How Can WHMCS Help with GDPR Compliance?

The General Data Protection Regulation (GDPR) is Europe's big new data privacy law. It comes into effect on 25th May 2018 and is intended to strengthen and unify data protection for all individuals within the European Union (EU).

We have introduced several new features and functionalities in WHMCS 7.5 that are designed to help you with compliance, and we'll run through them and the relevant sections of the regulation in this article.

What is GDPR?

Firstly, let us recap what GDPR is.

GDPR has been introduced to give control back to citizens and residents over their personal data and to simplify the regulatory environment for international businesses. When GDPR takes effect, it will replace the 1995 Data Protection Directive (Directive 95/46/EC).

It takes effect on 25th May 2018.

I'm not in the EU so surely it doesn't apply to me?

It's not that simple. If you offer any products and services that may be purchased by customers located within Europe, then GDPR will apply to you. Unlike a directive, it does not require national governments to pass any enabling legislation and so it is directly binding and applicable to businesses all over the world.

In the UK, on 25th May 2018 the current law, the Data Protection Act 1998 (DPA) will be replaced by GDPR. Even after Brexit, GDPR provisions will be enshrined in a new UK specific law - the Data Protection Act 2018 (DPA 2018).

What data is protected?

The data that is protected under GDPR (as with the DPA) is data concerning individuals (not companies). However the definition is wider under GDPR and "Personal Data" extends to any information pertaining to an individual, whether it relates to their private, professional or public life. It can be anything from a name, to a home address, photo, email address, bank account details, posts on social networking websites, medical information, a computer's IP address and more. In other words, if in the course of running your business you collect and use any data about anyone that identifies them this will be Personal Data and you are required to follow the law in the way it is handled, accessed, stored or transferred. The individual is called the Data

Subject.

Here is a link to an overview of the GDPR by the ICO: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr.

How can WHMCS help?

While WHMCS enables you to collect and store information, it's important to note that you as the site owner are the data controller (i.e. the individual, company or organization that controls and uses the personal data). If your site can collect data from EU citizens, including those in the UK, then we recommend that you review your data privacy and security practices and begin researching your responsibilities.

Individual Rights

The right to be informed

Learn More

WHMCS enables you to define the URL of your Terms of Service. This is found in ***Setup* > *General Settings* > *Ordering***. When enabled, customers are required to agree to your Terms of Service in order to register an account and complete checkout. A user account cannot be created, and an order cannot be placed, without the user checking a box to confirm their agreement to your Terms of Service. That Terms of Service should also include a link to your Privacy Policy and any other important terms and service agreements you wish to make available.

The right of access/right to rectification

Learn more

WHMCS provides a self-service client portal that gives your customers access to login and view their personal information (profile data). This same client portal also provides your customers with access to update their personal information including name, email address, postal address and phone number as well as any custom fields you define. Previously, under the DPA, as a data controller you could charge an admin fee of 10 GBP for this service. This will no longer be allowed under the GDPR and DPA 2018.

The right to data portability

Learn more

Data portability means the right to receive personal data in a machine-readable format and to request for such data to be transferred directly from one controller to another. This right only applies where the processing is based on consent or for the performance of contract; and; when processing is carried out by automated means. There is no right to charge fees for this service.

New functionality added in WHMCS 7.5 allows you to generate a customizable export of data relating to a given client. Accessed via ***Reports > Exports > Client***, this allows you to generate an export in JSON format containing the data entity types you choose from a list of over 12 options.

The right to erasure (also known as the 'right to be forgotten')

Learn more

If you receive a request for erasure, you can perform a deletion of the customer record from WHMCS using the Delete Client functionality . Using this feature removes all data relating to a given customer including, but not limited to, personal information in the user's profile, service and invoice history, activity log entries, support ticket and email history.

To aid with this and enable you to automate the enforcement of any data retention policies you have, new to WHMCS 7.5 is a data retention policy automation feature that allows you to define a period of time for which client records should be kept. When enabled, once the required period of time has passed with no activity, customer records can be automatically purged. You can learn more about this new functionality here.

