2026

GUIDE RGPD

Les essentiels de la conformité
en 8 points clés

Stéphane Ulmer Conseil

Consultant RGPD & DPO Externe

Introduction

Pourquoi ce guide ?

Le Règlement Général sur la Protection des Données (RGPD) est en vigueur depuis mai 2018, et pourtant, de nombreuses organisations peinent encore à se mettre en conformité. Les contrôles de la CNIL se multiplient, et les sanctions peuvent être lourdes : jusqu'à 20 millions d'euros ou 4% du chiffre d'affaires annuel mondial.

Ce guide vous présente les **8 points essentiels** pour assurer la conformité RGPD de votre organisation. Chaque point est expliqué de manière claire et actionnable, avec des exemples concrets.

⚠️ Attention

La conformité RGPD n'est pas un projet ponctuel mais un processus continu. Ce guide vous donne les bases, mais chaque organisation a des besoins spécifiques qui nécessitent souvent un accompagnement personnalisé.

À qui s'adresse ce guide ?

- **Municipalités et collectivités** : gérant des données de citoyens
- **Établissements de santé** : traitant des données de santé sensibles
- **Sites e-commerce** : collectant des données clients et utilisant des cookies
- **Associations** : gérant des fichiers de membres et donateurs
- **PME et entreprises** : traitant des données personnelles de clients ou employés

✅ Ce que vous allez apprendre

En 8 pages pratiques, vous découvrirez comment mettre en place les piliers fondamentaux de la conformité RGPD, éviter les erreurs courantes, et préparer votre organisation à un éventuel contrôle de la CNIL.

Point 1 : Le Registre des Traitements

Le document fondamental de votre conformité

Le registre des traitements est le document central de votre conformité RGPD. Il recense tous les traitements de données personnelles effectués par votre organisation.

Qu'est-ce qu'un traitement de données ?

Un traitement est toute opération effectuée sur des données personnelles : collecte, enregistrement, conservation, consultation, utilisation, transmission, effacement, etc.

Exemples de traitements :

- Gestion des candidatures (recrutement)
- Gestion de la paie et des RH
- Fichier clients et prospects
- Gestion des accès au bâtiment (badge)
- Vidéosurveillance
- Newsletter et campagnes marketing

Que doit contenir le registre ?

Pour chaque traitement, vous devez documenter :

1. **La finalité** : pourquoi collectez-vous ces données ?
2. **Les catégories de données** : nom, email, adresse, données de santé...
3. **Les catégories de personnes** : employés, clients, prospects...
4. **Les destinataires** : qui a accès aux données ?
5. **La durée de conservation** : combien de temps gardez-vous les données ?
6. **Les mesures de sécurité** : comment protégez-vous les données ?

> 💡 **Conseil pratique**
>
> Commencez par lister tous vos fichiers Excel, bases de données, logiciels qui contiennent des noms, emails ou autres données personnelles. Chaque fichier correspond généralement à un traitement différent.

⚠️ Erreur fréquente

Beaucoup d'organisations créent un registre incomplet puis l'oublient. Le registre doit être **maintenu à jour** : chaque nouveau traitement doit y être ajouté.

Point 2 : La Désignation du DPO

Le pilote de votre conformité RGPD

Le Délégué à la Protection des Données (DPO) est la personne responsable de la mise en œuvre et du suivi de la conformité RGPD dans votre organisation.

Qui doit désigner un DPO ?

La désignation d'un DPO est **obligatoire** pour :

- **Toutes les autorités et organismes publics** (municipalités, hôpitaux publics, administrations)
- Les organisations dont les activités principales nécessitent un **suivi régulier et systématique** des personnes à grande échelle
- Les organisations traitant à grande échelle des **données sensibles** (santé, origine ethnique, opinions politiques...)

> 💡 **En pratique**
>
> Même si vous n'êtes pas légalement obligé de désigner un DPO, c'est fortement recommandé. Cela démontre votre engagement en matière de protection des données et facilite vos relations avec la CNIL.

DPO interne ou externe ?

DPO interne :

- ✅ Connaissance approfondie de l'organisation
- ✅ Disponibilité immédiate
- ❌ Coût d'un salaire complet
- ❌ Risque de conflits d'intérêts
- ❌ Formation continue nécessaire

DPO externe (mutualisé) :

- ✅ Expertise immédiate
- ✅ Coût maîtrisé (quelques jours par an)
- ✅ Indépendance garantie
- ✅ Veille juridique assurée
- ❌ Connaissance progressive de l'organisation

Les missions du DPO

1. **Informer et conseiller** : sensibiliser l'organisation aux obligations RGPD
2. **Contrôler** : vérifier la conformité des traitements
3. **Conseiller sur les analyses d'impact** : pour les traitements à risque
4. **Coopérer avec la CNIL** : être le point de contact
5. **Tenir le registre** : maintenir à jour la documentation

✅ Point d'attention

Le DPO doit être **déclaré à la CNIL** via le site internet de l'autorité. Ses coordonnées doivent également être publiées dans votre politique de confidentialité.

