EU Cookie Law Compliance and Visitor Tracking

Alex Loveless

Feb 12

UserReplay®
Customer Experience Replayed

Contents

What is the EU cookie law?

On May 26th 2011 a new EU law came into effect that aims to protect the privacy of web users by requiring that websites request permission to use certain types of cookie. In the wording of the law, only cookies that are 'strictly necessary' may be used without first gaining user consent. This means that sites wishing to use cookies for tracking customer behaviour (among other uses) would require consent before placing them on the user's machine. The effects of this law will be profound and far-reaching. In the UK, the Information Commissioner's Office (ICO) has given UK businesses 1 year's grace until May 26th 2012 to become compliant with this law or potentially face legal action.

Does the cookie law affect my business?

If your business has a website, then almost certainly yes. The law affects any website using cookies, or any other client side data storage solution, which the vast majority of sites do. Some cookies can be deemed 'strictly necessary' and should not require consent (for example session cookies may fall into this category) but any cookies that facilitate tracking, advertising, recommendations, and personalisation will definitely require consent.

There is no single approach

Much has been said about the 'spirit of the law' but not a great deal about the practical applications of it. This is partly because the wording of the law itself could be interpreted in several different ways. In the UK, it's what the ICO think that really counts, but what they've said so far has begged as many questions as it has answered.

What is clear however is that the ICO believes in applying the law in a way that doesn't harm businesses and that online business owners need to decide the best approach for themselves. This means that businesses will need to devise a best-fit solution that broadly follows the 'spirit of the law' while also supporting business goals. As such this becomes a risk mitigation exercise – reducing the risk of being non-compliant while also managing the risk to the business of such changes. This will mean, for most businesses, a combination of solutions rather than just one thing. Some potential solutions will be covered in this paper.

We strongly advise you familiarise yourself thoroughly with the EU and ICO guidance on this before deciding on an approach, and consult your legal advisor before finalising your solution.

The whole solution – boxes that need ticking

Compliance with the cookie law isn't simply about gaining consent. A comprehensive solution requires a set of actions to raise awareness of cookie usage and allow customers full disclosure and control of how you use cookies when they use your site. The right solution for any given site and its users will vary, so taking all the contingent factors into account is important before attempting a solution. Here are some of the key areas to consider:

The prompt to consent

Just updating your privacy policy is not enough. The law clearly states that you must make your users explicitly aware of your intention to use cookies before setting them, and to get unambiguous consent to do so. This could be by using some sort of pop-up or banner, or perhaps an opt-in tick box at sign-up. We talk about some options for this in more detail below.

The facility to change consent option

The customer must have the facility to change their cookie preference at any time. This should be easy to find (perhaps in their personal settings, or clearly linked from the footer or privacy policy) and take immediate effect.

Privacy policy

The ICO guidelines make it clear that the privacy policy has a clear role in complying with the law. It should be prominent and easy to find and make clear reference to what cookies are used and for what purpose.

Cookie expiry

Your privacy settings should make clear reference to cookie expiry duration. Once a user has opted-in you can – assuming you've made your policy absolutely clear- set your cookies to expire after whatever duration you like, or to not expire at all. However, it may be wise to use a limited cookie duration as a softener to opting in. It's also fair to say that the ICO should look more favourably on a solution that included limited cookie durations.

Solutions for gaining consent

The main thrust of the law is to make website owners obtain prior and explicit consent from the visitor before setting a cookie. You only need to gain consent once, when a user first arrives on your site which can be assumed to continue to be the case across multiple sessions. There are many possible interpretations of this part of the law and how to implement it. The following are some of those mentioned specifically within the ICO guidelines as possible solutions. Which method is best and how to implement any given solution will vary from business to business depending on the nature of the site and business, and their preferred cookie use.

Banner/lightbox/pop-up solutions

This is currently the most obvious and popular solution. Essentially, the first time a user hits your site you bring up an obvious message requesting that the user gives or denies their consent (it would be valid to plant an anonymous cookie to record the customers consent preference across sessions, as long as you make it clear that this is what you're doing).

There are various possible ways to implement such a thing, some more intrusive than others. The idea is that the message and option to consent should be unavoidable or at least very hard to ignore. Not a great first experience, but one that users will get increasingly used to as more sites comply with the law. Should your method be too subtle and the user fails to choose a consent option and carries on using the site, then you're on a knife-edge as far as compliance goes should you then assume positive consent. In this circumstance the ICO recommend that you should employ clear reminders throughout that user's session warning them of their implicit consent and what it means to them. Here are some specific methods you could employ to gain consent:

A full screen lightbox – This would require the users to acknowledge it (in the form of consent preference) before allowing them to continue. This is very intrusive but would likely prove the most effective method of ensuring the option to consent is acknowledged and acted on.

