RGPD de l’Union Européenne
Règles Générales de Protection des Données

RKM - RGPD UE 25 mai 2018 v2.docx 17/04/18

Table des matières

[Concerne qui et où ? 3](#__RefHeading___Toc259_11923948)

[Application 3](#__RefHeading___Toc104_2562509590)

[Concerne quoi ? 3](#__RefHeading___Toc64_2562509590)

[Principes de base à respecter par le détenteur des données 3](#__RefHeading___Toc3089_2486438385)

[Mise en œuvre 3](#__RefHeading___Toc610_3978312432)

[1 Qui nous sommes 3](#__RefHeading___Toc82_2562509590)

[2 Conditions de collecte 3](#__RefHeading___Toc84_2562509590)

[3 Sécurité de transmission 3](#__RefHeading___Toc86_2562509590)

[4 Consentement 3](#__RefHeading___Toc88_2562509590)

[5 Mineurs 3](#__RefHeading___Toc90_2562509590)

[6 Partage de données 4](#__RefHeading___Toc92_2562509590)

[7 Effacement des données personnelles 4](#__RefHeading___Toc106_2562509590)

[RGPD et WordPress : Le guide pour se mettre en conformité 5](#__RefHeading___Toc303_11923948)

[C’est quoi ça, le RGPD ? 7](#__RefHeading___Toc263_11923948)

[1 Qu’est-ce qu’une donnée à caractère personnel ? 7](#__RefHeading___Toc265_11923948)

[2 Concrètement, qu’est-ce que la législation prévoit ? 7](#__RefHeading___Toc267_11923948)

[3 Qui est concerné ? 8](#__RefHeading___Toc269_11923948)

[4 Et les développeurs et agences WordPress, alors ? 8](#__RefHeading___Toc271_11923948)

[Quelles sanctions risque-t-on ? 9](#__RefHeading___Toc273_11923948)

[Que devez-vous changer sur votre site WordPress ? 9](#__RefHeading___Toc275_11923948)

[5 1. Mettre à jour ses conditions d’utilisation et sa politique de confidentialité 9](#__RefHeading___Toc277_11923948)

[1.1 Une politique de confidentialité claire comme de l’eau de source 10](#__RefHeading___Toc279_11923948)

[1.2 Des Conditions Générales d’Utilisation RGPD-friendly 10](#__RefHeading___Toc281_11923948)

[6 2. Revoir tous les formulaires de son site WordPress 11](#__RefHeading___Toc283_11923948)

[7 3. Mettre en conformité les commentaires de WordPress 14](#__RefHeading___Toc285_11923948)

[3.1 N’autoriser la publication de commentaires que lorsque l’utilisateur est connecté à son compte 14](#__RefHeading___Toc287_11923948)

[3.2 Ajouter un message-type de consentement “J’ai lu et accepte la politique de confidentialité de ce site” dans l’espace des commentaires. 14](#__RefHeading___Toc289_11923948)

[3.3 Et les plugins de gestion des commentaires alors ? 14](#__RefHeading___Toc291_11923948)

[8 4. Faire un point sur ses extensions WordPress 15](#__RefHeading___Toc293_11923948)

[9 5. Mettre en place un processus de sécurité des données ultra béton 15](#__RefHeading___Toc295_11923948)

[5.1 Créer un process d’effacement ou de modification des données 15](#__RefHeading___Toc297_11923948)

[5.2 Se préparer à une éventuelle faille de sécurité 16](#__RefHeading___Toc299_11923948)

[10 La suite traite des obligations pour le traitement massif des données collectées, ce qui ne nous concerne pas. 17](#__RefHeading___Toc301_11923948)

## Concerne qui et où ?

Une réglementation unique pour toutes les entreprises exerçant des activités conservant des données personnelles dans toute l’Union Européenne.

Source de l’UE : <http://ec.europa.eu/justice/smedataprotect/index_fr.htm>

## Application

Le 25 mai 2018, date à laquelle toute organisme ou société \* de l’UE doit être en conformité avec cette réglementation.

\* Il faudra trouver la référence désignant précisément qui doit se mettre en conformité.

## Concerne quoi ?

Le droit d’accès à ses données personnelles
Le droit à l’oubli de ses données personnelles
Les droits et conséquences en cas de violation

## Principes de base à respecter par le détenteur des données

Dire à l’utilisateur fournissant des données qui nous sommes et ce que nous conservons
Avoir son consentement pour conserver un enregistrement de ses données et pourquoi nous les conservons
Lui donner un accès à ses données conservées
Lui garantir la possibilité de les supprimer définitivement.

## Mise en œuvre

###  Qui nous sommes

Nous, c’est à dire le Secteur pastoral du Pays Mornantais, concerne ici les paroisses catholiques de St Jean-Pierre Néel et de Saint Vincent en Lyonnais.

