

Appendix — Security {#Security}

Our usage as defined by our [ISP below](#). You may need to review your hosting services and provide gamers with direct access to your ISP services, Terms of Use, and Privacy Policies.

References

- *If you don't read anything; read this one!* Better Rules for Small Businesses https://ec.europa.eu/justice/smedataprotect/index_en.htm
- Wordpress GDPR Framework <https://codelight.eu/wordpress-gdpr-framework/>
- An Introduction to GDPR Compliance for WooCommerce Stores (<https://woocommerce.com/2017/12/gdpr-compliance-woocommerce/>)
- <https://premium.wpmudev.org/blog/gdpr-how-it-affects-wordpress-site-owners-and-developers/>

Examples to Follow

- PlayCanvas.com (based in the UK) has, in my opinion, a thorough example to follow for [cookies](#), [Privacy](#) and [Terms of Usage](#).

Europe's GDPR

Europe's [General Data Protection Regulation \(GDPR\)](#) which goes live on May 25th, is aimed at addressing all security risks by enforcing a strict data protection regulation across the EU and beyond.

What is the GDPR all about?

The GDPR regulation is the most impactful piece of data privacy legislation in this century so far.

Coming on the heels of the recent Facebook scandal, which revealed that the data of millions of Facebook users had been misused for the sake of third-party campaigns, the GDPR regulation is designed to regain order in how personal data is handled and stored online.

Despite being an EU regulation, the GDPR practically affects any company that processes the personal information of EU citizens.


That said, it applies to whether or not that company is based in the EU.

For instance, if a US-based company provides goods or services to EU citizens, it automatically falls within the scope of the regulation.

Personal data and individual rights

Approved on April 14, 2016, the new set of rules treats personal data protection as "a fundamental right" of all EU citizens and consumers.

Regarding online services, personal data could include anything from an individual's name to a physical location or an IP address.



Art. 4 GDPR Definitions

For the purposes of this Regulation:

1. 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

The law also covers browser cookies that can track the web activity of EU individuals.

In an effort to give consumers a bit of power in the so-called “big data” world, the new regulation also gives EU individuals more rights to their information.

All EU individuals will have the explicit right to know whether, where and for what purpose their personal data is being processed.

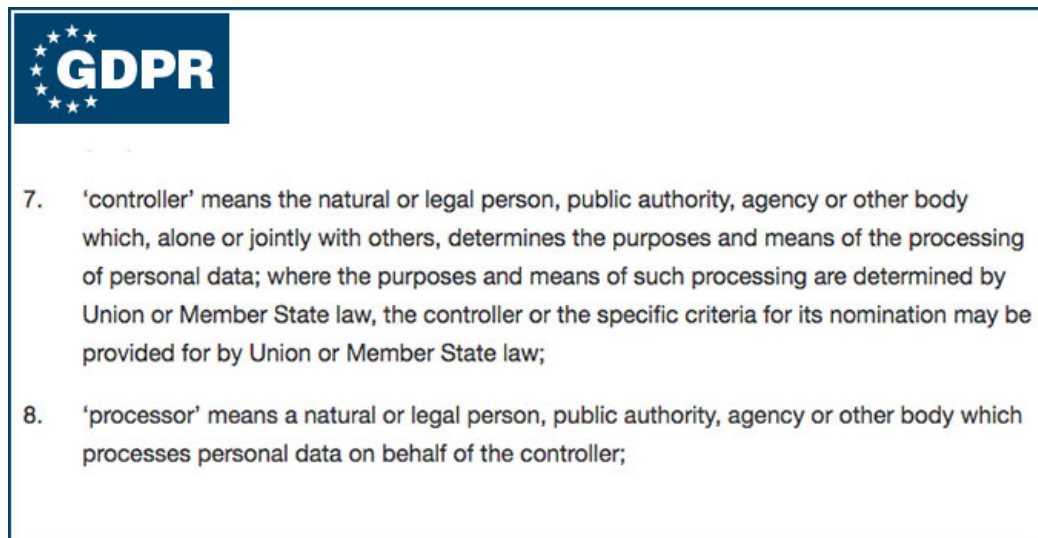
The GDPR empowers EU individuals to have their personal data erased or not processed further.

