

EU Cookie Law

2012-04-30 01:41:59 by Guardian

On May 26, 2012 sites that fail to comply with the EU ePrivacy Directive disclosure requirements could be subject to fines up to £500,000.

These changes were outlined in the European Directive 2002/58/EC, primarily in article 5. What is more commonly termed "The Cookie Law" passed into force last year and requires website owners to provide upfront information about what information they are recording and obtain user consent.

All websites across the EU, regardless of where their servers are located, will have to adhere to these new privacy requirements. This includes EU citizens operating private websites, domains registered within the EU or domain names whose owners are EU citizens, business' who operate within the EU or any business that conducts business with with EU citizens.

Even if you do not fall into one of the above, Code Authors highly recommends you adhere to "The Cookie Law" as a matter of best practise and to prevent possible problems in the future.

The Cookie Law is a bit of misnomer really, the EU Directive is not just about cookies, it's about the ways that websites have been identifying or profiling users by implanting something directly on their device. This means that any locally stored files (Flash, HTML5 local storage, cached images, cached CSS etc) are equally restricted, IF they impact privacy.

The UK's Information Commissioner's Office (ICO) website is an example of this, which has a pop-up that links to the website's privacy disclosure notice and requires the user to acknowledge that the site will collect cookies. It's important to note that when the ICO asked visitors for their consent, they received a 90% fall in recorded site traffic.

The United Kingdom's Government Digital Service recently highlighted an important point for EU-based web analytics in the Implementer Guide to Privacy & Electronic Communications Regulations. Quoting the ICO, as long as "clear information" is given about activities, the ICO is "unlikely to prioritise first-party cookies used only for analytical purposes in any consideration of regulatory action."

Here is some guidance to help you stay within the Law.

1. Do a cookie audit. You need to be aware of exactly what cookies your website is using and what they are used for.
2. Get rid of the rubbish. This audit will probably reveal a lot of cookies that aren't really used for anything anymore. These should be removed from the site immediately.
3. Classify your cookies. You need to break down the cookies your site uses into the following categories:

- i. **Essential** For example, a cookie used to mark a visitor as a logged-in user
 - ii. **Non-essential but benign** For example, remembering a user's email address on a login form. This isn't essential for website functionality but makes it easier to use.
 - iii. **Moderately intrusive** These cookies are used to track user behaviour but in a minimally intrusive way. For example, the default cookies used by Google Analytics are available only to the owners of the site the user is browsing and don't reveal personally identifiable information.
 - iv. **Highly intrusive** For example, the Facebook 'Like' button; Disqus or cookies that track products you've looked at on a retail website and send you adverts for those items when you visit other sites. Highly-intrusive cookies leak user information to third parties or track personally identifiable information about your users.
4. Don't worry about the essentials. You don't need to get user permission for cookies that are essential for the operation of your website, such as remembering logged-in users.
 5. Create a compliance plan. For all the other classes of cookie you need a plan to answer two questions:
 - i. How can we prevent our website from using this cookie? This is something for your IT/web team to determine.
 - ii. How are we going to ask the user's permission to use this cookie? For example, you could have a pop-up box, 'cookie status' bar or warning bar on the website. Each option has pros and cons you need to analyse.
 6. Decide how risk-averse you feel. Breaking the law can carry a fine of up to £500,000, but anything other than minimal compliance could put businesses at a competitive disadvantage. Unfortunately, the Information Commissioner's Office (ICO) is currently giving out mixed messages – suggesting it may not prosecute businesses using less-intrusive cookies.
 7. If you're conservative, cover everything. A risk-averse business should implement a plan to require user consent for all non-essential cookies before the 26th May.
 8. If you're feeling brave, do nothing. Businesses with a larger appetite for risk or those for whom highly-intrusive cookies are important for revenue can adopt a 'wait and see' strategy. As it becomes clearer how the law will be enforced and what breaches the ICO prosecute first, they can implement an appropriate compliance plan.
 9. If you're in the middle, just go for the worst offenders. The middle way, and one that will be appropriate for most online businesses, is to require consent for (or simply don't use) highly-intrusive cookies.
 10. Stay up to date. This law is big news for any business with a website – and particularly

those with e-commerce platforms – and no one is quite sure how it will be applied. Keep your compliance plans handy and be ready to implement or change them depending on how the law develops.

<http://www.code-authors.com/modules.php?name=News&file=article&sid=185>