###  Conditions de collecte

Nous enregistrons des données lorsque vous remplissez un formulaire en ligne
ou lorsque vous commenter un article du blog.

###  Sécurité de transmission

Vos données son transmises par une liaison sécurisée sous forme cryptée pour rester illisibles si elles étaient interceptées par un tiers malveillant (Protocole sécurisé HTTPS).

###  **Consentement**

Vous acceptez que vos nom, adresse postale, ou de messagerie électronique, ou No de téléphone, soient enregistrés pour que nous puissions vous contacter le cas échéant.

###  **Mineurs**

Si vous n’étiez pas majeur, vous certifiez que vous avez l’accord parental pour nous fournir les informations vous concernant.

###  **Partage de données**

Aucun autre organisme n’a accès à vos données en dehors des activités du Secteur Pastoral du Pays Mornantais.

###  Effacement des données personnelles

Vos données sont effacées définitivement sur votre simple demande ou lorsque nous estimons qu’il n’est plus nécessaire de les conserver (demande d’infos ponctuelles par exemple)

ébauche RKM

## RGPD et WordPress : Le guide pour se mettre en conformité

Source : La Marmite (18 mai 2018) [https://wpmarmite.com/rgpd-wordpress/?utm\_source=ActiveCampaign&utm\_medium=email&utm\_content=Le+guide+ultime+%28et+concret%29+sur+le+RGPD+%28et+le+d%C3%A9nouement+du+castorgate%29&utm\_campaign=RGPD](https://wpmarmite.com/rgpd-wordpress/?utm_source=ActiveCampaign&utm_medium=email&utm_content=Le+guide+ultime+(et+concret)+sur+le+RGPD+(et+le+dénouement+du+castorgate)&utm_campaign=RGPD)

J’ai reçu ce document de La Marmite, il complète ce que j’avais retenu du site de l’Union Européenne

Publié par [Eléonor (Équipe WPMarmite)](https://twitter.com/_eleonor_b) le 18 avril 2018 / [Pas de commentaire](https://wpmarmite.com/rgpd-wordpress/%22%20%5Cl%20%22comments)



Décidément, en ce début d’année 2018, l’univers du web s’agite de toutes parts !

Il y a quelques semaines, on vous parlait de [l’arrivée de WordPress 5.0 dans les mois à venir](https://wpmarmite.com/gutenberg-wordpress/), et de la véritable révolution qui se préparait.

Aujourd’hui, il nous semble essentiel de vous parler d’un autre sujet, qui bruisse tout autant sur toutes les lèvres : le RGPD.

Si vous êtes marketeur ou chef d’entreprise, et que vous traînez régulièrement sur LinkedIn, vous avez du entendre parler de cette nouvelle législation, qui entrera en application le 25 mai.

Le RGPD, acronyme pour Règlement Général pour la Protection des Données, ne cesse d’y faire parler de lui ! Vous l’avez peut-être aussi rencontré dans son acception anglaise, GDPR.

Mais si vous possédez un site web et que vous n’avez pas encore entendu parler du RGPD, alors il est temps de vous renseigner un peu pour vous préparer car ça va secouer !

Ça tombe bien : la Marmite a récemment rencontré des avocats spécialistes du sujet pour y voir un peu plus clair.

Du coup, nous avons pris le parti de vous détailler, pas à pas, les différents points-clés à examiner pour mettre votre site WordPress ou votre boutique WooCommerce en conformité avec la nouvelle législation.

Pas de jargon juridique, pas de références à d’obscures parties du Code Civil : que du concret pour les créateurs de sites WordPress et WooCommerce !

On vous le concède, cela n’a pas été facile. Si vous avez suivi [les stories d’Alex sur Instagram](https://www.instagram.com/wpmarmite/), vous avez vu qu’il a fallu remanier l’article plus d’une fois !

Ceci étant dit, nous estimons vous proposer une ressource qui se veut la plus concrète possible (contrairement à ce que l’on peut voir ailleurs) afin de vous aider à mettre votre site dans les clous.

Note du rédacteur : Pour rédiger cet article, nous avons fait appel à [l’expertise du cabinet d’avocats Langlais](http://www.langlais-avocats.com/) : merci à eux !

Cependant, il ne s’agit là que d’une source d’informations générales, qui ne peuvent être interprétées comme un véritable conseil juridique. Si vous maniez au quotidien un nombre important de données, nous ne pouvons que vous recommander de faire appel à des professionnels, comme ceux du cabinet Langlais, qui pourront vous accompagner à vous mettre en conformité.

