RGPD : Protection des données personnelles

Partie 2 - Formation complète

Sommaire

Introduction au RGPD : Historique et contexte

Le Règlement Général sur la Protection des Données (RGPD) est entré en vigueur le 25 mai 2018, remplaçant la directive européenne de 1995. Il constitue le cadre de référence européen en matière de protection des données personnelles.

Objectifs principaux

- **Harmonisation européenne**
  Unifier les règles dans les 27 États membres
- **Renforcement des droits**
  Meilleur contrôle des citoyens sur leurs données
- **Responsabilisation des entreprises**
  Obligation de démontrer la conformité (accountability)
- **Adaptation au numérique**
  Réponse aux défis du big data, IA et cloud

Chronologie

1995
Directive européenne 95/46/CE
Premier cadre juridique européen sur la protection des données

2012
Lancement des négociations
Début des travaux sur un règlement unifié

2016
Adoption du RGPD
Publication officielle du texte final

2018
Entrée en application
Application effective le 25 mai 2018

2024
Évolutions avec l'IA Act
Nouvelles règles spécifiques à l'IA

Champ d'application du RGPD

Critère d'établissement

S'applique aux responsables de traitement et sous-traitants **établis dans l'UE**, indépendamment du lieu où les données sont traitées.

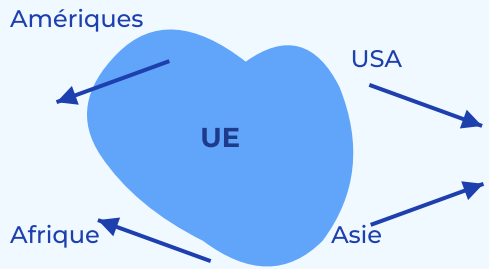
Critère de ciblage

S'applique aux organisations **hors UE** qui traitent des données de résidents européens dans le cadre :

- D'offre de biens ou services
- De suivi de comportement sur le territoire de l'UE

Principe d'extraterritorialité

Le RGPD peut s'appliquer **au-delà des frontières européennes**, créant des obligations pour des entreprises du monde entier.



Impact mondial :

Le RGPD a inspiré de nombreuses législations similaires dans le monde (CCPA en Californie, LGPD au Brésil), créant un standard global de protection des données.

Enjeux et principes fondamentaux

Les grands enjeux

Protection de la vie privée

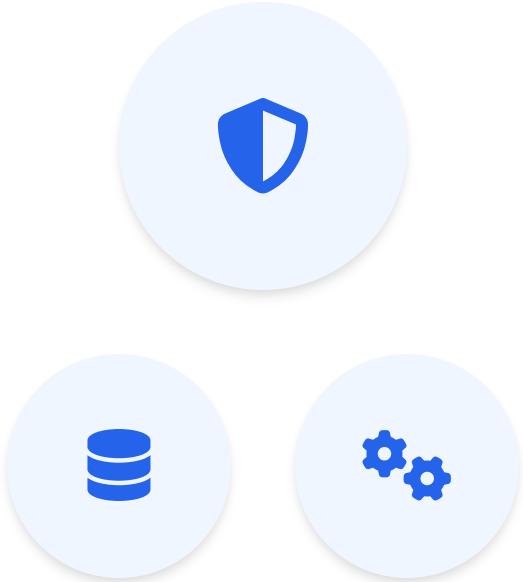
Droit fondamental reconnu dans l'UE, adaptation aux nouvelles technologies et encadrement des flux de données

Économie numérique

Renforcer la confiance des consommateurs et créer un avantage concurrentiel basé sur la protection des données

Innovation responsable

Permettre l'innovation tout en protégeant la vie privée et les droits fondamentaux des individus



Équilibre entre protection et innovation

Principes fondamentaux du RGPD

Licéité, loyauté et transparence
Traitement légal, équitable et avec information claire aux personnes concernées

Limitation des finalités
Collecte pour des finalités déterminées, explicites et légitimes

Minimisation des données
Données adéquates, pertinentes et limitées au strict nécessaire

Exactitude
Données exactes et tenues à jour, rectification des données inexactes

Limitation de la conservation
Conservation limitée à la durée nécessaire aux finalités

Intégrité et confidentialité
Protection contre le traitement non autorisé, la perte ou la destruction

Responsabilité (Accountability)
Obligation de démontrer la conformité aux principes du RGPD

Définitions clés : données personnelles

Définition légale

"Toute information se rapportant à une personne physique identifiée ou identifiable"

La personne peut être identifiée par des moyens raisonnablement susceptibles d'être utilisés.

