BOOKSWARM

What does GDPR mean for your website?

The General Data Protection Regulation (GDPR) represents the biggest shake up of data protection legislation for many years, designed to strengthen and unify data protection for all individuals within the European Union (EU).

GDPR has the wide-ranging effects on how businesses handle all types of personal data, including e-mail marketing, customer data, business e-mail. As the public face of your business, there are many aspects of your website or e-commerce site which will be affected by GDPR, and the penalties for non-compliance are much greater than in the past.

Ahead of GDPR coming in to force, we have been working with a number of our clients to ensure their websites are GDPR-ready. Here are some of the things we think you need to know.

1. What is the GDPR?

The GDPR will supersede the current UK laws on data protection, which are enforced by the Information Commissioner's Office (ICO). It introduces tougher fines for non-compliance and breaches, and gives people more say over what companies can do with their data. It also makes data protection rules identical throughout the EU.

The fact that the UK is leaving the EU in 2019 doesn't matter, because EU laws and regulations will be incorporated in to UK law, and, equally important to non-European website owners, even if data controllers and processors are based outside the EU, the GDPR will still apply to them so long as they're dealing with data belonging to EU residents.

The EU has substantially expanded the definition of personal data under the GDPR. To reflect the types of data organisations now collect about people, online identifiers such as IP addresses now qualify as personal data. Other data, like economic, cultural or mental health information, are also considered Personally Identifiable Information (PII).

2. When does the GDPR come in to force?

Technically, the GDPR came in to force on 24th May 2016, but it's only from 25th May 2018 that the adjustment period ends and the law applies.

3. Who does the GDPR apply to?

'Controllers' and 'processors' of data need to abide by the GDPR. A data controller states how and why personal data is processed, while a processor is the party doing the actual processing of the data. So the controller could be any organisation, from a profit-seeking company to a charity or government. A processor could be an IT firm doing the actual data processing.

Are you a data controller or processor?

If your website, built for you by Bookswarm or anyone else, does any of the following things, then you almost certainly are:

- E-commerce website which takes orders and stores customer data
- Website with user registration functionality
- Website which has forms through which users can submit information – this could be a contact or enquiry form, a content upload mechanism, etc.
- Website with a mailing list signup mechanism

Obviously there are loads of other, non-website-related circumstances under which you could be a data controller or processor (customer databases, CRM, client lists, mailing lists, and so on) but we are going to focus on the website aspects here.

4. What does GDPR require you to do?

It's the data controller's responsibility to ensure their processor abides by data protection law and processors must themselves abide by rules to maintain records of their processing activities. If processors are involved in a data breach, they are far more liable under GDPR than they were under the Data Protection Act.

Once the legislation comes into effect, controllers must ensure personal data is processed lawfully, transparently, and for a specific purpose. Once that purpose is fulfilled and the data is no longer required, it should be deleted.

One of the following justifications must apply in order to lawfully process data:

PRO-TIP: In many cases, multiple justifications may operate together. A customer creating an account on an e-commerce website is consenting to their data being processed (setting up an account so they can place orders more quickly next time) and entering in to a contract or legal obligation (placing an order they want you to fulfil).

1 **If the subject has consented to their data being processed**

2 **To comply with a contract or legal obligation**

3 To protect an interest that is "essential for the life of" the subject

4 If processing the data is in the public interest

5 If doing so is in the controller's legitimate interest – such as preventing fraud

The first two on that list (in bold) are the key ones for most of our clients:

1 "If the subject has consented to their data being processed" could include registering an account, filling in a contact form or signing up for a mailing list

2 "To comply with a contract or legal obligation" is the most relevant to e-commerce – if a customer has placed an order, they have entered in to a contract with you which you can't complete without processing their data

5. What does consent look like?

Consent must be an active, affirmative action by the data subject – passive acceptance (asking people to opt out, or opting them in by default) will not be permissible.