Sur ce, je vous propose de découvrir le sommaire :

* [C’est quoi ça, le RGPD ?](https://wpmarmite.com/rgpd-wordpress/?utm_source=ActiveCampaign&utm_medium=email&utm_content=Le+guide+ultime+(et+concret)+sur+le+RGPD+(et+le+dénouement+du+castorgate)&utm_campaign=RGPD" \l "definition)
	1. [Qu’est-ce qu’une donnée à caractère personnel ?](https://wpmarmite.com/rgpd-wordpress/?utm_source=ActiveCampaign&utm_medium=email&utm_content=Le+guide+ultime+(et+concret)+sur+le+RGPD+(et+le+dénouement+du+castorgate)&utm_campaign=RGPD" \l "donnees)
	2. [Concrètement, qu’est-ce que la législation prévoit ?](https://wpmarmite.com/rgpd-wordpress/?utm_source=ActiveCampaign&utm_medium=email&utm_content=Le+guide+ultime+(et+concret)+sur+le+RGPD+(et+le+dénouement+du+castorgate)&utm_campaign=RGPD" \l "legislation)
	3. [Qui est concerné ?](https://wpmarmite.com/rgpd-wordpress/?utm_source=ActiveCampaign&utm_medium=email&utm_content=Le+guide+ultime+(et+concret)+sur+le+RGPD+(et+le+dénouement+du+castorgate)&utm_campaign=RGPD" \l "qui)
	4. [Et les développeurs et agences WordPress, alors ?](https://wpmarmite.com/rgpd-wordpress/?utm_source=ActiveCampaign&utm_medium=email&utm_content=Le+guide+ultime+(et+concret)+sur+le+RGPD+(et+le+dénouement+du+castorgate)&utm_campaign=RGPD" \l "developpeurs)
	5. [Quelles sanctions risque-t-on ?](https://wpmarmite.com/rgpd-wordpress/?utm_source=ActiveCampaign&utm_medium=email&utm_content=Le+guide+ultime+(et+concret)+sur+le+RGPD+(et+le+dénouement+du+castorgate)&utm_campaign=RGPD" \l "sanctions)
* [Que devez-vous changer sur votre site WordPress ?](https://wpmarmite.com/rgpd-wordpress/?utm_source=ActiveCampaign&utm_medium=email&utm_content=Le+guide+ultime+(et+concret)+sur+le+RGPD+(et+le+dénouement+du+castorgate)&utm_campaign=RGPD" \l "wordpress)
	1. [Mettre à jour ses conditions d’utilisation et sa politique de confidentialité](https://wpmarmite.com/rgpd-wordpress/?utm_source=ActiveCampaign&utm_medium=email&utm_content=Le+guide+ultime+(et+concret)+sur+le+RGPD+(et+le+dénouement+du+castorgate)&utm_campaign=RGPD" \l "cgu)
	2. [Revoir les formulaires de son site WordPress](https://wpmarmite.com/rgpd-wordpress/?utm_source=ActiveCampaign&utm_medium=email&utm_content=Le+guide+ultime+(et+concret)+sur+le+RGPD+(et+le+dénouement+du+castorgate)&utm_campaign=RGPD" \l "formulaires)
	3. [Mettre en conformité les commentaires WordPress](https://wpmarmite.com/rgpd-wordpress/?utm_source=ActiveCampaign&utm_medium=email&utm_content=Le+guide+ultime+(et+concret)+sur+le+RGPD+(et+le+dénouement+du+castorgate)&utm_campaign=RGPD" \l "commentaires)
	4. [Faire un point sur ses plugins WordPress](https://wpmarmite.com/rgpd-wordpress/?utm_source=ActiveCampaign&utm_medium=email&utm_content=Le+guide+ultime+(et+concret)+sur+le+RGPD+(et+le+dénouement+du+castorgate)&utm_campaign=RGPD" \l "plugins)
	5. [Mettre en place un process de sécurité des données ultra béton](https://wpmarmite.com/rgpd-wordpress/?utm_source=ActiveCampaign&utm_medium=email&utm_content=Le+guide+ultime+(et+concret)+sur+le+RGPD+(et+le+dénouement+du+castorgate)&utm_campaign=RGPD" \l "securite)
	6. [Instaurer un registre interne de traitement des données](https://wpmarmite.com/rgpd-wordpress/?utm_source=ActiveCampaign&utm_medium=email&utm_content=Le+guide+ultime+(et+concret)+sur+le+RGPD+(et+le+dénouement+du+castorgate)&utm_campaign=RGPD" \l "registre)
* [Comment rendre une boutique WooCommerce conforme au RGPD ?](https://wpmarmite.com/rgpd-wordpress/?utm_source=ActiveCampaign&utm_medium=email&utm_content=Le+guide+ultime+(et+concret)+sur+le+RGPD+(et+le+dénouement+du+castorgate)&utm_campaign=RGPD" \l "woocommerce)
	1. [Des conditions générales de vente adaptées](https://wpmarmite.com/rgpd-wordpress/?utm_source=ActiveCampaign&utm_medium=email&utm_content=Le+guide+ultime+(et+concret)+sur+le+RGPD+(et+le+dénouement+du+castorgate)&utm_campaign=RGPD" \l "cgv)
	2. [Une page de commande où apparaît votre Politique de Confidentialité](https://wpmarmite.com/rgpd-wordpress/?utm_source=ActiveCampaign&utm_medium=email&utm_content=Le+guide+ultime+(et+concret)+sur+le+RGPD+(et+le+dénouement+du+castorgate)&utm_campaign=RGPD" \l "commande)
	3. [Des formulaires WooCommerce d’inscription nickel chrome](https://wpmarmite.com/rgpd-wordpress/?utm_source=ActiveCampaign&utm_medium=email&utm_content=Le+guide+ultime+(et+concret)+sur+le+RGPD+(et+le+dénouement+du+castorgate)&utm_campaign=RGPD" \l "formulaires-woocommerce)
	4. [Des avis clients en conformité avec la législation](https://wpmarmite.com/rgpd-wordpress/?utm_source=ActiveCampaign&utm_medium=email&utm_content=Le+guide+ultime+(et+concret)+sur+le+RGPD+(et+le+dénouement+du+castorgate)&utm_campaign=RGPD" \l "avis)
	5. [Le souci avec votre plugin d’abandon de panier](https://wpmarmite.com/rgpd-wordpress/?utm_source=ActiveCampaign&utm_medium=email&utm_content=Le+guide+ultime+(et+concret)+sur+le+RGPD+(et+le+dénouement+du+castorgate)&utm_campaign=RGPD" \l "abandon-panier)
* [Quelles pratiques marketing sont interdites par le RGPD ?](https://wpmarmite.com/rgpd-wordpress/?utm_source=ActiveCampaign&utm_medium=email&utm_content=Le+guide+ultime+(et+concret)+sur+le+RGPD+(et+le+dénouement+du+castorgate)&utm_campaign=RGPD" \l "marketing)
* [Bonus : La piste de la Marmite pour être en conformité…](https://wpmarmite.com/rgpd-wordpress/?utm_source=ActiveCampaign&utm_medium=email&utm_content=Le+guide+ultime+(et+concret)+sur+le+RGPD+(et+le+dénouement+du+castorgate)&utm_campaign=RGPD" \l "bonus)
* [Que doit-on penser du RGPD ?](https://wpmarmite.com/rgpd-wordpress/?utm_source=ActiveCampaign&utm_medium=email&utm_content=Le+guide+ultime+(et+concret)+sur+le+RGPD+(et+le+dénouement+du+castorgate)&utm_campaign=RGPD" \l "conclusion)
	1. [Les points de vigilance](https://wpmarmite.com/rgpd-wordpress/?utm_source=ActiveCampaign&utm_medium=email&utm_content=Le+guide+ultime+(et+concret)+sur+le+RGPD+(et+le+dénouement+du+castorgate)&utm_campaign=RGPD" \l "négatif)
	2. [Les points positifs](https://wpmarmite.com/rgpd-wordpress/?utm_source=ActiveCampaign&utm_medium=email&utm_content=Le+guide+ultime+(et+concret)+sur+le+RGPD+(et+le+dénouement+du+castorgate)&utm_campaign=RGPD" \l "positif)

