Jomres and the GDPR

What is GDPR and how does it affect Jomres?

The GDPR (General Data Protection Regulation) is legislation created by the EU that aims to give citizens more control over their personal data (PII). It impacts existing businesses across the EU and worldwide, as any companies holding or processing data from people in the EU will need to comply.

All Jomres users, most specifically site managers, therefore will need to be familiar with the GDPR because by its very nature Jomres is designed to capture the personal information of site visitors when they make bookings.

What functionality does Jomres have to make it compliant?

Personally Identifyable Information (PII) Encryption

GDPR : The requirement to report hacks of websites within 72 hours to those data subjects (users, aka guests) affected.

To begin with, unlike other self-hosted online booking engines Jomres encrypts all user data before it's saved to the database. This means that if the database is compromised through hacking or malicious actors then without the encryption key the data cannot be decrypted easily. The encryption key is stored by default in the /jomres/ directory, however *we advise you to move that file somewhere else outside of the site's root* and make it so that only the webserver user can use it. Once you have moved it you may need to modify /jomres/configuration.php with the new path.

Never, ever, ever delete the encryption key file, if you do you will not be able to decrypt your user and manager's data.

How does this make Jomres compliant?

It doesn't, however, in the event that your site has been hacked, then you are much less likely to be penalised by the GDPR Supervisory Authority if it can be demonstrated that the PII data recorded was encrypted *and the encryption key was not compromised*. User data encryption has long been a goal of ours to build into the system, and the introduction of the GDPR made it an ideal opportunity to add the feature.

What about other PII stored on the server, for example usernames and email addresses of the CMS users?

At the time of writing it is not possible for Jomres to force PII data stored elsewhere to be encrypted. You will need to contact the developers of any other installed systems and ask them about their GDPR compliance. Jomres can only be responsible for its own data.You as the data controller will need to ensure that you work holistically toward the site's compliance.

PII Opt-in

GDPR : The requirement to allow data subjects to opt into having their Personally Identifiable Information (PII) stored on the website.

Jomres is a booking engine. It's entire purpose is to make sales of bookings therefore it's very nature demands that it store user PII. When a user first visits the website they are presented with a message that asks them to confirm that the website can store PII. If the site visitor declines then they are limited in the actions that they can perform. They can for example perform searches and view property details pages however they cannot login or register or make bookings.. If they try they are redirected to a page explaining why and they are given the opportunity to opt-in to having their data stored. Both opt-ins and opt-outs are stored in a table so that in the event that they dispute that they have given the website permission to store their data, the website administrator is able to refer to the opt-in table to confirm or deny those facts.

Scheduled data cleanup

GDPR : The requirement that data should only be stored for as long as it is needed.

Jomres has built-in scheduled task handling. This isn't something that you need to configure on setup, the defaults are typically sufficient however you can change some settings in the administrator area.

When a visitor accesses any Jomres areas of the site, then basic information is stored in the sessions table. This information includes IP number, general location (country level) and if they make a booking then the information they entered into the booking form. This allows them to visit the booking form for various properties and they do not need to re-create the form's contents.

This session information is stored for about 24 hours. After that time the schedule system automatically cleans this session information.

When a booking is made, the booking engine's "state" at booking time is saved to a booking data archive table. This is required by the Booking Enquiries functionality because a booking has not been fully made until the manager approves the booking and the guest returns to the site to pay the deposit. This booking state information is retained in the archive for 60 days, then the schedule system will delete it.

Bookings themselves are stored in the system. Whilst the booking is still open, and for a certain time after it has been completed or cancelled, the booking will remain in the database. This gives property managers the opportunity to refer back to recent booking histories of individual

guests. After that time the booking data will be deleted. By default this period is 365 days, however it is possible to change this setting in Site Configuration.

This functionality is at odds with various nation's requirements to store invoice information for a period of years, for example in Germany invoices must be stored for 10 years. To that end, when an invoice is created the booker and seller's PII are stored encrypted in two tables. This data cannot be modified by property managers or guests, they are a snapshot of the booking and if the user requests that their information be anonymised later on this information is not affected by anonymisation features. Again, a setting in Site Configuration determines how long these invoices are stored. Once the invoices have gone over that threshold they too are deleted by the system's scheduling software.