Identification directe

- Nom et prénom
- Numéro de sécurité sociale
- Numéro de passeport
- Adresse postale

Identification indirecte

- Téléphone
- Email
- Adresse IP
- Cookie
- Plaque d'immatriculation
- Données biométriques

Critères d'identifiabilité

- Moyens raisonnablement susceptibles d'être utilisés
- Évolution prévisible des techniques
- Coût et temps nécessaires à l'identification

Responsable de traitement, sous-traitant et co-responsable

Responsable de traitement

Personne physique ou morale qui détermine les finalités et les moyens du traitement

- Pouvoir de décision sur les finalités
- Influence sur les moyens essentiels
- Bénéfice économique du traitement

Sous-traitant

Personne physique ou morale qui traite des données personnelles pour le compte du responsable

- Agit sur instruction du responsable
- N'a pas de pouvoir sur les finalités
- Relation contractuelle formalisée

Co-responsables

Plusieurs entités déterminent conjointement les finalités et moyens du traitement

- Responsabilité partagée et définie
- Accord transparent obligatoire
- Point de contact unique pour les personnes concernées

Relations entre les acteurs

Relations clés :

- Personne concernée → droits d'accès, rectification
- Responsable → définit finalités et moyens
- Sous-traitant → exécute selon instructions
- Co-responsables → décident ensemble

Données sensibles, données particulières

Le RGPD définit certaines catégories de données personnelles comme "particulièrement sensibles" en raison des risques qu'elles présentent pour les droits et libertés fondamentaux.

Catégories particulières de données

- Origine raciale ou ethnique
- Opinions politiques
- Convictions religieuses ou philosophiques
- Appartenance syndicale
- Données génétiques
- Données biométriques à des fins d'identification
- Données concernant la santé
- Vie sexuelle ou orientation sexuelle

Principe d'interdiction

Le traitement des données sensibles est **interdit par défaut**, sauf si l'une des 10 exceptions strictement définies par l'article 9 du RGPD s'applique.

Représentation visuelle

Données professionnelles & commerciales

Données RH

- **Données courantes**
  État civil, coordonnées, formation, diplômes, expérience professionnelle
- **Données de performance**
  Évaluations professionnelles, objectifs, compétences, évolution de carrière
- **Données sensibles en contexte RH**
  Données de santé (arrêts maladie, médecine du travail), données biométriques (contrôle d'accès), informations syndicales

Données clients et prospects

- **Données commerciales**
  Identité et coordonnées, historique d'achat, préférences et comportements, données de géolocalisation
- **Profilage commercial**
  Scores de solvabilité, segmentation comportementale, analyses prédictives
- **Précautions spécifiques**
  Information claire sur le profilage, droit d'opposition, limitation des données collectées, durées de conservation adaptées

Droits des personnes concernées

Le RGPD renforce considérablement les droits des personnes concernées, leur offrant un contrôle accru sur leurs données personnelles. Ces droits sont opposables à tout responsable de traitement, qui doit y répondre dans un délai d'un mois.

Comment exercer ses droits ?

- Demande écrite avec pièce d'identité
- Réponse sous 1 mois (extensible à 3 mois)
- Gratuit (sauf demandes infondées/excessives)
- Possibilité de recours auprès de l'autorité de contrôle

À noter

Certains droits peuvent être limités par des obligations légales ou l'intérêt public. Le responsable doit justifier tout refus d'exercice d'un droit.

Information et accès

Droit d'être informé des traitements et d'obtenir une copie des données

Rectification et effacement

Droit de corriger des données inexactes et d'obtenir l'effacement ("droit à l'oubli")

Limitation et portabilité

Droit de geler temporairement un traitement et de récupérer ses données

Opposition

Droit de s'opposer à un traitement, notamment pour motifs légitimes

Décision automatisée

Droit de ne pas faire l'objet d'une décision fondée uniquement sur un traitement automatisé

Exercice concret de ses droits

Demande écrite

La demande est à formuler de préférence par écrit avec une pièce d'identité pour vérification

Délais de réponse

Un mois à compter de la réception de la demande, prorogeable de deux mois en cas de complexité

Gratuité de principe

Gratuit sauf demandes manifestement infondées ou excessives (frais administratifs raisonnables possibles)

Exceptions et nuances

Limitations possibles pour obligation légale, motifs d'intérêt public, protection judiciaire ou sécurité nationale

Notification aux tiers

Le responsable de traitement doit informer les destinataires des données de toute rectification ou effacement, sauf effort disproportionné

Recours en cas de refus

Possibilité de saisir l'autorité de contrôle (CNIL) ou d'introduire un recours juridictionnel

Obligations des responsables de traitement

Le principe d'Accountability

Le responsable de traitement doit être en mesure de **démontrer** sa conformité au RGPD à tout moment. Il s'agit d'une approche **proactive** et non plus seulement réactive.