## C’est quoi ça, le RGPD ?



Le Règlement Général pour la Protection des Données est une réglementation européenne qui prend application très prochainement, le 25 mai pour être exact. Votée au Parlement Européen en 2016, sa mise en application est mondiale, et [l’organisme en charge de son respect en France est la CNIL](https://www.cnil.fr/fr/se-preparer-au-reglement-europeen), la Commission Nationale de l’Informatique et des Libertés.

Le but de cette réglementation, qui va venir secouer les pratiques des professionnels et particuliers sur le web : assurer à tout individu le contrôle et la protection des données à caractère personnel qu’il dissémine lors de ses navigations sur la toile.

### Qu’est-ce qu’une donnée à caractère personnel ?

Petit point définition : Est considérée comme une donnée à caractère personnel toute donnée qui permet d’identifier directement ou indirectement un individu :

* On peut identifier directement un internaute grâce à son nom, son prénom, mais également son adresse email ou son numéro de téléphone, et tout type de donnée démographique (fonction professionnelle, sexe, âge…) ou géographique (localisation, lieu de travail…).
* Comptent aussi dans ces données à caractère personnel les informations purement numériques d’un internaute (adresse IP), ou ses data comportementales (actions menées sur un site web, comme les visites ou les clics). Même les données partagées de sa propre initiative, comme la mise en ligne d’une photo ou un like, comptent également dans cette définition.

Ça promet, hein ?

