4% du CA mondial**

Exemples d'Amendes Récentes

Entreprise	Montant	Motif	Année
Meta (Facebook)	1,2 Md€	Transfert illégal de données vers les États-Unis	2023
Amazon	746 M€	Publicité ciblée sans consentement valable	2021
Google	50 M€	Manquement aux obligations d'information	2019
CNIL (France)	40 M€	Non-respect du droit d'opposition	2020

Risques Non Financiers

- **Atteinte à la réputation** de l'organisation
- **Perte de confiance** des clients et partenaires
- **Restrictions** sur le traitement des données
- **Obligation** de mettre en conformité sous surveillance
- **Responsabilité pénale** pour les dirigeants (dans certains cas)

Facteurs Aggravants

- Nature intentionnelle ou négligente de l'infraction