How To Make A WooCommerce Website GDPR Compliant? (12 Steps)

This is a direct copy of this article https://businessbloomer.com/how-to-make-a-woocommerce-website-gdpr-compliant-12-steps/ written by Rodolfo Melogli author of eCommerce and Beyond

Ok, we all know that the EU General Data Protection Regulation (GDPR) will come into force on the 25th May 2018.

So the main question is: what **changes do we need to make on our WooCommerce website** to become compliant? And another important query might be: how does **GDPR affect non-European WooCommerce websites**?

In this article, I will tell you EXACTLY what you need to do. There are a million articles and plugins on WordPress GDPR compliance, but there is no "ultimate" blog that tells you what you should be doing.

If you don't know what GDPR is or need a good refresher, read Wikipedia's GDPR page or the "Introduction to GDPR Compliance for WooCommerce Stores" on the official WooCommerce blog.

Many blogs I've read and WordCamp events I've attended didn't really give me the answers I needed. I don't particularly care about GDPR itself, I just want to know what I need to do on my WooCommerce website.

So, let's see what changes you're required to make.

Please note: I'm not a lawyer and cannot guarantee this article is going to make you 100% compliant – make sure to assess your GDPR compliance with a qualified consultant.

WooCommerce GDPR Compliance: Summary

In order to be GDPR compliant, you will need to audit your WooCommerce website and marketing procedures.

Please note: EU GDPR will affect businesses **both inside and outside of the EU**. Any non-EU company dealing with EU customers will have to comply with the GDPR.

To achieve full compliance by the end of May 2018, WooCommerce businesses will need to:

1. Tell the user who you are, what **data** you collect, why you collect the data, for how long you retain it and which third parties receive it (if any)
2. Get a clear **consent** before collecting any data
3. Let users **access** their data
4. Let users **download** their data
5. Let users **delete** their data
6. Let users know if a data **breach** has occurred

If you don't strictly adhere to these rules, you will eventually get fined up to €20 million or 4% of your worldwide annual turnover, whichever is greater…

Now, this is good to know, but actually the most important question is: **what changes am I required to do on my WordPress/WooCommerce website**?

Well, with my goal being translating GDPR in plain English and in "WordPressian" (a new language I just created), the 6 rules outlined above will have implications on:

- WooCommerce Terms & Conditions (Checkout page)
- WooCommerce Privacy Policy (Checkout page)
- WooCommerce User registration (My Account page)
- WooCommerce Cart Abandonment (Checkout page)
- WooCommerce product reviews (Single Product page)
- WordPress comments (Blog pages)
- WordPress & WooCommerce opt-in forms (Newsletter, Lead magnets, etc.)
- WordPress contact forms (Contact Us page, widgets, etc.)
- WooCommerce analytics (Google Analytics, Metorik, etc.)
- WordPress and WooCommerce Plugins & APIs (Payments, Email marketing, etc.)
- Breach notifications

That's quite a lot of work… but given I have to do it for Business Bloomer, why not sharing it with you too? So, here are the **12 GDPR compliance steps I'm going to take and the same ones you, as a WooCommerce store owner, should work on**. *Once again, please double check this with a lawyer or a GDPR consultant as I'm neither of the two.*

A Quick Note re: Upcoming WordPress & WooCommerce GDPR Changes

The WooCommerce team is working hard to implement data removal and data export for a given customer (see status on GitHub), so we won't need to worry about that part. They are possibly going to add these new functionalities to the "My Account" tabs.

Also, the WooCommerce development team posted an article on April 10th called "How we're tackling GDPR in WooCommerce core" which I recommend you to read. They confirm they're working on releasing some **improvements to the Checkout Page** (mostly in regard to T&C and Privacy Policy).

Finally, WordPress itself is also working on new functionalities (here are the completed GDPR tasks) such as:

1. **Privacy Policy generator** 🙂
2. **Comment Form** opt-ins
3. Helper functions to **anonymize data**

GDPR Compliance Step 1: WooCommerce Terms & Conditions

Based on Quora's article, "What is the difference between Privacy Policy and Terms and Conditions?", the Privacy Policy is to inform the user about the data you gather, while the Terms and Conditions (also called T&C, Terms of Service or ToS) include the legal terms and rules that bind the customer to your business.

Therefore, while the biggest changes will need to be done on your Privacy Policy (as well as showing this everywhere, see following section), you should also amend your T&C page in regard to the new GDPR terminology and the gathering of customer data from the WooCommerce checkout.