### Concrètement, qu’est-ce que la législation prévoit ?

Pour être très concret, le RGPD comporte trois volets importants, qu’il s’agit de prendre en compte :

* L’amélioration du consentement de l’utilisateur lorsqu’un site web récolte ses données à caractère personnel. Que ce soit via des formulaires, ou bien vis-à-vis des cookies, le visiteur doit être informé qu’il partage ses données, et savoir explicitement à quelles fins.
* La traçabilité et la haute sécurité des données des utilisateurs. La législation durcit les lois existantes en matière de failles de sécurité de la data, et rend l’entreprise qui les récolte responsable de leur bon stockage et de leur protection.
* Le droit de l’internaute à rectifier, modifier, supprimer ou recueillir ses données à caractère personnel, et ce à tout moment.

Autant d’éléments qui vont influencer la manière de créer et de gérer un site web.

### Qui est concerné ?

Le RGPD concerne toute personne, physique ou morale, qui serait amenée à toucher de près ou de loin à des données à caractère personnel de citoyens de l’Union Européenne dans le cadre de son activité professionnelle.

Si vous collectez, utilisez ou stockez ce type de données, surprise : vous êtes pile dans la cible de cette législation (et potentiellement dans le viseur de la CNIL) ! Et ce, quels que soient le secteur d’activité ou la taille de votre structure.

À noter que le RGPD s’applique également aux données internes aux entreprises : celles que vous récoltez sur vos employés, dans des fichiers du personnel, par exemple.

Autre point très important : même si votre entreprise ou vous-même êtes basés, ou que vous stockez vos données, en-dehors de l’Union Européenne, le RGPD s’applique à votre activité.

La législation se place en effet du point de vue de l’internaute : si vous traitez des données d’un individu résidant dans l’un des 28 membres de l’UE, vous êtes concerné.

### Et les développeurs et agences WordPress, alors ?

Bon nombre de lecteurs de la Marmite, et notamment les développeurs ou agences WordPress, se diront : “ok, mais moi, je ne fais que traiter les données de seconde main que mes clients récoltent”.

Minute papillon ! Vous êtes également concernés, en tant que sous-traitants. Grosso modo, si le traitement que vous faites des données de vos clients ne rentre pas en conformité avec le GDPR, vous risquez également de vous faire taper sur les doigts.

Et surtout, si vous n’êtes pas conformes au RGPD, vous risquez de voir certains clients refuser de faire affaire avec vous désormais !

Il s’agit donc dès maintenant pour vous de revoir la manière dont vous abordez cette utilisation des données dans vos contrats clients, actuels et futurs. En recherchant des informations à ce sujet, je suis tombée sur [une infographie bien ficelée](http://blog.diduenjoy.com/rgpd-conseils-experts), dont la seconde partie traite des questions à aborder avec vos clients en tant que prestataire.

Voici quelques éléments à ajouter à vos contrats, dans une partie spécifique à l’utilisation que vous faites de vos données, pour être dans les clous :

* Le nom et les coordonnées de [votre Délégué à la Protection des Données (DPO)](https://www.cnil.fr/fr/devenir-delegue-la-protection-des-donnees) (pas besoin d’en nommer un si vous ne brassez pas une masse de data quotidiennement) ;
* La méthode que vous utilisez pour récolter, stocker et utiliser vos données ;
* Vos méthodes de sécurisation des données ;
* Vos éventuelles relations à d’autres sous-traitants, qui utiliseraient ces mêmes données ;
* Votre méthode de notification de faille de sécurité, et éventuellement votre processus de rectification ou suppression des données à la demande des utilisateurs ([direction la partie 5 de ce tutoriel](https://wpmarmite.com/rgpd-wordpress/?utm_source=ActiveCampaign&utm_medium=email&utm_content=Le+guide+ultime+(et+concret)+sur+le+RGPD+(et+le+dénouement+du+castorgate)&utm_campaign=RGPD" \l "securite) : toute le monde est concerné !).

### Quelles sanctions risque-t-on ?

Avant même le RGPD, le droit français prévoyait déjà des sanctions pénales en cas d’infractions portant sur des données personnelles. Certes, dans les faits, celles-ci étaient rarement appliquées, ou par des amendes relativement faibles.

On se rappelle notamment de OUICAR qui n’a écopé que d’un avertissement alors que les données personnelles des utilisateurs de son site sont restées librement accessibles pendant près de trois ans…

Mais le RGPD vient renforcer le système de sanctions déjà mis en place. Et les amendes administratives détaillées dans la législation sont beaucoup plus dissuasives ! Il est prévu qu’elles pourront atteindre 2 % à 4 % du chiffre d’affaires de la personne ou entreprise concernée, et jusqu’à 20 millions d’euros pour les infractions les plus graves.

Il y a 99% de chances pour que vous ayez cette tête en lisant cet article.

En tous cas, chez la Marmite, on vous avoue qu’on est un peu dubitatifs quant à l’application concrète du RGPD. N’empêche qu’on ne se risquerait pas trop à aller chercher la CNIL pour lui faire des pieds de nez…

C’est pourquoi nous allons maintenant vous guider pas à pas dans la mise en conformité de votre site face à ces nouvelles obligations.