PII Downloads

GDPR : The requirement to allow users to download all information about them that the website has about them.

Jomres allows all registered users to download any PII that is stored about them. PII is stored in two tables, the guest profiles table, and the guests table. The guest profiles table is generally considered to be the master copy of the user's PII and any changes made by the user are automatically filtered down to the guest's table. This allows users to update their records and any hotel that has received their data in the past will find the guest's details are automatically updated.

Hotels themselves have their own guest records. These are unique to the individual hotels meaning that managers of Property B cannot see the guest details for Property A. The only time that this rule can be broken is when the manager is a manager of two properties, for example A & B. This ensures that guest data is safely sandboxed and only authorised users can see that data.

Any registered user can request that the site make available to them all PII that the site stores for them. When they do that they are taken to a new page where they are presented with the contents of both of these tables.

Right to be Forgotten

GDPR : The requirement to allow users to delete their information where required. (Right to be Forgotten)

All users have the right to request that their PII be deleted. Because it is important to retain some information about users, who can and cannot have their data deleted depends on their status within the system.

If a user is not registered on the site and no PII has been stored for them, then naturally there is nothing to remove.

If a user is registered, but they do not have any outstanding bookings then they will be able to have their PII anonymised. The system does not outright delete data because that could cause problems, so instead at the user's request we will anonymise their records. This is acceptable to the GDPR.

If a user is a property manager they cannot have their PII deleted. They first need to contact the site administrator (you) and ask that their properties be assigned to another manager. Alternatively they can delete their properties themselves or let a Super Property Manager do it for them. At that point they are still a property manager, lack of properties notwithstanding, and the site administrator will need to rescind their property manager status (via the Users page in the administrator area). Once that has been done then the user will be able to use the RTBF functionality to anonymise their records.

To be GDPR compliant Jomres has been altered so that every non-registered user who makes a booking automatically has a user created for them in the CMS. In previous versions the ability to create users when bookings were made was an optional setting. This means that installations that have been in place for a long time may have many guest records where the guest cannot login and have their details anonymised. To allow the site administrator to be compliant with the GDPR site administrators have access to a menu option in the administrator area where they can view all guests from all properties and if requested they can anonymise those records themselves. This means that the site administrator will need at the very least to have a contact form on the site that users can use to contact the site administrators.

Does this mean that sites with Jomres installed are GDPR compliant?

No, it does not.

All this means is that Jomres helps you to ensure that the Jomres specific areas of your site, and its associated functionality, are compliant. Many sites will have other plugins installed that may or may not capture PII and you are advised to contact those plugin developers to ensure that they too are compliant. Ensuring that you, as a data controller, are compliant with the GDPR is something that you will have to analyse and put into place policies for yourself. We do everything that we can to help in this matter, however Jomres GDPR compliance is only a small part of the puzzle.

By using GDPR compliant software like Jomres you will be able to demonstrate to GDPR Supervisory Authorities that you are acting in good faith to be compliant. At this stage of the GDPR's introduction I am of the opinion that SAs will be more interested in supervising and/or penalising unscrupulous companies or individuals who are making no effort to be compliant. This will surely change in the future, and I will monitor the subject closely to ensure that I've done everything I can to protect our users and our user's users.

The GDPR Optins table

If you have a busy site, you will find that the xxxxx_jomres_gdpr_optins table gets quite large.

This table holds a record of every user who has opted in to having their data stored and is a requirement under the rules of the GDPR. If you have chosen to not enable the GDPR functionality then visitors to your site are automatically opted in to having their data stored.

If you deal with customers from the EU then you are legally required to store this information indefinately because it proves that a user, at X ip address, at Y date and time, gave you permission to store their information. The problem is that over time this table will get quite large.

When that happens, our advice is that you manually export the contents of that table to a storage location, and then truncate that table.