# Conformité RGPD en développement web

Support de cours pour la formation Conformité RGPD en développement web de Décembre 2024

Formateur : Dufrène Valérian

“Déclaration d’activité enregistrée sous le numéro 32800232680 auprès du préfet de région HAUTS-DE-FRANCE”

## Objectifs

La formation "**Conformité RGPD en développement web**" est découpée en 5 chapitres et est accessible à tout public ayant des notions de bases en développement web.

À l'issue de cette formation, les participants seront en mesure de :

- ➔ **Comprendre les enjeux** liés à la protection des données personnelles.
- ➔ **Identifier les principales obligations** du RGPD.
- ➔ **Mettre en place les actions nécessaires** pour se conformer au règlement.
- ➔ **Répondre aux questions** des personnes concernées.

À l'issue de cette formation, les développeurs web seront en mesure de :

- ➔ **Intégrer les principes du RGPD** dès la conception de leurs applications.
- ➔ **Mettre en œuvre des solutions techniques** pour garantir la protection des données personnelles.
- ➔ **Rédiger une documentation** claire et concise sur le traitement des données.
- ➔ **Collaborer efficacement** avec les autres acteurs de l'entreprise (DPO, juristes).

## Déroulé

- ➔ **Introduction au RGPD**
  - ◆ Rappel des fondamentaux du RGPD.
  - ◆ Les spécificités du traitement des données personnelles dans le développement web (cookies, analytics, formulaires, etc.).
  - ◆ Responsabilités des développeurs dans la mise en conformité.

- ➔ **Les principes clés du RGPD**
  - ◆ Licéité du traitement : consentement, base légale du traitement.
  - ◆ Minimisation des données : conception de formulaires, collecte de données strictement nécessaires.
  - ◆ Sécurité des données : protection des données personnelles lors du développement et du stockage.

- ➔ **Les droits des personnes concernées**
  - ◆ Droit d'accès, de rectification, d'effacement : mise en œuvre technique.

- Gestion des cookies : bandeau d'information, consentement, outils de gestion.
- Portabilité des données : formats de données, API.

➔ **Les sanctions en cas de non-respect du RGPD**
➔ **Les obligations des responsables de traitement**
➔ **Les bonnes pratiques de développement pour respecter le RGPD**
- Choix des technologies respectueuses de la vie privée.
- Cryptage des données, pseudonymisation, anonymisation.
- Tests de sécurité et audits réguliers.

➔ **Cas pratique**
- Mise en place de la maquette d'une bannière cookies.

## Spécificité dans le domaine du développement web

**Cookies et traceurs:**

➔ Typologie des cookies (techniques, de mesure d'audience, publicitaires).
➔ Obtention du consentement éclairé.
➔ Gestion des préférences de l'utilisateur.

**Formulaires de collecte de données:**

➔ Conception claire et concise des formulaires.
➔ Information sur l'utilisation des données collectées.
➔ Sécurité des formulaires (protection contre les injections SQL, XSS).

**Stockage des données:**

➔ Choix d'un hébergeur respectueux du RGPD.
➔ Sauvegardes et restauration des données.

**API et échanges de données:**

➔ Sécurité des API.
➔ Transferts de données en dehors de l'UE.

# Introduction au RGPD

## Qu’est-ce que la RGPD ?

Conformité RGPD en développement web

### Qu’est-ce que la RGPD ?

Le Règlement Général sur la Protection des Données (RGPD) est une loi européenne visant à protéger les données personnelles des individus.

Il établit un cadre juridique commun pour tous les pays de l'UE, garantissant ainsi un niveau de protection élevé pour les citoyens.


## Quelles données sont considérées comme des données personnelles ?

Conformité RGPD en développement web

### Quelles données sont considérées comme des données personnelles ?

Toute information relative à une personne physique identifiée ou identifiable est considérée comme une donnée personnelle.

Cela peut inclure le nom, l'adresse, le numéro de téléphone, l'adresse email, mais aussi des données plus sensibles comme les données de santé ou les opinions politiques.

## Qu’englobe réellement le traitement des données personnelles ?

Conformité RGPD en développement web

### Qu’englobe réellement le traitement des données personnelles ?

Le traitement des données personnelles englobe toutes les opérations effectuées sur ces données, telles que :

- la collecte
- l'enregistrement
- l'organisation
- la conservation
- l'adaptation
- la modification
- l'extraction
- la consultation
- l'utilisation
- la communication par transmission
- la diffusion ou toute autre forme de mise à disposition
- le rapprochement ou l'interconnexion
- le verrouillage
- l'effacement
- la destruction

## Les principes clés du RGPD

Conformité RGPD en développement web

### Les grands principes du RGPD

Le RGPD repose sur des principes fondamentaux tels que la **licéité**, la **loyauté** et la **transparence**, la **minimisation des données**, l'**exactitude**, la **conservation limitée**, l'**intégrité** et la **confidentialité**.

## Licéité, loyauté et transparence

Le traitement des données doit être **légal**, **loyal** et **transparent**.