## Que devez-vous changer sur votre site WordPress ?



Allez, c’est parti : penchons-nous sur ce que vous allez devoir revoir sur votre site WordPress.

### 1. Mettre à jour ses conditions d’utilisation et sa politique de confidentialité

Premier point essentiel du RGPD : la nécessité d’apposer, à même son site web, des mentions d’information claires et transparentes pour les utilisateurs.

Même si cela devait déjà être le cas avant l’arrivée du RGPD, il va quand même vous falloir plancher sérieusement sur deux éléments-clés : la politique de confidentialité de votre site, ainsi que ses conditions générales d’utilisation et de vente (si vous avez une boutique).

#### 1.1 Une politique de confidentialité claire comme de l’eau de source

Voilà un élément à modifier en vue du RGPD, qui va vous demander de bien analyser comment vous traitez vos données utilisateurs.

Votre page de politique de confidentialité, généralement située dans votre pied de page, doit désormais expliquer concrètement ce que vous faites avec ces données.

Faites-y donc apparaître :

* Vos coordonnées, ainsi que l’éditeur du site, son hébergeur, et la personne morale ou physique qui se charge de sa maintenance.
* Quel type de données vous récoltez lors de l’inscription ou de la commande sur votre site web : noms, prénoms, email, téléphone, adresse postale, adresse IP…
* Pourquoi vous collectez ces données : communication par newsletters, facturation, suivi du comportement de l’utilisateur sur le site…
* Combien de temps vous stockez ces données : vous pouvez garder les données marketing 3 ans maximum, et les données liées à la facturation des commandes 6 ans maximum.
* Les mesures de sécurité que vous avez mises en place pour assurer la protection de ces données, ainsi que la manière dont ils peuvent exercer leur droit de modification ou de suppression de ces données. C’est ce qui nous intéressera dans l’étape 5 de cet article.

Non seulement ces éléments doivent apparaître dans une page intégrée à votre pied de page, mais aussi à chaque moment où vos utilisateurs partageront leurs données (typiquement, dans les formulaires de contact ou de téléchargement).

Pour ce faire, rien de plus simple : il vous suffit de rajouter une case à cocher supplémentaire à votre formulaire.

Cette case, très commune sur la plupart des sites, demande à l’utilisateur de confirmer “J’ai lu et accepte la politique de confidentialité de ce site” (en incluant un lien URL vers votre page dédiée).

Note du rédacteur : À chaque fois que vous ajouterez une case à cocher quelque part, celle-ci ne devra pas être pré-cochée !

L’objectif est que l’utilisateur donne à voir un consentement clair, et l’acte de cocher la case compte comme tel.

#### 1.2 Des Conditions Générales d’Utilisation RGPD-friendly

La page de Conditions Générales d’Utilisation de votre site WordPress va devoir également muter face au RGPD. Comme vous le savez déjà sans doute, il s’agit de la page qui indique à vos visiteurs les conditions légales qui vous lient à eux.

Il est recommandé d’y ajouter dès maintenant votre politique de confidentialité toute neuve, avec toutes les directives RGPD que vous y avez incluses.

Si tout cela vous semble un peu capillotracté, souvenez-vous d’une chose : avec le bruit que fait le RGPD dans les médias, de plus en plus de visiteurs connaissent aujourd’hui leurs droits.

Mettre en place ces éléments sur votre site WordPress, c’est avant tout vous éviter des soucis avec eux (signalements à la CNIL et autres menaces…), et installer une aura de confiance.

### 2. Revoir tous les formulaires de son site WordPress

Les éléments qui vont sans doute être le plus impactés par le RGPD sur le web sont les formulaires. Il s’agit en effet d’un point de contact-clé entre vous et vos visiteurs, où ils partagent avec vous leurs données à caractère personnel.

Et sur un site, il y en a, des formulaires ! Voyons donc voir comment les optimiser pour être conforme à la législation.

Nombreux sont les sites qui mettent en place des formulaires, notamment pour proposer l’inscription à une newsletter ou le téléchargement de documents. Or, à ce point de contact, vos utilisateurs vous partagent des données personnelles : email, prénom, nom a minima.

Les créateurs de sites WordPress gèrent généralement ces formulaires, dits “d’opt-in”, via des plugins comme [OptinMonster](https://optinmonster.com/) couplé à un [MailChimp](https://mailchimp.com/) ou encore [MailPoet](https://wpmarmite.com/mailpoet-wordpress/) (il en existe beaucoup d’autres).

Nous voici ici dans le cas de figure où la mise en conformité de votre site web dépend donc d’une tierce personne, dont nous parlons dans la partie “Faire le point sur ses plugins WordPress”.