Active, affirmative action could be:

- Explicit. Ticking a box which says "I agree to the processing of my personal data by X for the purposes of Y and Z"
- An affirmative act. Not explicit but done in the clear expectation of how the information would be used, e.g. user enters their e-mail address into an e-mail field marked "optional", with a short disclaimer underneath reading "Enter your e-mail address to receive information about products and services we think will interest you"

"Silence, pre-ticked boxes or inactivity should not ... constitute consent"

Recital 32

Controllers must keep a record of how and when an individual gave consent, and that individual may withdraw their consent whenever they want. This is really important – it means if you can't provide a record of exactly where and when a user gave their consent, then you could be held in breach.

6. When can people access the data stored by a data controller?

People can ask for access at "reasonable intervals", and controllers must generally respond within one month. The GDPR requires that controllers and processors must be transparent about how they collect data, what they do with it, and how they process it, and must be clear (using plain language) in explaining these things to people.

People have the right to access any information a company holds on them, and the right to know why that data is being processed, how long it's stored for, and who gets to see it. Where possible, data controllers should provide secure, direct access for people to review what information a controller stores about them.

They can also ask for that data, if incorrect or incomplete, to be rectified whenever they want.

Individuals also have the right to demand that their data is deleted if it's no longer necessary to the purpose for which it was collected. This is known as the 'right to be forgotten'. Under this rule, they can also demand that their data is erased if they've withdrawn their consent for their data to be collected, or object to the way it is being processed.

7. What happens if there's a data breach?

It's the controller's responsibility to inform its data protection authority of any data breach that risks people's rights and freedoms within 72 hours of becoming aware of it. The UK authority is the Information Commissioner's Office. Those who fail to meet the 72-hour deadline could face a penalty of up to 2% of their annual worldwide revenue, or €10 million, whichever is higher. They also have to inform affected customers within the 72-hour deadline.

8. What happens if there's a failure to observe the rules?

If you don't follow the basic principles for processing data, such as consent, ignore individuals' rights over their data, or transfer data to another country, the fines are even worse. Your data protection authority could issue a penalty of up to €20 million or 4% of your global annual turnover, whichever is greater.

9. What about cookies and other tracking data?

As you probably already know, websites use cookies to track returning visitors and collect usage information. It seems likely that visiting a website with a browser set to accept cookies will be taken as affirmative consent to place those cookies on the user's device. In other words, there is an assumption that if you didn't want cookies being placed on your device, you would make the appropriate changes to stop them from being set. That's good news – and it also means that those annoying cookie consent pop-ups will no longer be needed.

10. What should we be checking on our website?

Ensure your website has a Privacy Policy, written in plain English.

Ensure that the Privacy Policy explicitly identified all the ways in which the data controller (that's you) may use the data gathered (on that basis it's better to ask for permission for the broadest possible range of uses)

PRO-TIP: If in doubt, modify forms with a checkbox that users must agree to, with wording along the lines of:

'By using this form you agree with the storage and handling of your data by this website.'

Include a simple 'opt-out' form on any site which gathers user data, allowing the user to freely withdraw their consent. In broad terms this would be a very simple form – name, e-mail address – allowing a user to contact you and request opt-out or removal. What you do with that information depends on what you are doing with the data – it could be as simple as manually unsubscribing them from a mailing list, or it could be more complicated (removing them from in-house databases, deleting all of their e-mails).

Ensure your existing mailing lists are compliant. That means being able to say exactly how and when each user signed up, and that they have consented to be on the list. If your existing list contains any users who you added manually (because they were existing customers, or any other form of implied consent), or you can't say how and when people gave permission, you should no longer use that list.

Review all forms and other data collection points on your website to ensure they are compliant. It should be clear what purpose users are providing their data for. Existing forms may need to be re-worded or tweaked to make permissions more explicit.

In conclusion, GDPR is the biggest shake-up of data protection and management for many years. Don't ignore or neglect the changes you need to make – and if in doubt, seek professional legal advice.

About the author

Simon Appleby is the founder and Managing Director of Bookswarm, the only digital agency in the UK dedicated to delivering projects for publishers, authors and others in the world of books. Bookswarm has unrivalled experience in meeting the communications needs of publishers and authors in a way that is both excellent value for money and very easy to use, and specialises in WordPress development.

You can e-mail Simon – simon.appleby@bookswarm.co.uk – or call him on +44 (0) 7847 912989.