In my opinion, it's simply sufficient to **add a paragraph to your ToS that links to the revised Privacy Policy** and therefore the whole personal data usage document.

If you have no T&C page at all, you can use some of the online generators (google "terms and conditions generator" or "terms and conditions template"), use a premium service like iUbenda, or alternatively take a look at T&C pages on popular ecommerce websites to get some inspiration 🙂

Needless to say – you definitely need a T&C page now and also a checkout checkbox that users must click (it cannot be "checked" by default).

Thankfully you can do that from the WooCommerce settings (*WordPress Dashboard > WooCommerce > Settings > Checkout > Terms and Conditions > Select a Page*):

WordPress Dashboard > WooCommerce > Settings > Checkout > Terms and Conditions > Select a Page
Once this is done, the WooCommerce checkout will show a checkbox on the checkout page with default text and a link to the T&C page you selected in the previous step:

WooCommerce Checkout page: "I've read and accept the terms & conditions" checkbox
To-do list:

- Create a T&C page if you have none (you can use a T&C generator or take a look at popular ecommerce T&C pages – remember to refine the document for your specific legal agreements and have it revised by a lawyer)
- Add a new GDPR paragraph to your T&C that links to your Privacy Policy page
- Use the WooCommerce Checkout Settings to add a checkbox to the Checkout page

GDPR Compliance Step 2: WooCommerce Privacy Policy

The Privacy Policy page is the one that requires a lot of editing and copywriting. On top of this, we will need to show the Privacy Policy opt-in message on the checkout page and other places, such as contact forms and opt-in forms (see following sections).

In regard to the **Privacy Policy page content**, you must inform the user about the data you collect, store and use.

Once again, the suggestion here is to take a look at reliable ecommerce websites Privacy Policy pages and see how they're approaching the new GDPR rules.

Surely, you will need to cover the following:

- **who you are** (company, address, etc)
- **what data you collect** (IP addresses, name, email, phone, address, etc)
- **for what reason** you collect the data (invoicing, tracking, email communication, etc)
- **for how long** you retain it (e.g. you keep invoices for 6 years for accounting purposes)
- **which third parties** receive it (MailChimp, Google, CRM, etc)
- **how to download** data (either automatically or by emailing the Data Protection Officer)
- **how to delete** data (either automatically or by emailing the Data Protection Officer)
- **how to get in touch** with you for data-related issues (the contact details of the assigned Data Protection Officer, probably you)

Please note: WordPress is working on a Privacy Policy document generator, so if I were you I would wait a little longer ad use their upcoming functionality (it will be added to the "Tools" menu in the dashboard) to save time.

Now that you've written your Privacy Policy, you need to show this on every page of the website (a link in the footer would do) and – on top of that – a privacy policy checkbox on any opt-ins, user registration forms and checkout forms.

Based on the useful comments I received on this article, users need to **actively "check" or "agree" to the Privacy Policy** (exactly in the same way people do so with your T&C) so you must show a checkbox (and you cannot pre-select that checkbox by default).

So, how do you **add a "Privacy Policy" checkbox on the checkout page**? Well, in this case you can add a **second checkbox**, on top of the default "I've read and accept the terms & conditions".

This second checkbox might say something like "*I've read and accept the Privacy Policy*" (or a more user-friendly label such as "*Your personal data will help us create your account and to support your user experience throughout this website. Please read and accept our Privacy Policy document, where you can find for more information on how we use your personal data*"). You can use a simple WooCommerce snippet to add another checkbox to the checkout, including validation in case this is not checked by the customer.

So, this concludes the Privacy Policy work.

To-do list:

- Create a Privacy Policy page if you have none or wait for WordPress to release their PP generator
- Add who – what – how – why – when to Privacy Policy
- Display link to Privacy Policy in the footer
- Use a WooCommerce snippet to display the Privacy Policy on the checkout page

GDPR Compliance Step 3: WooCommerce User Registration

Ok, now that you got a little more familiar with the GDPR, we'll fly through the next WooCommerce website changes.

The WooCommerce "My Account" page has a **registration form with username and password**, if you've enabled this from the WooCommerce settings (*WordPress Dashboard > WooCommerce > Settings > Accounts > Enable customer registration on the "My account" page*):

WordPress Dashboard > WooCommerce > Settings > Accounts > Enable customer registration on the "My account" page
As this is personal data, **we need to show the Privacy Policy checkbox on the frontend**, similarly to what we've done on the checkout page.