Que vous déléguiez cette tâche à un plugin, ou que vous ayez construit vos formulaires vous-même, il vous faut en tous cas vérifier que vous pouvez :

* Rajouter une case à cocher indiquant que l’utilisateur consent à partager ses données (“J’autorise l’entreprise X à enregistrer mes données”)
* Spécifier la raison de la récolte des données (“Entrez votre adresse email pour recevoir notre newsletter”)
* Proposer aux utilisateurs de se désinscrire ou d’accéder à leurs données aisément et à tout moment

Voici un bien / pas bien de la future apparence de vos formulaires (si vous avez une newsletter qui peut proposer des offres commerciales) :



Biennnnnn



Pas biennnnnn

Merci à [Codeur.com](https://www.codeur.com/blog/rgpd-formulaire-email-conforme/) pour ces illustrations

Notez également que vous ne pouvez plus demander à un client de vous laisser des données qui n’ont aucun rapport avec ce pour quoi ils s’inscrivent.

Si vous leur demandez par exemple de s’inscrire à une newsletter, inutile de leur demander leur sexe ou encore leur âge.

Fini le Big Data, passage imminent au Smart Data !

Pour les formulaires de contact, la problématique semble assez similaire. Que vous ayez choisi d’utiliser [Contact Form 7](https://wpmarmite.com/contact-form-7/), [Gravity Forms](https://wpmarmite.com/gravity-forms/), tout autre plugin de formulaires de contact, ou bien que vous ayez créé vos formulaires à la main, vous devez y rajouter une case de consentement à cocher.

Placez-la en-dessous ou à côté du bouton “Envoyer”, pour éviter toute méprise, avec une ligne de texte type “En cochant cette case, j’accepte la Politique de confidentialité de ce site”.

Note du rédacteur : La plupart des plugins de formulaires très populaires planchent depuis un moment sur leur conformité au RGPD. N’hésitez pas à consulter leur documentation pour en apprendre plus sur leurs efforts, et choisir celui qui conviendra le mieux à la législation.

Les formulaires, c’est plié : récolte du consentement assurée. Allez hop, on enchaîne.

### 3. Mettre en conformité les commentaires de WordPress

Les commentaires sont un autre point de contact entre vous et vos visiteurs, où ils vous laissent potentiellement des données. Sur ce point, deux possibilités s’offrent à vous pour être sûr de récolter le consentement de ceux qui souhaitent s’y exprimer.

#### 3.1 N’autoriser la publication de commentaires que lorsque l’utilisateur est connecté à son compte

Dans ce cas, direction les Réglages de WordPress, onglet “Discussions”, où vous cochez alors la case “Un utilisateur doit être enregistré et connecté pour publier des commentaires”.



Si la personne est enregistrée, elle a forcément accepté votre politique de confidentialité lors de la création de son compte. Donc inutile de lui redemander.

#### 3.2 Ajouter un message-type de consentement “J’ai lu et accepte la politique de confidentialité de ce site” dans l’espace des commentaires.

Pour ce deuxième point, youpi ! On vous a trouvé un plugin tout prêt : [WP Comment Policy Checkbox](https://fr.wordpress.org/plugins/wp-comment-policy-checkbox/), qui rajoutera une case à cocher près du bouton “Envoyer”, et diffusera un message d’erreur si ce n’est pas fait.

Le plugin n’est pas traduit en Français, mais est assez simple à prendre en main (si vous utilisez [Loco Translate](https://fr.wordpress.org/plugins/loco-translate/), vous pourrez le traduire en un rien de temps).

#### 3.3 Et les plugins de gestion des commentaires alors ?

Vous voilà de nouveau devant la même problématique qu’avant : votre plugin est-il conforme au RGPD ?

Certains des plus performants, comme Jetpack ou Disqus, [dont nous vous parlions dans un article il y a déjà longtemps](https://wpmarmite.com/systeme-commentaire-wordpress/%22%20%5Cl%20%2222-jetpack), planchent activement sur le sujet, et s’assurent que tout soit en règle pour le 25 mai. [La version 6.0 de Jetpack](https://wptavern.com/jetpack-6-0-takes-steps-towards-gdpr-compliance) est d’ailleurs dès à présent disponible, prête à affronter la législation !

Mais justement, comment savoir si un plugin WordPress est conforme aux nouvelles obligations du RGPD ?

### 4. Faire un point sur ses extensions WordPress

Pour savoir si vos extensions restent dans les clous du RGPD, il va vous falloir mener votre petite enquête personnelle.

Oui, ça va prendre un peu de temps…

Commencez par lister toutes vos extensions qui pourraient avoir un rapport avec :

* La récolte du consentement et des données de vos utilisateurs : plugins de formulaires, de commentaires, de retargeting…
* L’utilisation de vos données utilisateurs : plugins de personnalisation de contenus, de suivi du comportement des visiteurs, de newsletters, de marketing automatisé, …

Ensuite, cherchez sur les sites officiels de ces plugins ou dans leur documentation ce que font leurs développeurs pour s’aligner avec le RGPD.

