LIVRE BLANC

Comment savoir si mon site internet est conforme au RGPD

LA CHECKLIST

Oniti

À l'ère du numérique, où la présence en ligne est devenue une nécessité pour les entreprises et les individus, la protection des données personnelles est devenue un enjeu majeur. **Chaque jour, des milliers de données sont échangées, stockées et traitées sur le web, rendant la question de leur sécurité et de leur confidentialité d'autant plus cruciale.**

Le Règlement Général sur la Protection des Données (RGPD) est venu répondre à cette préoccupation croissante. Instauré pour encadrer le traitement des données personnelles sur le territoire de l'Union Européenne, il vise à renforcer le contrôle des citoyens sur l'utilisation de leurs données.

Mais comment s'assurer que son site est en conformité avec ce règlement ?

Ce livre blanc a pour objectif de vous fournir une checklist complète pour déterminer si votre site ***(site vitrine uniquement)*** respecte les exigences du RGPD.

Nous aborderons les fondamentaux du RGPD, les acteurs concernés, et les étapes clés pour garantir la conformité de votre site.

Que vous soyez un professionnel cherchant à optimiser la conformité de votre site ou simplement un curieux du numérique, ce guide est fait pour vous.

VOTRE PARCOURS

1. Introduction au RGPD

2. Applicabilité du RGPD

3. Vérification de la Conformité RGPD de votre Site Internet

1 INTRODUCTION AU RGPD

Définition du RGPD

Le Règlement Général sur la Protection des Données (RGPD) est **un cadre légal de l'Union Européenne** qui vise à **protéger les données personnelles des individus**. Mis en application le 25 mai 2018, il remplace la directive sur la protection des données de 1995.
Le RGPD impose de nouvelles obligations aux entreprises et organisations publiques et privées traitant des données de résidents européens, garantissant ainsi une meilleure maîtrise par les citoyens de **leurs données personnelles.**

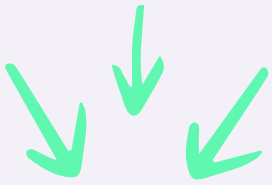
Rôle et importance de la CNIL

La Commission Nationale de l'Informatique et des Libertés (CNIL) joue un rôle crucial **dans l'application du RGPD en France**. En tant qu'autorité de contrôle, elle a pour mission de veiller à ce que le traitement des données personnelles se fasse **dans le respect des droits et libertés individuels.**
La CNIL guide également les entreprises et les organisations dans leur démarche de mise en conformité, tout en ayant le **pouvoir de sanctionner** les manquements au RGPD.

Qu'est-ce qu'une donnée personnelle ?

Une donnée personnelle est **toute information se rapportant à une personne physique identifiée ou identifiable**. Cela inclut des éléments tels que le nom, une photo, une adresse email, des données bancaires, des publications sur les réseaux sociaux, des informations médicales ou encore une adresse IP.

Le traitement de données personnelles désigne **toute opération ou ensemble d'opérations effectuées sur ces données**, quels que soient les moyens utilisés.



Cela comprend la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou 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, ainsi que l'effacement ou la destruction de données personnelles.

2

APPLICABILITÉ DU RGPD

Qui est concerné par le RGPD ?

Le RGPD s'applique **à toutes les organisations**, qu'elles soient dans l'Union Européenne ou non, **dès lors qu'elles traitent des données personnelles de résidents de l'UE**. Cela inclut non seulement les entreprises basées en Europe, mais aussi celles situées en dehors de l'UE si elles offrent des biens ou des services à des personnes dans l'UE ou surveillent leur comportement.

Ainsi, que vous soyez une PME, une startup, une multinationale, ou même une association, si vous traitez des données de citoyens de l'UE, **vous devez vous conformer au RGPD.**

Conséquences du non-respect du RGPD

Les conséquences du non-respect du RGPD peuvent être sévères. Les sanctions incluent des amendes substantielles qui peuvent atteindre **jusqu'à 4% du chiffre d'affaires annuel mondial de l'entreprise** ou 20 millions d'euros (selon le montant le plus élevé). Au-delà des aspects financiers, le non-respect peut également entraîner **une perte de confiance de la part des clients, une atteinte à la réputation de l'entreprise, et des conséquences juridiques impliquant des litiges et des compensations**. Il est donc crucial pour toute organisation de s'assurer de sa conformité au RGPD pour éviter ces risques.

3

CHECKLIST CONFORMITÉ RGPD DE VOTRE SITE

3 questions à vous poser

1

Mon site collecte t'il les données personnelles de mes visiteurs ?

2

Mon site partage t'il des données avec des tierces parties ?

3

Mon site rend t'il accessible les documents légaux nécéssaires ?

1

Mon site collecte t'il les données personnelles de mes visiteurs ?

La première étape pour assurer la conformité de votre site au RGPD est **d'identifier si et comment vous collectez des données personnelles**. Cela inclut toute information permettant d'identifier une personne, telle que le **nom, l'adresse email, l'adresse IP**, etc.