Point 3 : La Politique de Confidentialité

L'information transparente de vos contacts

La politique de confidentialité explique aux personnes comment vous collectez, utilisez et protégez leurs données personnelles. C'est une obligation légale qui doit être facilement accessible.

Où publier votre politique de confidentialité ?

- **Sur votre site web** : lien visible dans le footer
- **Dans vos formulaires** : mention et lien avant la collecte
- **Dans vos emails** : lien dans le footer
- **Dans vos documents** : mention dans les contrats, devis, etc.

Que doit contenir votre politique de confidentialité ?

1. **Identité du responsable de traitement**

   Nom de votre organisation, coordonnées, et coordonnées du DPO

2. **Finalités des traitements**

   Pourquoi collectez-vous des données ? (gestion des commandes, newsletter, recrutement...)

3. **Base légale**

   Sur quelle base juridique (consentement, contrat, obligation légale, intérêt légitime) ?

4. **Destinataires des données**

   Qui a accès aux données ? (employés, prestataires, partenaires)

5. **Durée de conservation**

   Combien de temps gardez-vous les données ?

6. **Droits des personnes**

   Droit d'accès, de rectification, d'effacement, d'opposition, de portabilité...

7. **Sécurité des données**

   Comment protégez-vous les données ? (chiffrement, accès restreints...)

8. **Cookies**

   Si votre site utilise des cookies, expliquez lesquels et pourquoi

⚠️ Erreurs courantes

- Politique de confidentialité copiée d'un autre site (non adaptée)
- Politique non mise à jour depuis des années
- Langage juridique trop complexe et incompréhensible
- Politique impossible à trouver sur le site

💡 Conseil pratique

Rédigez votre politique dans un langage clair et accessible. Évitez le jargon juridique. Vous pouvez utiliser un langage simple tout en restant conforme.

Point 4 : Le Consentement Valide

L'accord libre et éclairé de vos utilisateurs

Le consentement est l'une des bases légales les plus courantes pour traiter des données personnelles. Mais attention : un consentement RGPD doit respecter des règles strictes.

Les 4 critères d'un consentement valide

1. **Libre**

   La personne doit pouvoir refuser sans subir de préjudice. Pas de consentement "forcé".

2. **Spécifique**

   Un consentement par finalité. Vous ne pouvez pas demander un consentement global pour "tout".

3. **Éclairé**

   La personne doit comprendre à quoi elle consent (finalité claire, identité du responsable).

4. **Univoque**

   Acte positif clair (cocher une case, cliquer sur un bouton). Le silence ou l'inaction ne valent pas consentement.

Comment recueillir un consentement valide ?

✅ Bonnes pratiques

- **Case à cocher NON pré-cochée**
- Texte clair expliquant la finalité
- Possibilité de refuser facilement
- Conservation de la preuve du consentement (date, heure, contenu)
- Possibilité de retirer le consentement aussi facilement qu'il a été donné

Exemple de formulation correcte :

> J'accepte de recevoir la newsletter de [Nom de l'organisation] contenant des actualités et conseils sur [sujet]. Je peux me désinscrire à tout moment via le lien présent dans chaque email.

❌ Pratiques interdites

- Case pré-cochée
- Consentement via défilement de page ou navigation
- Consentement groupé pour plusieurs finalités distinctes
- "En continuant, vous acceptez..." (non-valide)
- Acceptation obligatoire de la newsletter pour acheter

Traçabilité du consentement

Vous devez pouvoir **prouver** que vous avez recueilli le consentement. Conservez :

- La date et l'heure du consentement
- Le contenu de l'information fournie
- La manière dont le consentement a été recueilli
- L'identité de la personne (email, ID unique)

Points 5 & 6 : Cookies et Sécurité

Point 5 : Les Cookies Conformes

Les cookies sont de petits fichiers déposés sur l'ordinateur des visiteurs de votre site. Leur utilisation est strictement encadrée par le RGPD et la directive ePrivacy.

Règle générale : Vous devez obtenir le **consentement préalable** avant de déposer des cookies, sauf pour les cookies strictement nécessaires au fonctionnement du site.

Cookies exemptés de consentement :

- Cookies de panier d'achat
- Cookies d'authentification
- Cookies de préférence de langue
- Cookies de sécurité

Cookies nécessitant un consentement :

- **Google Analytics** et autres outils de mesure d'audience
- **Facebook Pixel**, LinkedIn Insight Tag
- Cookies publicitaires (Google Ads, etc.)
- Cookies de réseaux sociaux (boutons de partage)
- Tout cookie qui n'est pas strictement nécessaire

Solution : Installer un gestionnaire de consentement conforme (banner cookie) qui :

- Bloque les cookies avant consentement
- Présente les finalités clairement
- Permet de refuser aussi facilement que d'accepter
- Conserve la preuve du consentement

Point 6 : La Sécurité des Données

Vous devez mettre en place des **mesures techniques et organisationnelles** appropriées pour protéger les données personnelles contre :

- La perte
- La destruction accidentelle
- L'accès non autorisé
- La divulgation non autorisée

✅ Mesures de sécurité essentielles

- **Mots de passe robustes** : au moins 12 caractères, changés régulièrement
- **Chiffrement** : des données sensibles et des communications (HTTPS)
- **Sauvegardes régulières** : quotidiennes et testées
- **Antivirus et pare-feu** : à jour
- **Accès restreints** : principe du moindre privilège
- **Journalisation** : traçabilité des accès
- **Formation du personnel** : sensibilisation sécurité

Points 7 & 8 : Droits et Contrats

Point 7 : Les Droits des Personnes

Le RGPD accorde aux personnes concernées plusieurs droits sur leurs données. Vous devez être en mesure de répondre à leurs demandes dans un **délai d'un mois**.