Pour la plupart, étant donné que leur site sera en anglais, recherchez GDPR directement sur leur site ou faites une recherche Google de ce type : site:woocommerce.com GDPR

Bon nombre d’entre elles, parmi les plus utilisées, ont déjà lancé des mises à jour pour être réglo. Il vous faudra donc mettre celles-ci à jour dès que possible.

Dans le cas où une extension n’est pas encore apte à respecter le RGPD, il est conseillé de trouver rapidement une alternative pour la remplacer. Pas aisé, on vous le concède… mais absolument nécessaire.

D’ailleurs, faites-nous part des résultats de vos recherches dans la section commentaires afin d’en faire profiter les autres lecteurs (cela leur évitera de faire les mêmes recherches que vous).

Note du rédacteur : Toutes les API que vous avez autorisées (Facebook, Twitter, ou Mailchimp, pour ne prendre que ces exemples célèbres) sont également concernées. Mais évitez de trop vous casser la tête : tant que vous savez quelles API votre site utilise, quelles données elles traitent, et que vous consignez tout ça dans votre registre (voir la partie dédiée à ce point) : pas besoin de les éliminer de votre site WordPress.

### 5. Mettre en place un processus de sécurité des données ultra béton

Il est plus que jamais de la responsabilité de celui qui détient des données de les bichonner, notamment en les protégeant contre toute faille de sécurité, mais aussi en permettant aux individus d’avoir un droit de regard dessus.

#### 5.1 Créer un process d’effacement ou de modification des données

Avec le RGPD, chaque type de données a désormais une durée légale de conservation spécifique. Vous n’avez plus le droit de garder indéfiniment une donnée client ou utilisateur sans l’utiliser, juste “au cas où”

Google Analytics [vient d’ailleurs d’intégrer cela à sa solution](https://support.google.com/analytics/answer/7667196?hl=fr), on peut dire adieu à notre historique des visites.

Les données marketing, par exemple, peuvent être conservées 3 ans maximum après le dernier contact avec l’individu.

Mais le RGPD prévoit aussi que vous devez informer tout utilisateur, avant qu’il ne vous partage ses données, qu’il est en droit de retirer à tout moment son consentement. Et par-dessus le marché, la législation spécifie que cela doit se faire aisément pour l’utilisateur !

Il va donc vous falloir mettre en place une procédure simple qui permette à vos utilisateurs de :

* Retirer leur consentement
* Accéder à leurs données
* Les modifier
* Demander à les effacer
* Demander à les transférer vers un tiers (on appelle cela le “droit à la portabilité”)

Il est ainsi conseillé de créer une page spécifique dédiée à cette procédure sur votre site, contenant un formulaire de demande précis.

Incluez cette page non seulement à votre pied de page, mais à tous les points de contact où vos utilisateurs sont susceptibles de vouloir retirer leur consentement.

Pensez donc à faire de même sur vos newsletters, mais aussi dans vos bandeaux de signalement de cookies, ou encore à vos bannières publicitaires si vous en avez…

Mon conseil : refaites vous-même le parcours utilisateur de votre visiteur, pour détecter tous les moments où il pourrait avoir envie d’exercer son droit de retrait ou d’effacement. Un véritable travail d’orfèvre, qui vous permettra de mettre en place un processus vraiment clair.

Pensez aussi à créer une boîte email spécifique, type protectiondedonnees@votresite.com, qui vous permettra de recevoir toutes les demandes d’exercice du droit des personnes.

Puis, à réception de chaque demande :

* De retrait de consentement, il vous faudra supprimer ou modifier les données personnelles de l’internaute au plus vite et sur l’ensemble de vos lieux de stockage (y compris dans les fichiers de sauvegarde de votre site WordPress).
* De portabilité des données, vous devrez exporter toutes les données que vous possédez dans un format lisible par une machine, afin que la personne puisse transmettre ses données à une autre entité sans avoir à les ressaisir. Le format n’étant pas défini, ni la structure, tout est à ce jour possible… (cela dit il y a de grandes chances pour le format CSV soit celui qui soit privilégié).

Bye bye data !

#### 5.2 Se préparer à une éventuelle faille de sécurité

Il vous faudra également vous assurer que vous garantissez efficacement la sécurité des données à caractère personnel de vos internautes.

Voici quelques éléments qu’il vous faudra donc prendre en compte :

* Il est nécessaire de mettre en place des mesures et techniques adéquates pour garantir un haut niveau de sécurité des données de vos utilisateurs. Chiffrement de la data, *pseudonymisation*, cryptage… Vos process internes doivent être clairs à ce sujet.
* Il vous faudra informer la CNIL dans les 72 heures en cas de faille de sécurité. Dans certains cas, il vous faudra même informer l’utilisateur concerné, notamment si la faille est susceptible d’engendrer un risque élevé pour ses droits et libertés.

### La suite traite des obligations pour le traitement massif des données collectées, ce qui ne nous concerne pas.