Cela signifie que vous devez avoir une **base légale** pour **traiter les données** (**consentement**, **intérêt légitime**, **obligation légale**...), que le **traitement** doit être effectué de **manière loyale** et que **les personnes concernées doivent être informées** de **manière claire** et **complète** sur le **traitement de leurs données**.


Conformité RGPD en développement web

## Limitation des finalités

Les **données collectées** doivent être **adéquates**, **pertinentes** et **limitées** à ce qui est **nécessaire au regard des finalités déterminées**, **explicites** et **légitimes** pour lesquelles elles sont traitées.

En d'autres termes, vous ne pouvez **pas collecter de données pour une finalité et les utiliser pour une autre**.

## Exactitude

Les **données** doivent être **exactes** et, si nécessaire, **tenues à jour**.

Il est important de prendre des mesures pour **rectifier les données inexactes ou incomplètes**.


Conformité RGPD en développement web

## Limitation de la conservation

Les **données** ne doivent **pas être conservées au-delà de la durée nécessaire** au regard des finalités pour lesquelles elles sont traitées.

Vous devez **définir des durées de conservation adaptées** et **supprimer les données** lorsqu'elles ne sont plus utiles

## Intégrité et confidentialité

Les **données** doivent être **traitées de manière à assurer leur sécurité**, notamment en les **protégeant contre les traitements non autorisés ou illégaux**, la **perte**, la **destruction** ou les **dommages accidentels**.




## Principe de minimisation des données

Il signifie que vous ne devez **collecter que les données strictement nécessaires** pour atteindre les objectifs poursuivis.

Ce principe est **étroitement lié à la limitation des finalités**.

# Les droits des personnes concernées

Conformité RGPD en développement web

## Les droits des personnes concernées

Toute personne dont les données sont traitées dispose de **droits fondamentaux**.

Parmi les principaux, on retrouve :

Conformité RGPD en développement web

## Le droit d'accès

Toute personne a le droit de savoir si **ses données sont traitées** et, le cas échéant, **d'en obtenir une copie**.

## Le droit de rectification

Si les **données** sont **inexactes** ou **incomplètes**, la personne concernée peut **demander leur rectification**.



## Le droit à l'effacement (droit à l'oubli)

**Dans certains cas**, la personne peut demander la **suppression de ses données**.

## Le droit à la limitation du traitement

La personne peut demander la **suspension du traitement de ses données** dans certains cas précis.



## Le droit d'opposition

La personne peut **s'opposer au traitement de ses données**, notamment à des fins de **prospection commerciale**.

Conformité RGPD en développement web

## Le droit à la portabilité des données

La personne peut demander à **recevoir ses données** dans un **format structuré**, couramment utilisé et lisible par machine, **afin de les transmettre à un autre responsable de traitement**.

# Les droits des personnes concernées

Conformité RGPD en développement web

## Les sanctions en cas de non-respect du RGPD

Le **non-respect du RGPD** peut entraîner de **lourdes sanctions financières**.

Les **autorités de contrôle**, comme la **CNIL**, peuvent infliger des **amendes** pouvant atteindre jusqu'à **4 % du chiffre d'affaires mondial annuel d'une entreprise** ou **20 millions d'euros, selon le montant le plus élevé**.

Les sanctions peuvent également être **complémentaires**, comme l'**obligation de publier une décision de sanction**, des **mesures correctives** ou des **suspensions d'opérations de traitement**.

## Les obligations des responsables de traitement

Un responsable de traitement est toute personne physique ou morale, autorité publique, service ou organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement.

Les obligations des responsables de traitement sont nombreuses et détaillées dans le RGPD. Parmi les principales, on retrouve :

- ➔ **La mise en œuvre de mesures techniques et organisationnelles appropriées:** Pour garantir la sécurité des données et protéger les droits des personnes.
- ➔ **La tenue d'un registre des activités de traitement:** Un document qui recense toutes les opérations de traitement réalisées.
- ➔ **La désignation d'un délégué à la protection des données (DPO) dans certains cas:** Lorsque les activités de traitement sont susceptibles d'avoir des incidences importantes sur les droits et libertés des personnes.
- ➔ **La coopération avec les autorités de contrôle:** En fournissant les informations nécessaires à l'exercice de leurs missions.

## Les bonnes pratiques de développement pour respecter le RGPD

## Prise de conscience et formation

- **Comprendre les principes fondamentaux du RGPD:** Licéité, loyauté, transparence, minimisation des données, etc.
- **Identifier les données à caractère personnel (DCP):** Savoir reconnaître et catégoriser les différentes types de données collectées sur un site web (cookies, formulaires, etc.).
- **Sensibiliser toute l'équipe de développement:** Assurer une compréhension commune des enjeux.



## Identifier les données à caractère personnel (DCP)

Nous avons déjà vu **les principes fondamentaux du RGPD**, nous allons donc nous intéresser aux **DCP**.