Also remember to **only collect information you strictly require** to run your business (more in a following section).

Here's a snippet that allows you to add content on the WooCommerce My Account Register form – however, you will need to change "hook" and instead of using "*woocommerce_register_form_start*" you could try with "*woocommerce_register_form_end*" so that your HTML checkbox can be positioned below the register button.

To-do list:

- Double check if you have enabled WooCommerce My Account registrations
- If yes, add a Privacy Policy checkbox to the registration form with a WooCommerce snippet

GDPR Compliance Step 4: WooCommerce Cart Abandonment

This is a huge, super important, heavily affected WooCommerce functionality. Cart Abandonment plugins **collect email addresses without consent**. In fact, when a user is on the checkout page and enters her email address without completing the payment, she had "no time" to tick & accept the Terms and Conditions and read the Privacy Policy.

This is against the GDPR, which requires explicit consent (i.e. ticking a box).

Hopefully, the major Cart Abandonment plugins (YITH and Jilt) are already working on this and will provide you with a workaround to comply with GDPR.

Either way – I fear we might need to add a privacy policy link or – even worse – a checkbox below the **WooCommerce Checkout billing email address field**.

Here's how I imagine it:

A possible solution for GDPR-compliant cart abandonment plugins
In order to add that HTML content, I simply edited the "billing_email" checkout field label by using a default WooCommerce filter. If you want to give it a go, follow this WooCommerce tutorial: https://docs.woocommerce.com/document/tutorial-customising-checkout-fields-using-actions-and-filters/#section-2

An other alternative, could be to enable a "multi-step" checkout (though, that's terrible for your conversion rate) where you only **collect an email address in the first step and give users a checkout for consent**. Only then, you move to step #2 and make them complete the checkout.

Or you could "**disable guest checkouts**" from the WooCommerce settings. Once again, a terrible idea for your sales conversion rate, but a very good one indeed for GDPR… In this way users will be required to create an account in order to proceed to checkout – and you can therefore use your Cart Abandonment strategies with no hassle.

To-do list:

- Ask WooCommerce Cart Abandonment plugin developers how they are going to implement GDPR compliance

GDPR Compliance Step 5: WooCommerce Product Reviews

Ah, product reviews! In ecommerce, they really matter, don't they?

Of course, reviews contain personal data. You got it, you need user consent.

A good way to avoid this "consent" is to **only allow logged in customers who purchased the product to leave a review** (under *WordPress Dashboard > WooCommerce > Settings > Products > General > Reviews can only be left by "verified owners"*):

WordPress Dashboard > WooCommerce > Settings > Products > General > Reviews can only be left by "verified owners"
This is a nice compromise. **Customers will have already opted-in to your T&C and Privacy Policy**, so nothing will need to be added to the product review form if they're logged in.

If you allow reviews from non-logged-in, non-purchaser users, that's another story. Not sure why you'd do that, but in this case you'll need to add the Privacy Policy checkbox to the product review form.

Simple as that 🙂

To-do list:

- Tick the "Reviews can only be left by "verified owners"" checkbox in the WooCommerce settings

GDPR Compliance Step 6: WordPress Comments

If your WordPress pages and posts have comments enabled, here comes another GDPR compliance problem.

Users are usually prompted to enter their **name, email address and website URL together with their message** without the need to register an account (this happens on Business Bloomer for example, but maybe in your case you might force user registration in which case you're GDPR compliant in regard to WordPress comments by default).

This information (which also includes the user IP address and cookies to "remember" the user comment input fields if she wants to submit a second comment) is then stored within the WordPress Dashboard (Comments), WordPress single pages and single posts (Edit Post > Comments) and of course in **your WordPress Database**.

Once again this is pretty simple – you will need to add a **Privacy Policy consent message in the "Leave a comment" form and a "cookies opt-out"**.

I use the default WordPress Comments and they are working on making the comment form UX smoother and GDPR-friendly.

To-do list:

- Use the default WordPress Comments (GDPR updates coming soon) or select a GDPR-compliant WordPress Comments plugin
- Make sure to display the Privacy Policy checkbox before users submit a comment

GDPR Compliance Step 7: WordPress & WooCommerce Opt-in Forms

An opt-in form is a contact form where users enter their name and email address (usually) **to join your email marketing list (or database of contacts)**.

