

April 2018



With a growing amount of personal data being captured on a daily basis, the regulations and laws imposed on organisations holding and processing individual's data has significantly increased in order to protect them.

The new European Union [General Data Protection Regulation \(GDPR\)](#) is a data privacy regulation that applies to all companies processing and holding the personal data of data subjects residing in the European Union. It aims to provide people with greater control over their privacy. The compliance deadline is on the 25th May 2018.

The GDPR can be summarised by the rights it grants to individuals; these include the...

- [Right to be informed](#): you will need to clearly inform your customers about the data you collect and how you will use that data
- [Right of access](#): customers should be able to gain access to all of their personal data
- [Right of rectification/erasure](#): your customers should be able to request the removal (except for certain limitations i.e. legal obligations) of their personal data and/or have any errors corrected.
- [Right to data portability](#): it should be possible to request a portable copy of data you hold (for example a CSV file)

You may also need to consider the [right to object](#), the [right to restrict processing](#) and the [right not to be subject to automated decision-making including profiling](#).

We recommend that a complete audit of your site is carried out by us in order to help you identify the data you collect, where it is held and the purpose you collect it along with any third parties it is shared with. This will help your business to achieve full transparency.

To help you to ensure your organisations compliance with the regulations we have prepared a handy 9-point helpsheet to assist you with auditing your Magento website for GDPR.

|                                              |          |
|----------------------------------------------|----------|
| <b>1. Consent</b>                            | <b>3</b> |
| <b>2. Admin access</b>                       | <b>4</b> |
| <b>3. Data storage</b>                       | <b>4</b> |
| <b>4. Third-parties and tracking scripts</b> | <b>5</b> |
| <b>5. Erasure</b>                            | <b>5</b> |
| <b>6. Data export</b>                        | <b>6</b> |
| <b>7. Opt-in and out</b>                     | <b>6</b> |
| <b>8. Cookies</b>                            | <b>6</b> |
| <b>9. Privacy policy</b>                     | <b>6</b> |

# 1. Consent

You will need to ensure that all customer data you hold is processed with full consent given (or perhaps another [lawful basis](#); such as to fulfil contractual obligations or legitimate interests in the case of email marketing) and that customers are well informed at the point of consent about how this data is to be used. Records to evidence consent should also be kept – including when, how, and what they were told.

Where, traditionally, a single terms and conditions checkbox at the end of the checkout may have been sufficient, you now need to be more explicit. For example, you may wish to offer a tooltip alongside the telephone number field to explain why you are collecting their number if you intend to use it for anything other than fulfilling your contractual obligations to them in the future (i.e. marketing). The ICO calls these “just-in-time” notices and might look similar to this:

## Create an account

Title

Mr

Name

Joe Bloggs

Email address

Username

Password

Confirm password

Create account

We use your email address as part of allowing you access to your account, and in order to contact you with important information about any changes to your account. [Please follow this link for further information.](#)

If you wish to obtain consent and not rely on [legitimate interests](#), you may wish to give further options for opting-in to different marketing channels (i.e. phone, email, text).

It is also recommended that privacy notices are presented in a [layered way](#) (i.e. follow this link for more information) which allows you to show the key privacy information immediately with more detailed information elsewhere. This is especially helpful for mobile users and for maintaining good UX.

## 2. Admin access

The Magento Admin likely provides full access to most, if not all, of the private data you collect. Access should be limited to GDPR trained members of your organisation and only third parties, such as ourselves, who are also GDPR compliant. Passwords should be strong to protect the data you hold.

Users should be assigned to limited access “roles” which allow you to limit the amount of data they can access to only that which they require.

All websites we run should operate with enforced SSL encryption. We can also setup IP restrictions on your Magento Admin area to limit which machines can access it as well as logging those that do.

## 3. Data storage

Have you considered who has access to your customers data in your store’s database? You should ensure that your hosting provider is GDPR compliant and that access to the database itself is limited to you and us. At outer/edge we will aim to ensure that all customer data is anonymised before being used for development purposes.

You may also want to discuss putting in place a regular vulnerability scan and penetration testing regime. You can also use the [MageReport.com](#) website to test for easy to spot security issues.

## 4. Third-parties and tracking scripts

If you send customer data to third parties for processing (for example; analytics and marketing segmentation tools) then your customers should be made clearly aware of this. You will also need to check that these third parties also comply with the GDPR and review your contract with them.

Google Analytics provides an option to anonymise users IP addresses. Combine this, with ensuring that users aren't identifiable in Analytics through the page URLs or the User ID feature.

We recommend moving all of your tracking scripts to Google Tag Manager. This provides a single location for enabling tracking once consent has been granted by the customer and dramatically decreases complexity.

## 5. Erasure

GDPR requires that a customer can request their data be removed (except, for example, where you have a legal obligation to retain it). Magento may record sales data even if the order has not resulted in a completed sale.

We can provide an extension to Magento that allows you to fully anonymise/erase customer data from all of these areas. We can also support you with the implementation of an option to allow your customers with accounts to remove this data. Customer data that may need to be made removable might include:

- Invoices and order history
- Contact form submissions
- Saved payment methods
- Product reviews
- Newsletter signups

## 6. Data export

You will need to be able to provide your customers with a portable version (CSV, for example) of the personal data you hold on them within 30 days of the request. We can advise on implementing methods to automate this, or, assist with individual requests.

## 7. Opt-in and out

There should no longer be any pre-filled checkboxes for opt-in on your site. The customer should be required to give explicit consent for you to contact them for marketing purposes (and thereafter the option to opt-out).

If you have collected data before GDPR for marketing purposes without consent, you will need to seek consent to retain this data or remove it.

## 8. Cookies

Implied consent cookie pop-ups (i.e. "This website uses cookies") are no longer sufficient - simply visiting a site doesn't count as consent. You will need to consider implementing a method to withhold certain cookies from being set until consent is given; this may be in the form of a pop-up or toolbar with an opt-in box or a setting in their account. You should clearly explain what cookies will be set (and why). Once enabled, this could trigger Google Tag Manager to activate all of your tracking scripts. It must also be possible for the customer to change these settings after given consent.

You will need to ensure that your cookie policy is up-to-date and correctly describes all of the cookies your website uses and their purpose.

## 9. Privacy policy

You will need to make sure that your privacy policy and terms are updated with GDPR compliance information. This is a good place to include a summary of the data you and your suppliers collect and how/why you collect and use it. Your policy should be easy to read and understand.

**Whilst we've spent a lot of time with GDPR to understand its intent and meaning, these recommendations should not be relied upon as legal advice or to determine how GDPR might apply to you and your organisation. We encourage you to work with a legally qualified professional to discuss GDPR, how it applies specifically to your organisation, and how best to ensure compliance.**

If you're just starting out on your GDPR journey, a great place to start is with the ICO's [12 steps to take now](#) and with Magento's own [GDPR FAQs](#)

*outer/edge is an ecommerce agency, specialising in Magento website development and ecommerce strategy. If you have a question about GDPR, would like us to undertake an audit or need any advice, get in touch with our experts today.*