Lawful basis for processing

Contract

Learn more

In most cases, users register an account in your WHMCS instance as part of the process of submitting an order for services. In doing so, often end users are entering a contract with you to provide services. Collecting personal data about an individual in order to fulfill a contractual obligation is one possible lawful basis for the collecting of personal data. In a scenario such as this it may mean asking users for consent is not required. If this is something you choose to do, you should document your decision to rely on this lawful basis and ensure that you can justify your reasoning.

Consent

Learn more

The obligation to obtain the Data Subject's consent to collecting and processing their data under the GDPR is very onerous and will be strictly enforced. Consent cannot now be a pre-checked box, deemed automatic on registering for an online shop (for example) or inferred from silence or inactivity.

Consent must be given freely, be informed, be specific and be made by a clear affirmative action.

WHMCS 7.5 has introduced more flexibility and control over how your users opt into marketing emails such as those sent by the mass mail system which can be used for newsletters and similar products.

The Marketing Email settings can be found in ***Setup > General Settings > Other***.

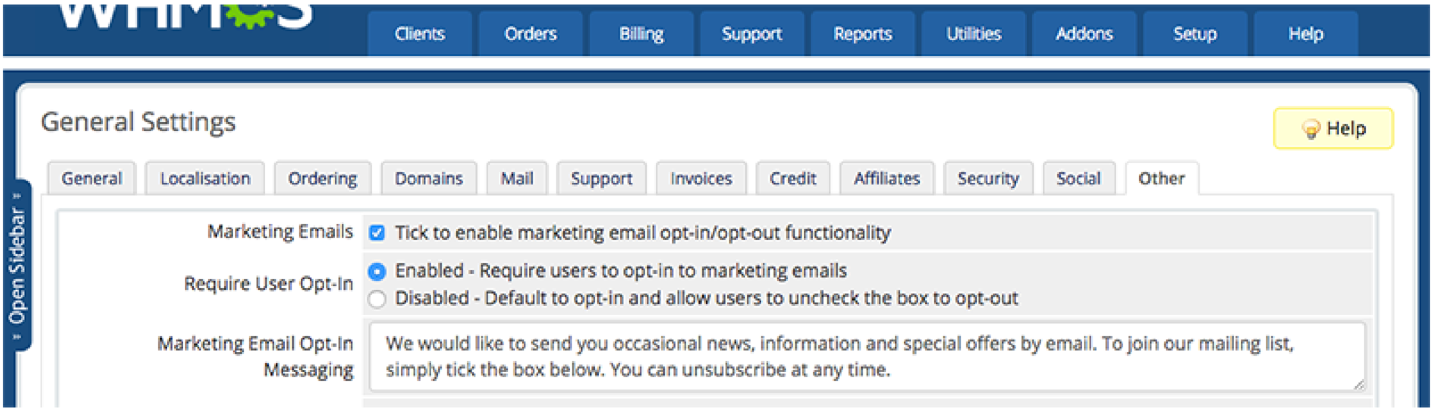
Learn more

The obligation to obtain the Data Subject's consent to collecting and processing their data under the GDPR is very onerous and will be strictly enforced. Consent cannot now be a pre-checked box, deemed automatic on registering for an online shop (for example) or inferred from silence or inactivity.

Consent must be given freely, be informed, be specific and be made by a clear affirmative action.

WHMCS 7.5 has introduced more flexibility and control over how your users opt into marketing emails such as those sent by the mass mail system which can be used for newsletters and similar products.

The Marketing Email settings can be found in ***Setup > General Settings > Other***.