First of all, you must **remove all automatic opt-ins on your site**. All **checkboxes must be not checked** by default (a "checked" checkbox by default cannot imply acceptance).

Besides, are you passing those email addresses to sub-companies or other partners? Hopefully not…

Either way, users must:

- **consent**
- **know why** their personal data is needed ("*Enter your email address to receive our weekly newsletter*")
- **give you only relevant information** (to join your newsletter you don't need to ask for the date of birth… unless you want to send them a gift on their birthday! In this case, you've got to make it clear WHY you want that personal piece of data
- **know how to delete/download** the data at any time
- **know how to opt-out**

Usually, an opt-in form is tied to a specific software e.g. Mailchimp. In this case, Mailchimp should be **providing you the "revised", GDRP-compliant opt-in form in an upcoming plugin release**.

Whoever you send that email address to, make sure they are reliable (Mailchimp, ConvertKit, Aweber, etc.) and that they are actively working on HELPING you being GDPR-ready.

To-do list:

- Audit all your opt-in forms
- See if your opt-in form / newsletter / email marketing provider has a GDPR solution
- Make sure to display the Privacy Policy checkbox before users opt-in

GDPR Compliance Step 8: WordPress Contact Forms

Many of us use Contact Form 7, Ninja Forms, Gravity Forms etc. on our Contact Us pages and other WordPress pages.

These **forms now require Privacy Policy consent**.

Simply put, you should add a checkbox (very easy with any of the above plugins) close to the "Submit" button, to make sure users are agreeing to your Privacy Policy.

To add an "acceptance checkbox" to **Contact Form 7**, for example, look at https://contactform7.com/acceptance-checkbox/

To-do list:

- Add Privacy Policy checkbox to all your contact forms
- If the contact form is going to store personal data in a database and/or is tied to an email marketing software, you need to tell your users why and where you're storing data

GDPR Compliance Step 9: WooCommerce Analytics

I wrote a big article last week on advanced WooCommerce tracking. Whether you use Google Analytics, Metorik, or both, **you're capturing user data and using cookies without consent**. Same applies to Google AdWords, Facebook pixels and similar.

The best thing to do in this case is to check each provider's GDPR policy, because THEY are collecting the data and not YOU. You're just passing data to THEM: "*Under the GDPR, if you use Google Analytics, then Google is your Data Processor. Your organization is the Data Controller since you control which data is sent to Google Analytics*".

According to Google Analytics Team (they sent an email to all account holders on April 11th 2018):

- GDPR requires your attention and action even if your users are not based in the European Economic Area (EEA)
- They introduced **granular data retention controls** that allow you to manage how long your user and event data is held on our servers. Google Analytics will automatically delete user and event data that is older than the retention period you select
- Before May 25, Google Analytics will also introduce a new **user deletion tool** that allows you to delete all data associated with an individual user (e.g. site visitor) from your Google Analytics properties
- GA remain committed to providing features for **customizable cookie settings, privacy controls, data sharing settings, data deletion on account termination, and IP anonymization**
- They are also updating their policies as Data Processors

Indeed, I just found this new section in my GA account:

New GDPR section @ Google Analytics Admin

Also, if you use Metorik for tracking and reporting, then take a look at their "Metorik & GDPR" article where you will find detailed information.

To-do list:

- Only use reliable, GDPR-compliant tracking software
- Ask software providers how they're handling GDPR compliance
- Add to your Privacy Policy who handles your tracking data

GDPR Compliance Step 10: WordPress and WooCommerce Plugins

This is a very important section, but I won’t keep you here for too long.

It’s very easy.

Does plugin _____ either get, read, store, use, edit, handle, access user personal data?

Simply ask yourself this question for each plugin.

If the answer is yes:

- make sure it’s a reliable plugin
- make sure they are GDPR ready
- make sure to add the plugin to the list of “third parties” that get access to user data in your Privacy Policy

If the answer is no:

- are you 100% sure?
- really, really sure?
- good then, you don’t need to do anything

The beauty of GDPR is that **the WordPress ecosystem will improve exponentially in regard to data handling, security, transparency**.

Who knew GDPR was actually a good thing!

To-do list:

- Ask yourself the “magic” GDPR question about each plugin and theme
- Select GDPR-compliant plugins
- Discard non-GDPR-compliant plugins

GDPR Compliance Step 11: WordPress and WooCommerce APIs

We already mentioned this before, but "API" cover a lot of different applications. But first, what the heck is an API (in plain English pleaseeee)?