Les formulaires

Pensez aux formulaires de contact, aux inscriptions à des newsletters, et aux systèmes de commentaires.

Chaque point de collecte de données doit être conforme aux principes du RGPD : licéité, loyauté, transparence, finalité déterminée, minimisation des données, exactitude, limitation de la conservation, et intégrité et confidentialité.

Les cookies non nécessaires au bon fonctionnement du site

*Un cookie est un **petit fichier informatique, un traceur**, déposé et lu par exemple lors de la consultation d'un site internet, de la lecture d'un courrier électronique, de l'installation ou de l'utilisation d'un logiciel ou d'une application mobile et ce, quel que soit le type de terminal utilisé (ordinateur, smartphone, liseuse numérique, console de jeux vidéos connectée à Internet, etc.).*

Les cookies et autres traceurs requièrent un **consentement explicite** et informé de la part des utilisateurs.

Votre site doit offrir un moyen clair et accessible pour que les visiteurs puissent **accepter, refuser ou personnaliser leur choix en matière de cookies**.

Certains cookies sont nécessaires et ne nécessitent pas de consentement

Les cookies considérés comme nécessaires sont les suivants :

- les traceurs **conservant le choix exprimé** par les utilisateurs sur le dépôt de traceurs
- les traceurs destinés à **l'authentification auprès d'un service**, y compris ceux visant à assurer la sécurité du mécanisme d'authentification, par exemple en limitant les tentatives d'accès robotisées ou inattendues
- les traceurs destinés à garder en mémoire le contenu **d'un panier d'achat** sur un site marchand ou à facturer, à l'utilisateur, le(s) produit(s) et/ou service(s) acheté(s)
- les traceurs de personnalisation de l'interface utilisateur (par exemple, pour le choix de la langue)
- les traceurs permettant aux sites payants de limiter l'accès gratuit à un échantillon de contenu demandé par les utilisateurs (quantité prédéfinie et/ou sur une période limitée)
- certains traceurs de mesure d'audience dès lors qu'ils respectent certaines conditions. (exemple Matomo configuré d'une certaine façon sur un site non e-commerce)

2

Mon site partage t'il des données avec des tierces parties ?

Si votre site partage des données personnelles avec des tiers (comme des fournisseurs d'analyses web, des partenaires publicitaires, etc.), **vous devez vous assurer que ces échanges respectent le RGPD**. Les utilisateurs doivent être informés de ces partages et, dans certains cas, donner leur consentement.

Transferts de données en dehors de l'UE :

Si des données sont transférées en dehors de l'Union Européenne, vérifiez que **les pays destinataires assurent un niveau de protection adéquat** ou que des garanties appropriées sont en place.

vous pouvez consulter la carte des pays qui disposent ou non d'une adéquation :

https://www.cnil.fr/fr/la-protection-des-donnees-dans-le-monde)

En ce qui concerne les États Unis, le 10 juillet 2023, la Commission européenne a adopté un nouveau cadre de confidentialité des données (Privacy Shield 2.0).
Le nouvel accord répond à certaines préoccupations de la précédente invalidation, limitant la manière dont les agences d'espionnage américaines peuvent recueillir des renseignements.
Cependant il faut s'assurer que l'organisme figure sur une liste mise à disposition sur le site du Département du Commerce des États-Unis

C'est le cas de google analytics

FOCUS GOOGLE ANALYTICS

Il fait bien partie de la liste **des organismes autorisés.**

Ainsi, théoriquement, les sites internet peuvent donc l'utiliser à nouveau mais ils doivent considérer le risque que l'accord ne soit pas suffisant (**et qu'il soit à nouveau invalidé**).

En effet il est déjà critiqué par le CEPD (comité européen de la protection des données, le PE (le Parlement Européen) et NOYB (organisation de protection de la vie privée).

D'autant que, en ce qui concerne Google Analytics, d'autres facteurs ne sont pas conforme :

- Google utilise les données pour améliorer son service
- Les annonceurs de Google Ads connaissent les préférences des utilisateurs et peuvent à leur tour cibler ces utilisateurs avec de la publicité

3

Mon site rend t'il accessible les documents légaux nécéssaires ?

Votre site doit rendre facilement accessibles ses **politiques de confidentialité**, de **cookies**, et ses **mentions légales.**

Politique de confidentialité :

Ce document doit détailler **comment les données sont collectées, utilisées, protégées, et partagée**s. Il doit aussi expliquer les droits des utilisateurs concernant leurs données.

Pages Politique de cookies et mentions légales :

Les pages dédiées aux cookies doivent fournir des informations claires sur les types de cookies utilisés et leur finalité.

Les mentions légales doivent inclure des informations sur le propriétaire du site, les coordonnées, et d'autres exigences légales.

Des questions ?

www.oniti.fr

02 85 52 33 42

Oniti