Documentation obligatoire
Registre des traitements, analyses d'impact (AIPD), politiques internes

Privacy by Design
Intégration de la protection des données dès la conception des traitements

Privacy by Default
Paramètres par défaut respectueux de la vie privée et minimisation automatique

Délégué à la Protection des Données
Désignation obligatoire dans certains cas (autorité publique, suivi à grande échelle, données sensibles)

Checklist de conformité

- **Tenir un registre des traitements**
  Cartographier tous les traitements de données personnelles
- **Réaliser des analyses d'impact (AIPD)**
  Pour les traitements susceptibles de présenter des risques élevés
- **Documenter les mesures de sécurité**
  Techniques et organisationnelles pour garantir la sécurité des données
- **Encadrer les relations avec les sous-traitants**
  Contrats conformes à l'article 28 du RGPD
- **Désigner un DPO si nécessaire**
  Indépendant, compétent et disposant des ressources adéquates

Registre, DPO & Documentation

Registre des traitements

- Obligatoire pour toutes les entreprises (sauf exceptions)
- Exemption pour les TPE (<250 employés), sauf si traitement non occasionnel ou risqué
- Contient : finalités, catégories de personnes/données, destinataires, délais d'effacement
- Version responsable et version sous-traitant

Documentation obligatoire

- Registre des traitements et des violations
- Analyses d'impact sur la protection des données (AIPD)
- Politique de protection des données
- Procédures internes de gestion des droits et incidents

Missions du DPO

- Informer et conseiller l'organisation et ses employés
- Contrôler le respect du RGPD et d'autres dispositions
- Dispenser formation et sensibilisation au personnel
- Coopérer avec l'autorité de contrôle et servir de point de contact
- Participer aux analyses d'impact et donner son avis

Indépendance et statut du DPO

- Ne peut recevoir d'instructions sur l'exercice de ses missions
- Absence de conflit d'intérêts avec d'autres fonctions
- Accès direct à la direction et autonomie d'action
- Ressources et moyens nécessaires pour exercer ses missions

Licéité du traitement des données

Les 6 bases légales

Consentement
Libre, spécifique, éclairé et univoque, avec possibilité de retrait

Contrat
Nécessaire à l'exécution d'un contrat ou de mesures précontractuelles

Obligation légale
Obligation prévue par le droit de l'UE ou national (fiscal, comptable...)

Intérêts vitaux
Protection des intérêts vitaux de la personne ou d'un tiers

Mission d'intérêt public
Exécution d'une mission d'intérêt public ou relevant de l'autorité publique

Intérêt légitime
Équilibre entre intérêt légitime et droits fondamentaux de la personne

Cas particuliers

Traitement des données des mineurs
- Âge du consentement : 16 ans (ou minimum 13 ans selon les États)
- Autorisation parentale obligatoire sous cet âge
- Information adaptée à la compréhension des enfants

Traitement des données des employés
- Déséquilibre de pouvoir : consentement rarement approprié
- Bases recommandées : contrat, obligation légale, intérêt légitime
- Transparence renforcée et principe de proportionnalité

Décisions automatisées et profilage
- Base légale spécifique pour le traitement sous-jacent
- Droit de ne pas faire l'objet d'une décision automatisée
- Exceptions : contrat, autorisation légale, consentement explicite
- Garanties : intervention humaine, contestation possible

Sécurité des données & gestion des violations

Mesures de protection

Mesures techniques

- Chiffrement des données (transit et stockage)
- Pseudonymisation et anonymisation
- Sauvegarde régulière et sécurisée
- Contrôle d'accès strict et authentification

Mesures organisationnelles

- Politiques de sécurité documentées
- Formation et sensibilisation du personnel
- Gestion des habilitations et accès
- Audits de sécurité réguliers

⚠ Gestion des violations de données

En cas de violation de données personnelles, notification :

À l'autorité de contrôle dans les 72 heures

Sauf si pas de risque pour les droits et libertés des personnes

Protection technique

Notification des violations

Contrôles et vérifications

Transferts internationaux de données

Principe général

Interdiction de principe : Les transferts de données personnelles vers un pays tiers sont interdits, sauf garanties appropriées.

Niveau de protection : Assurance d'un niveau de protection essentiellement équivalent au RGPD.

