

GDPR

Customer guidance

This document is provided to customers of Spectulise Ltd. to help in their preparation for GDPR (General Data Protection Regulation). We don't make any guarantee of the completeness, accuracy or relevance to your particular circumstance. If you have particular questions, please contact us and we will do our best to assist.

There are also lots of resources on the Information Commissioner's website at <https://ico.org.uk>

What is the new law?

In a nutshell GDPR is about transparency about how our personal data is used.

Whilst there have been various examples of best practice, the collection of data has always been quite vague with users having to be careful about what they do or don't tick.

Moving forward companies have to be much more upfront about the data they collect and store, why they do so and how it will be used.

If a person's data is used in a way that they wouldn't reasonably expect, then the Information Commissioner will be able to take action.

The law also gives individuals more rights in terms of their access to their data.

If you haven't already started your own preparation, it is worth looking at the ICO 12 step guide - <https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf>

It is outside of the scope of this document to cover everything regarding GDPR but some key considerations you may want to look at regarding your website:

Email accounts

Emails you receive will undoubtedly contain personal data. The most obvious form is the name and email address of the person contacting you, but you may also be provided other personal information such as form submissions, contact details and more.

To aid keeping your email traffic secure it is recommended that you setup your email account using our secure connection settings. This makes it hard for messages to be intercepted as they are encrypted. If you haven't done so already, you can find the Secure SSL email settings in your control panel.

You should also consider steps to ensure the security of the devices that you access your emails on. This includes protection in the case of the device being lost or stolen – this might include passwords, encryption etc. and steps to prevent against viruses and malware.

Contact forms

If your website collects personal information such as via a form or contact form, you should consider the information being collected and why you need it and how long you will store it for.

You should also establish the lawful basis for processing that information?

<https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/>

In many cases, visitors to your website will be using your contact form to make an enquiry or ask a question – for example getting a quotation.

In cases like this the basis for collecting that information will probably be ‘contract’, meaning there is a general expectation that you will use their data to fulfil their request.

If, however, you plan to use that information going forwards – for example subscribing them to your mailing list, then that action should be explicitly explained as part of your form with an option box allowing them to select that outcome if they wish. The lawful basis in this instance would change to ‘Consent’.

Purchases

If your website allows purchases to be made, you should follow similar considerations. If you will simply fulfil the order then your legal basis may be ‘Contract’. If you add the customer to a database and use this information to market to them in the future you will need to consider the implication in terms of the options provided and the lawful basis for processing.

Assuming that the payment is taken by a third party provider you may also want to document this in your privacy policy.

Mailing lists

When operating a mailing list it should be optional for users to subscribe. You should make it clear what the person is signing up for, ideally through a double opt-in process (where the customer signs up and then confirms their interest by clicking a confirmation email).

Blogs

Blogs will often include the ability for users to make comments. These often collect a small amount of data (name and email address) to identify the person leaving the comment. You should include why and how you use this, if applicable, in your privacy policy.

With any data collected you should be considering how you keep it secure and how long you store it for.

SSL

We can now setup SSL (Secure Sockets Layer) on your website, on request, at no additional cost (except where a more substantial certificate is required due to the nature of the website). When websites use SSL, information is transferred between the server and end user securely by encrypting the data. You will normally see a green padlock in the corner of the URL bar and the address will start https://. This makes it a safer way to transmit personal data. To activate this, please contact us.