Data protection responsibilities under the GDPR

The GDPR sets out the rights of EU individuals and the respective obligations of data processing companies and organizations in a total of 99 articles.

The main business takeaway is that each company will have to justify the collection of personal data and to follow very strict rules in the process.

The regulation makes a clear differentiation between companies that direct the collection of data (data controllers) and those that actually process it (data processors).



Both controllers and processors will be delegated data protection responsibilities that will make them equally pursuant to GDPR compliance audits.

The GDPR requires companies to revise and update their privacy policies and to make them clearer and more transparent to EU users.

They will need to clearly specify what personal information is collected, for what purposes it is used and what legal basis each purpose is backed up by.

Apart from justifying their data processing activities, however, companies will also need to take specific technical and organizational measures to ensure the highest level of in-house data protection.

Wordpress Privacy Policy Guide

WordPress provides an excellent *Example Template* in their updated 4.9.6 release. It is provided below as a guide to model after and comply with GDPR requirements.

Introduction

Suggested text follows:

Hello,

This text template will help you to create your web site’s privacy policy.

We have suggested the sections you will need. Under each section heading you will find a short summary of what information you should provide, which will help you to get started. Some sections include suggested policy content, others will have to be completed with information from your theme and plugins.

Please edit your privacy policy content, making sure to delete the summaries, and adding any information from your theme and plugins. Once you publish your policy page, remember to add it to your navigation menu.

It is your responsibility to write a comprehensive privacy policy, to make sure it reflects all national and international legal requirements on privacy, and to keep your policy current and accurate.

Who we are

In this section, you should note your site URL, as well as the name of the company, organisation, or individual behind it, and some accurate contact information.

The amount of information you may be required to show will vary depending on your local or national business regulations. You may, for example, be required to display a physical address, a registered address, or your company registration number.

Suggest text: Our website address is: <http://gose-internet-services.net>.

What personal data we collect and why we collect it

In this section you should note what personal data you collect from users and site visitors. This may include personal data, such as name, email address, personal account preferences; transactional data, such as purchase information; and technical data, such as information about cookies.

You should also note any collection and retention of sensitive personal data, such as data concerning health.

In addition to listing what personal data you collect, you need to note why you collect it. These explanations must note either the legal basis for your data collection and retention or the active consent the user has given.

Personal data is not just created by a user's interactions with your site. Personal data is also generated from technical processes such as contact forms, comments, cookies, analytics, and third-party embeds.

By default WordPress does not collect any personal data about visitors, and only collects the data shown on the User Profile screen from registered users. However some of your plugins may collect personal data. You should add the relevant information below.

Comments

In this subsection you should note what information is captured through comments. We have noted the data which WordPress collects by default.

Suggest text: When visitors leave comments on the site we collect the data shown in the comments form, and also the visitor's IP address and browser user agent string to help spam detection.

An anonymised string created from your email address (also called a hash) may be provided to the Gravatar service to see if you are using it. The Gravatar service privacy policy is available here: <https://automattic.com/privacy/>. After approval of your comment, your profile picture is visible to the public in the context of your comment.

Media

In this subsection you should note what information may be disclosed by users who can upload media files. All uploaded files are usually publicly accessible.

Suggest text: If you upload images to the website, you should avoid uploading images with embedded location data (EXIF GPS) included. Visitors to the website can download and extract any location data from images on the website.

Contact forms

By default, WordPress does not include a contact form. If you use a contact form plugin, use this subsection to note what personal data is captured when someone submits a contact form, and how long you keep it. For example, you may note that you keep contact form submissions for a certain period for customer service purposes, but you do not use the information submitted through them for marketing purposes.

Cookies

In this subsection you should list the cookies your web site uses, including those set by your plugins, social media, and analytics. We have provided the cookies which WordPress installs by default.

Suggest text: If you leave a comment on our site you may opt-in to saving your name, email address and website in cookies. These are for your

convenience so that you do not have to fill in your details again when you leave another comment. These cookies will last for one year.

If you have an account and you log in to this site, we will set a temporary cookie to determine if your browser accepts cookies. This cookie contains no personal data and is discarded when you close your browser.