Mécanismes de transfert

Décisions d'adéquation

Reconnaissance par la Commission européenne qu'un pays tiers offre un niveau de protection adéquat (Japon, Suisse, Royaume-Uni...)

Clauses contractuelles types (SCC)

Contrats standardisés adoptés par la Commission européenne, mis à jour en 2021 suite à l'arrêt Schrems II

Règles d'entreprise contraignantes (BCR)

Politiques internes aux groupes multinationaux, approuvées par les autorités de contrôle

Codes de conduite et certifications

Mécanismes volontaires approuvés avec engagements contraignants

Pays UE Pays tiers

Pays avec décision d'adéquation :

- Andorre
- Argentine
- Canada (comm.)
- Suisse
- Japon
- Nouvelle-Zélande
- Royaume-Uni
- Corée du Sud

Sanctions et contrôles

Autorités nationales

Autorités indépendantes dans chaque État membre avec pouvoirs d'enquête, correctifs et d'autorisation

Mécanisme de cohérence

Comité européen de la protection des données (CEPD) adoptant des avis et lignes directrices harmonisées

Amendes administratives

- Catégorie 1 : jusqu'à 10 millions € ou 2% du CA mondial
- Catégorie 2 : jusqu'à 20 millions € ou 4% du CA mondial

Mesures correctrices

- Avertissements et mises en demeure
- Limitation ou interdiction temporaire/définitive des traitements
- Suspension des flux de données internationaux

Critères de détermination

Aggravants

- Gravité et durée de la violation
- Caractère intentionnel
- Préjudice subi par les personnes

Atténuants

- Coopération avec l'autorité
- Notification proactive
- Mesures techniques préventives

RGPD & IA générative : enjeux spécifiques

Défis posés par l'IA générative

Collecte massive
Utilisation de volumes importants de données provenant de sources diverses pour l'entraînement

Réutilisation non prévue
Utilisation des données pour des finalités non initialement communiquées

Mémorisation
Risque de reproduction de données d'entraînement contenant des informations personnelles

Biais algorithmiques
Reproduction et amplification des biais présents dans les données

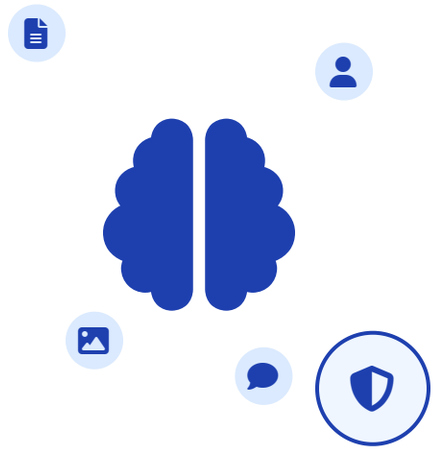
Spécificités de conformité

Phase d'entraînement
Base légale adaptée et test de proportionnalité rigoureux

Gestion des logs
Traitement conforme des données d'entrée, de sortie et métadonnées

Droits d'accès/effacement
Mécanismes techniques pour localiser et supprimer les données des modèles

Anonymisation avancée
Techniques sophistiquées comme la confidentialité différentielle



Bonnes pratiques pour la conformité

La conformité RGPD est un processus continu qui nécessite une approche structurée et des mesures à la fois techniques et organisationnelles.

Cycle de conformité RGPD

1

Audit initial

Cartographie des traitements et évaluation des risques

2

Plan d'action

Priorisation et allocation des ressources

3

Gouvernance

Politiques, procédures et responsabilités

4

Formation

Sensibilisation et compétences des équipes

5

Privacy by Design

Intégration dès la conception des projets

6

Contrôle continu

Audits et amélioration continue

Facteurs clés de succès :

- Implication de la direction et ressources adéquates
- Documentation complète et maintenue à jour
- Outils adaptés pour la gestion des droits
- Veille réglementaire et adaptation continue

Conclusion & messages clés

> Le RGPD impose de vraies garanties et une démarche de conformité continue, notamment pour l'IA générative qui représente un défi particulier en matière de protection des données.

Respect des droits fondamentaux

Protection effective des droits des personnes concernées malgré la complexité technique des systèmes

Accountability

Démonstration de la conformité par une documentation rigoureuse et des mesures proactives

Adaptation continue

Veille réglementaire et technologique pour anticiper les évolutions et maintenir la conformité

Leviers techniques

Privacy by design, minimisation, anonymisation et chiffrement comme fondements de la protection

Leviers organisationnels

Gouvernance, formation, responsabilisation et culture de la protection des données à tous les niveaux