**Exemples de DCP :**

- Données d'identification
- Données de localisation
- Données comportementales
- Données liées aux appareils

## Données d'identification - Exemple

- Nom
- Prénom
- Date de naissance
- Adresse postale
- Adresse électronique
- Numéro de téléphone
- Identifiants de connexion (nom d'utilisateur, mot de passe)
- Numéro de sécurité sociale (dans certains cas très spécifiques et avec une autorisation légale)



## Données de localisation - Exemple

- Adresse IP
- Données de géolocalisation (si l'utilisateur a autorisé leur utilisation)
- Historique de navigation

## Données comportementales - Exemple

- Historique de recherche
- Pages visitées
- Produits consultés
- Durée de visite sur chaque page
- Taux de rebond



## Données liées aux appareils - Exemple

- Type d'appareil (ordinateur, tablette, smartphone)
- Système d'exploitation
- Navigateur web
- Résolution d'écran

## Les moyens de collecte des DCP

- **Formulaires:**
  - Formulaires de contact
  - Formulaires d'inscription
  - Formulaires de commande
  - Sondages
- **Cookies:**
  - Cookies de session
  - Cookies persistants
  - Cookies tiers
- **Pixels espions:**
  - Pixels Facebook
  - Pixels Google Analytics
- **Balises web:**
  - Balises intégrées dans les emails



## Comment catégoriser les données ?

Pour catégoriser les données, il faut se poser les questions suivantes :

- **À qui appartiennent ces données ?** (à l'utilisateur, à l'entreprise, à un tiers ?)
- **Quelle est la finalité de la collecte de ces données ?** (améliorer l'expérience utilisateur, personnaliser les publicités, réaliser des analyses statistiques, etc.)
- **Quelle est la durée de conservation de ces données ?**

## Exemple concret : Site e-commerce

Collecte des données d'identification pour la création de compte, des données de localisation pour la livraison, des données comportementales pour personnaliser les recommandations de produits, et des données liées aux appareils pour optimiser l'affichage du site.

Conformité RGPD en développement web

## Exemple concret : Site d’informations

Collecte des données de navigation pour mesurer l'audience, des données de localisation pour proposer des contenus localisés et des données liées aux appareils pour adapter l'affichage aux différents supports.

## Exemple concret : Réseau social

Collecte un large éventail de données personnelles (nom, photo de profil, contacts, centres d'intérêt, etc.) pour proposer des services de socialisation, de ciblage publicitaire et d'analyse.



## Pourquoi est-il important de catégoriser les données ?

- → **Pour respecter le RGPD:** En identifiant les types de données collectées, vous pouvez évaluer si leur traitement est conforme aux principes du RGPD (licéité, minimisation des données, etc.).
- → **Pour mettre en place des mesures de sécurité adaptées:** Chaque type de données nécessite des mesures de sécurité spécifiques.
- → **Pour informer les utilisateurs:** Vous devez informer les utilisateurs des types de données collectées, de la finalité de leur traitement et de leurs droits.

## Cas pratique : Mise en place de la maquette d'une bannière cookie


**Objectif :** Créer une maquette de bannière cookie conforme au RGPD, permettant à l'utilisateur de donner son consentement de manière claire et informée.

**Éléments à inclure :**

- ➔ Informations claires et concises sur les types de cookies utilisés.
- ➔ Possibilité de personnaliser les préférences (accepter tous les cookies, refuser tous les cookies, choisir les cookies).
- ➔ Lien vers la politique de confidentialité.
- ➔ Bouton de validation du consentement.

**Conseils :**

- ➔ Utiliser un langage simple et clair.
- ➔ Éviter les termes juridiques trop complexes.
- ➔ Tester la bannière sur différents appareils et navigateurs.

## Exemple de logique à suivre pour cet exercice

**1. Analyse des besoins :**

- ➔ Quels types de cookies sont utilisés sur le site ? (techniques, de mesure d'audience, publicitaires)
- ➔ Quelles sont les informations à fournir à l'utilisateur ? (finalités des cookies, durée de conservation, etc.)
- ➔ Quelles sont les options de consentement proposées ? (tout accepter, tout refuser, choix personnalisé)

**2. Conception de la maquette :**

- ➔ **Visuel :**
  - ◆ Design simple et intuitif.
  - ◆ Utilisation de couleurs claires et contrastées.
  - ◆ Taille de police lisible.
- ➔ **Contenu :**
  - ◆ En-tête expliquant la finalité de la bannière.
  - ◆ Liste des catégories de cookies avec une description concise.
  - ◆ Options de consentement claires et bien différenciées.
  - ◆ Lien vers la politique de confidentialité.
- ➔ **Positionnement :**
  - ◆ La bannière doit être visible dès l'arrivée sur le site.
  - ◆ Elle ne doit pas bloquer l'accès au contenu.

**3. Développement technique :**

- ➔ **Choix de la technologie :**
  - ◆ Bibliothèque JavaScript spécialisée (Cookiebot, OneTrust, etc.)
  - ◆ Développement personnalisé (en utilisant des frameworks comme React, Angular, etc.)
- ➔ **Intégration dans le site :**
  - ◆ Placement de la bannière dans le code HTML.
  - ◆ Gestion des événements utilisateur (clic sur les boutons, fermeture de la bannière).
  - ◆ Stockage des préférences de l'utilisateur.