When you log in, we will also set up several cookies to save your login information and your screen display choices. Login cookies last for two days, and screen options cookies last for a year. If you select "Remember Me", your login will persist for two weeks. If you log out of your account, the login cookies will be removed.

If you edit or publish an article, an additional cookie will be saved in your browser. This cookie includes no personal data and simply indicates the post ID of the article you just edited. It expires after 1 day.

Embedded content from other websites

Suggest text: Articles on this site may include embedded content (e.g. videos, images, articles, etc.). Embedded content from other websites behaves in the exact same way as if the visitor has visited the other website.

These websites may collect data about you, use cookies, embed additional third-party tracking, and monitor your interaction with that embedded content, including tracing your interaction with the embedded content if you have an account and are logged in to that website.

Analytics

In this subsection you should note what analytics package you use, how users can opt out of analytics tracking, and a link to your analytics provider's privacy policy, if any.

By default, WordPress does not collect any analytics data. However, many web hosting accounts collect some anonymous analytics data. You may also have installed a WordPress plugin that provides analytics services. In that case, add information from that plugin here.

Who we share your data with

In this section, you should name and list all third-party providers with whom you share site data, including partners, cloud-based services, payment processors, and third party service providers, and note what data you share with them and why. Link to their own privacy policies if possible.

By default WordPress does not share any personal data with anyone.

How long we retain your data

In this section you should explain how long you retain personal data collected or processed by the web site. While it is your responsibility to come up with the schedule of how long you keep each dataset for and why you keep it, that information does need to be listed here. For example, you may want to say that you keep contact form entries for six months, analytics records for a year, and customer purchase records for ten years.

Suggest text: If you leave a comment, the comment and its metadata are retained indefinitely. This is so we can recognise and approve any follow-up comments automatically instead of holding them in a moderation queue.

For users that register on our website (if any), we also store the personal information they provide in their user profile. All users can see, edit, or delete their personal information at any time (except they cannot change their username). Website administrators can also see and edit that information.

What rights you have over your data

In this section, you should explain what rights your users have over their data and how they can invoke those rights.

Suggested test: If you have an account on this site, or have left comments, you can request to receive an exported file of the personal data we hold about you, including any data you have provided to us. You can also request that we erase any personal data we hold about you. This does not include any data we are obliged to keep for administrative, legal, or security purposes.

Where we send your data

In this section, you should list all transfers of your site data outside the European Union and describe the means by which that data is safeguarded to European data protection standards. This could include your web hosting, cloud storage, or other third party services.

European data protection law requires data about European residents which is transferred outside the European Union to be safeguarded to the same standards as if the data was in Europe. So in addition to listing where data goes, you should describe how you ensure that these standards

are met either by yourself or by your third-party providers, whether that is through an agreement such as Privacy Shield, model clauses in your contracts, or binding corporate rules.

Suggested test: Visitor comments may be checked through an automated spam detection service.

Your contact information

In this section, you should provide a contact method for privacy-specific concerns. If you are required to have a Data Protection Officer, list their name and full contact details here as well.

Additional information

If you use your site for commercial purposes and you engage in more complex collection or processing of personal data, you should note the following information in your privacy policy in addition to the information we have already discussed.

How we protect your data

In this section you should explain what measures you have taken to protect your users' data. This could include technical measures such as encryption; security measures such as two-factor authentication; and measures such as staff training in data protection. If you have carried out a Privacy Impact Assessment, you can mention it here too.

What data breach procedures we have in place

In this section, you should explain what procedures you have in place to deal with data breaches, either potential or real, such as internal reporting systems, contact mechanisms, or bug bounties.

What third parties we receive data from

If your website receives data about users from third parties, including advertisers, this information must be included in the section of your privacy policy dealing with third-party data.

What automated decision making and/or profiling we do with user data

If your web site provides a service which includes automated decision making* for example, allowing customers to apply for credit, or aggregating their data into an advertising profile* you must note that this is taking place, and include information about how that information is used, what decisions are made with that aggregated data, and what rights users have over decisions made without human intervention.

Industry regulatory disclosure requirements

If you are a member of a regulated industry, or if you are subject to additional privacy laws, you may be required to disclose that information here.