> **Les 8 droits des personnes :**
>
> 1. **Droit d'accès** : obtenir une copie de ses données
> 2. **Droit de rectification** : corriger des données inexactes
> 3. **Droit à l'effacement** : "droit à l'oubli"
> 4. **Droit à la limitation** : bloquer temporairement un traitement
> 5. **Droit d'opposition** : s'opposer à un traitement
> 6. **Droit à la portabilité** : récupérer ses données dans un format structuré
> 7. **Droit de ne pas faire l'objet d'une décision automatisée**
> 8. **Droit de définir des directives post-mortem**

Comment faciliter l'exercice des droits ?

- Publier une adresse email dédiée : dpo@votre-organisation.fr
- Mettre en place un formulaire en ligne
- Répondre dans le délai d'un mois
- Vérifier l'identité du demandeur
- Conserver la trace des demandes et réponses

Point 8 : Les Contrats Fournisseurs (DPA)

Dès qu'un prestataire traite des données personnelles pour votre compte (hébergeur, logiciel SaaS, service marketing...), vous devez conclure un **contrat de sous-traitance** (Data Processing Agreement - DPA).

Exemples de sous-traitants :

- Hébergeur de site web (OVH, AWS, etc.)
- Logiciel de gestion (CRM, ERP)
- Service d'emailing (Mailchimp, Sendinblue)
- Outils marketing (Google Analytics, Facebook)
- Prestataire de paie

✅ Clauses obligatoires du DPA

- Objet, durée, nature et finalité du traitement
- Type de données et catégories de personnes
- Obligations du sous-traitant (sécurité, confidentialité)
- Sous-traitance ultérieure (nécessite autorisation)
- Assistance au responsable de traitement
- Sort des données en fin de contrat

⚠️ Point d'attention : transferts hors UE

Si votre sous-traitant héberge des données hors de l'Union Européenne, vous devez mettre en place des **garanties appropriées** (clauses contractuelles types, règles d'entreprise contraignantes, ou certification).

Checklist de Conformité RGPD

Utilisez cette checklist pour évaluer rapidement votre niveau de conformité. Pour chaque point non coché, vous avez identifié un axe d'amélioration.

Documentation

- Registre des traitements créé et à jour
- DPO désigné et déclaré à la CNIL
- Politique de confidentialité publiée et accessible
- Mentions d'information sur tous les formulaires

Technique

- Cookies déposés uniquement après consentement
- Gestionnaire de consentement installé et configuré
- Site web en HTTPS (connexion sécurisée)
- Hébergement des données dans l'UE ou garanties appropriées
- Sauvegardes régulières et testées

Organisationnel

- Procédure d'exercice des droits mise en place
- Adresse email dédiée (ex: dpo@votre-organisation.fr)
- Contrats de sous-traitance (DPA) signés avec tous les prestataires
- Formation du personnel au RGPD réalisée

- Procédure de notification des violations de données définie

Formulaires et Consentement

- Cases à cocher NON pré-cochées
- Consentement granulaire (une case par finalité)
- Conservation de la preuve du consentement
- Possibilité de retirer le consentement facilement

🎯 Votre score

16-18 points : Excellente conformité ✅

12-15 points : Bonne base, quelques ajustements nécessaires ⚠️

8-11 points : Des progrès importants à réaliser 📋

< 8 points : Audit urgent recommandé ❌

Prochaines Étapes

Que faire maintenant ?

Ce guide vous a présenté les **8 piliers essentiels** de la conformité RGPD. Mais chaque organisation a des besoins spécifiques qui nécessitent un accompagnement personnalisé.

🎯 Audit Gratuit de 30 Minutes

Je vous offre un premier diagnostic gratuit de votre site web et de vos pratiques pour identifier vos priorités de mise en conformité.

Mes services d'accompagnement RGPD

📋 Audit RGPD Complet

- Analyse technique de votre site web (cookies, trackers, formulaires)
- Revue documentaire (registre, politiques, contrats)
- Rapport détaillé avec plan d'action priorisé
- Accompagnement post-audit

👤 DPO Externe Mutualisé

- Désignation officielle à la CNIL
- Tenue du registre des traitements
- Veille réglementaire
- Support et conseil continu
- Gestion des demandes d'exercice de droits

🎓 Formation RGPD

- Sensibilisation de vos équipes
- Formation des référents RGPD
- Ateliers pratiques

Me Contacter

Stéphane Ulmer
Consultant RGPD & DPO Externe

📧 **ulmer.stephane@suconseil.com**

🌐 **www.suconseil.com**

📅 Prenez rendez-vous pour votre audit gratuit de 30 minutes