

RGPD pour les développeurs web & web mobile

Introduction

Le **RGPD** (Règlement Général sur la Protection des Données) est une réglementation européenne entrée en vigueur le **25 mai 2018**. Il vise à protéger les données personnelles des citoyens de l'Union Européenne et s'applique à **toute organisation qui collecte ou traite des données personnelles**, y compris les développeurs et les entreprises web.

Objectifs du RGPD

- Renforcer les droits des personnes sur leurs données.
 - Responsabiliser les acteurs qui traitent les données.
 - Harmoniser les règles à l'échelle européenne.
-

Pourquoi c'est important pour les développeurs ?

En tant que développeur web ou web mobile, vous êtes souvent en première ligne pour :

- Concevoir des formulaires de collecte.
 - Gérer les cookies et traceurs.
 - Mettre en place des systèmes de stockage et de traitement des données.
 - Sécuriser les accès et les transmissions.
-

Données personnelles : définition

Les **données personnelles** sont toutes les informations permettant d'identifier **directement ou indirectement** une personne physique :

- Nom, prénom
 - Adresse email
 - Adresse IP
 - Identifiants de connexion
 - Localisation GPS
 - Données de navigation, etc.
-

Principes fondamentaux du RGPD

1. **Licéité, loyauté et transparence**

- L'utilisateur doit être informé clairement de la collecte de ses données.

2. **Limitation des finalités**

- Les données doivent être collectées pour un usage spécifique et légitime.

3. Minimisation des données

- On ne collecte que ce qui est **strictement nécessaire**.

4. Exactitude des données

- Les données doivent être à jour et exactes.

5. Limitation de la conservation

- Les données ne doivent pas être conservées indéfiniment.

6. Intégrité et confidentialité

- Les données doivent être protégées contre l'accès non autorisé.

Obligations techniques du développeur

Sécurité des données

- Utiliser HTTPS
- Hasher les mots de passe (bcrypt, Argon2...)
- Éviter les fuites de données dans les logs
- Appliquer les principes de sécurité "by design" et "by default"

Cookies & traceurs

- Afficher un **bandeau d'information** avant toute collecte.
- Demander un **consentement explicite** (opt-in).
- Permettre à l'utilisateur de **refuser ou personnaliser** les cookies.

Formulaires de collecte

- Informer l'utilisateur sur l'utilisation des données.
- Ajouter une case à cocher (non cochée par défaut) pour le consentement.
- Proposer un lien vers la **politique de confidentialité**.

Gestion des droits des utilisateurs

Vous devez permettre à l'utilisateur de :

- Accéder à ses données
- Les modifier ou les supprimer
- S'opposer à leur traitement
- Exporter ses données (portabilité)

Exemple : Check-list pour un site web conforme

- ☐ Consentement cookie (opt-in avant tracking)

- ☐ Formulaire clair avec mentions légales
- ☐ Données minimisées (pas de collecte inutile)
- ☐ Mots de passe stockés de façon sécurisée
- ☐ Politique de confidentialité disponible
- ☐ Possibilité de supprimer/modifier ses données
- ☐ Journalisation des accès aux données sensibles
- ☐ DPO (délégué à la protection des données) identifié si nécessaire

Sanctions en cas de non-respect

- Jusqu'à **20 millions d'euros** ou **4 % du chiffre d'affaires annuel mondial**, selon le montant le plus élevé.
- Mise en demeure de la CNIL
- Blocage ou suppression de votre site/app

Outils utiles

- [CNIL - RGD Développeur](#)
- [Cookie Consent Manager](#) (ex : [tarteacitron.js](#), [Cookiebot](#))
- [SecurityHeaders.com](#)
- [Let's Encrypt](#) pour les certificats SSL gratuits

Conclusion

Le RGPD n'est pas qu'un sujet juridique, c'est une **exigence technique et éthique**. En tant que développeur, vous jouez un rôle clé pour assurer la protection des données des utilisateurs.

 **Respecter le RGPD, c'est construire des sites plus fiables, plus transparents et plus respectueux des droits humains.**