An API (Application Programming Interface) is basically "a piece of code" that **allows you to access an external software without ever leaving your website**.

API is used for transmitting data between two parties. A good analogy is to think about a bus traveling from one city to another, back and forth, moving people between the two points (data). Another good one (allow me to be a little Italian about it!) is to think about API as a waiter that takes your pizza order and lets the kitchen know what toppings you want 🙂 Either way, an API is a "data connector" – **private data might be passed from your website to another software and viceversa**, hence GDPR applies.

Examples:

- users can join your Mailchimp list without ever leaving your website, thanks to **Mailchimp API**
- users can checkout with Stripe without ever leaving your site, thanks to **Stripe API**
- and so on…

Facebook, Twitter, any kind of third party software give you APIs. These APIs connect your WooCommerce store to the outside world, **passing data to it – possibly private, personal user data**.

As long as you know:

- what APIs you use
- what data is sent
- if the API is GDPR compliant

…then you're good to go. As usual, you have to add to your Privacy Policy the detailed list of APIs that handle user data.

To-do list:

- Audit all your APIs
- Discard non-GDPR-compliant APIs
- Add APIs to your Privacy Policy

GDPR Compliance Step 12: Breach Notifications

Under the GDPR, if your website experiences a data breach this needs to be immediately communicated to those users affected by the breach. A notification must be sent within 72 hours.

What's a data breach by the way?

Well, this occurs when personal information is passed to:

- an unauthorized data processor or subcontractor
- a non-GDPR compliant body
- a third party without the knowledge of the data subject
- a hacker

On top of this, you will need to have **a security data breach response plan and process in place**.

To-do list:

- Secure your WordPress/WooCommerce website please!
- Subscribe to all your third-party software / API providers so that you can become aware as soon as a data breach that affects your users occurs
- Reduce the amount of data you store. Brilliant workaround, isn't it?
- Have a data breach emergency plan

(NEW!) GDPR Compliance Step 13: Consent From Existing WooCommerce Customers / Subscribers

One of you brought this up, so I did some research in regard to GDPR, WooCommerce and whether the new privacy changes should be retroactive or not.

Well, at the same time, I got several emails from various websites I'm subscribed to – asking me to accept their new T&C and Privacy Policy.

You can see where I'm going: GDPR is also retroactive. You must re-contact all your existing subscribers, customers, users, and ask them to actively give you "consent" as well as telling them how to download, delete or access their personal data.

It seems, however, it really all depends on how you captured the user data pre-GDPR:

1. Consent was provided, and asked in a GDPR compliant fashion
2. **Consent was provided, but asked in a not compliant GDPR fashion**
3. **Consent was not provided**

If you are within 2) or 3) you have two choices:

- Email existing users asking them to consent to your new policy
- Delete existing users (oh, it has been done already!)

You can use your email marketing platform to reach out to your existing customers/ subscribers if you imported your WordPress users into it at the time.

Otherwise you can download the WooCommerce "customers" with an export/import plugin, or even use an app called Metorik to reach out to your customer database.

Marketing Stuff You Can't Do Any Longer

We've seen so far what you should work on… but what about those "gray area" strategies some people have been using so far on their WordPress/WooCommerce websites?

Well, this needs to stop:

- Sending **unsolicited emails** (no more buying email lists please)
- Sending emails unless the shopper has opted in (hello, cart abandonment…)
- Sending unsolicited text messages (you need consent for this too)
- Doing any kind of "shady" marketing

Hopefully you haven't been doing any of this – nothing has changed. The only difference is that **you will now be fined**. I love GDPR 🙂

GDPR Compliance for WooCommerce: Wrapping Up

GDPR is not simple and is somewhat a gray area.

If you have experience within EU with digital sales, VAT, cookie laws and so on – you already know this is madness. Each accountant thinks this differently.

And you can expect the same with GDPR. Each lawyer, company, user will think this differently. **Interpretations will be completely contrasting**.

So, instead of waiting… please take action!

Complete steps 1-12 for your WooCommerce website and get some legal advice, no matter if you're based in EU or not. Or at least make sure to use only GPDR-compliant plugins and APIs, and write that Privacy Policy you've been postponing it for the last 20 years…

If you want to contribute to this post, give me useful links, correct any unlawful thing I might have written, please use the comment area below.

Here are documents you can gt some inspiration from:

- Business Bloomer Terms and Conditions
- Business Bloomer Privacy Policy (coming soon)

Good luck with GDPR!