General Settings

Marketing Emails ☑ Tick to enable marketing email opt-in/opt-out functionality

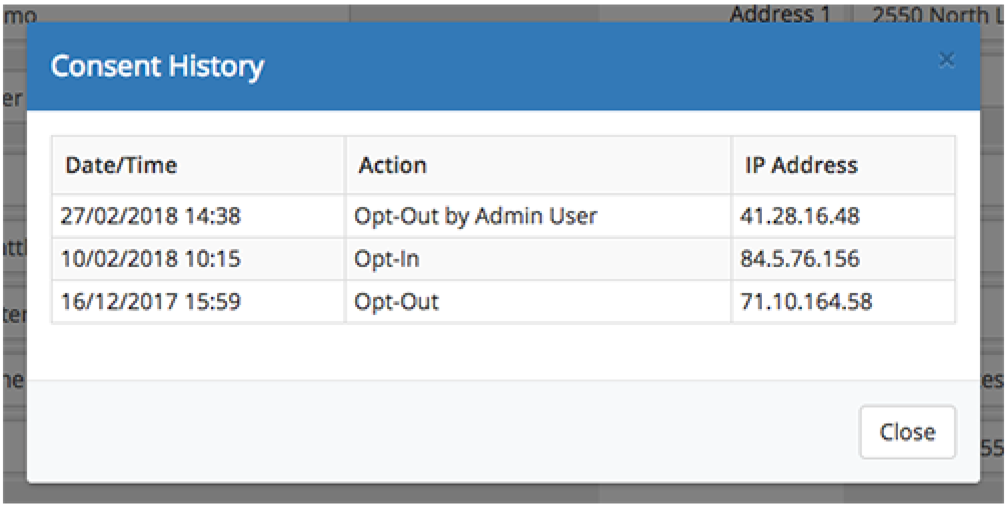
Require User Opt-In
● Enabled - Require users to opt-in to marketing emails
○ Disabled - Default to opt-in and allow users to uncheck the box to opt-out

Marketing Email Opt-In Messaging: We would like to send you occasional news, information and special offers by email. To join our mailing list, simply tick the box below. You can unsubscribe at any time.

If you're collecting consent for the purpose of marketing, a positive opt-in must also be separate from other terms and conditions, and you cannot bundle several uses under one consent. You need to specify clearly how you intend to use the data and obtain the consent for each specific use. You will also need to have simple ways for people to withdraw consent.

Recording when consent is given is an important part of the concept of accountability in GDPR, whereby organizations will have to demonstrate compliance with the principles relating to the processing of personal data.

With that in mind, in WHMCS 7.5 we've introduced a new consent log that records each time the consent setting is changed. For each change, WHMCS will record the date/time of that change, who it was initiated by and the IP address of the user. This new log can be accessed via the Profile tab with the admin clients profile summary.



Date/Time	Action	IP Address
27/02/2018 14:38	Opt-Out by Admin User	41.28.16.48
10/02/2018 10:15	Opt-In	84.5.76.156
16/12/2017 15:59	Opt-Out	71.10.164.58

Other new features include:

- A one-time conversion utility that allows you to migrate customers from the current opt-out setting to the new opt-in system, with a choice of whether to assume opt-in for existing customers or explicitly require it
- The ability to request consent from your users at any time using new email merge fields that are available to include opt-in and opt-out links in any emails you send
- New mass mail functionality that allows you to build and restrict as mass mail email recipient list based on country

Summary

We hope these new tools available with WHMCS 7.5 make it easier for you to meet your compliance needs and obligations with GDPR if you choose to do so.

As we mentioned in the How can I prepare for GDPR? article, every business is different and that may effect what you need to do to comply with GDPR. We really do encourage you to work with legal and other professional counsel to determine precisely how the GDPR might apply to you and your business. As a start, you may want to read the guidance published on the ICO website, subscribe to their newsletter and if you have specific queries there is a helpline dedicated to small organizations 0303 123 1113. You should seek legal advice from an intellectual property lawyer or data protection specialist if you have any concerns and especially if you have any threats or complaints in relation to data protection.

Please note these are guidelines only and should not be relied upon as legal advice. If you have any questions please contact the ICO or seek independent legal advice.