A javascript pop-up – This slightly more subtle option would pop-up in the centre of the page, or perhaps emerge from the side – somewhere the user cannot avoid seeing it – invasive but without preventing the use of the site. The user would then need to express consent to make the box go away. This is a good compromise solution by being noticeable while not being overly intrusive.

A banner or pop-down at the top of the webpage – This is the more subtle option that will likely prove the most popular. Given that such things are quite commonplace (many browsers use similar methods to ask whether to save users' passwords) this would be quite easy to miss or ignore and thus this method could prove less effective. You may wish to leave the banner in place for subsequent page views should the user ignore it, or even employ a more forceful method such as a much bigger banner in this circumstance.

All these solutions should display some unambiguous text stating what the user is being asked to consent to with the details, or clear links to details, of what cookies there are and how they will be used.

Consent at sign-up

A valid scenario for attaining consent specifically mentioned by the ICO is to do so at the point of sign-up. When a user signs up for a service (chooses a username and password, enters details etc.) you could have an opt-in checkbox. This approach is common with attaining consent for email marketing. This is a perfectly valid approach but comes with a significant caveat: no cookies can be employed prior to the signup event, unless you employ some other means of gaining consent at an earlier stage. This may not be a big issue for a site for which the majority of its traffic requires the user to be logged in, for example a social network. However, for ecommerce sites this may be a problem as it becomes hard to monitor and measure traffic prior to someone signing up, thereby making marketing metrics inaccurate and user experience hard to attain.

Here are some other slightly more questionable approaches to gaining consent.

Browser settings

There is a view that browser settings are the logical home for consent preferences, and both the EU and ICO guidelines mention this as a valid approach. The user would store generic or even site-specific preferences in the browser and websites would honour these. In practice though, this is currently not a workable solution and some argue it never will be. There is currently a basic ‘Do Not Track’ user setting standard that allows users to state a preference as to whether they are tracked or not across all sites. This is not implemented across all browsers (Google are refusing to implement this for Chrome) and at present very few sites honour this.

Even if all browsers suddenly implement a universal standard tomorrow then it would still fall to the website owner to implement a solution for reading and acting on these settings. This of course assumes that, (a) the user has a browser that supports this and (b) the user is aware of and has adjusted these settings to their preference. Should this not be the case with any given user, the responsibility still falls to the site owner to attain a consent status, or assume non-consent. Given that awareness of this functionality will take some time to seep into the public consciousness, sites that need to plant cookies will need to implement some other solution.

Like it or lump it approach

The wording in the ICO guidelines is ambiguous in places and appears to leave room for solutions that don’t, in theory, require consent. Solutions that evade the spirit of the guidelines and that attempt to exploit this ambiguity will not likely be tolerated. However the ‘like it or lump it’ approach is one that could slip through. Essentially, if you’re brave enough (or foolish enough!) to say to your users ‘if you don’t like cookies you cannot use our site’ then in theory no consent is required. If and this is a BIG IF, you either (a) make it continuously and explicitly clear, that this is what’s happening, or(b) you simply bar users who don’t agree. In this option, you would give the option to either consent or leave the site.

There’s some argument about whether this constitutes a valid approach in the eyes of the law, and it’s hard to see what sort of business could safely employ such a brutal approach, but at the time of writing this it still appears to be a valid one.

Alternative tracking

It's not just cookies

Although everyone is calling this the 'cookie law', the actual EU legislation doesn't actually explicitly mention cookies. The paragraphs in question mention 'information stored, in the terminal equipment of a subscriber' and in most cases this means cookies. But the ICO has been clear to point out that this includes any client side method of storing information (anonymous or otherwise) about the user. This logically extends to JavaScript tags that do not store information but are a means of communicating visitor movements and browser entries:

1 JavaScript tags that fire in the Visitors browser, track visitors interactions and report to 3rd party 'analytics' aggregators

2 In most cases the visitor isn't willingly or knowingly giving their information to such 3rd parties

3 Depending on the actual personal identifiable information being tracked, there may be PCI issues in addition to the obvious concerns about information risk

For the reasons above, solutions that allow you to continue to track user behaviour while honouring their no cookie choice may still leave you on the wrong side of the law if used surreptitiously. The point in question with these solutions is that they are invasive for the customer and the data collected is not stored within the host organisation. If you are transparent about your usage of such technologies then these products, in the context of a broader compliant cookie strategy, could still be a vital tool in your cookie compliance toolkit.

The server-side solution

So how will you know how many people are still on your site if a lot of your customers opt out of cookies? Here are some solutions that don't rely on cookies.

Tracking visitors from inside your firewall

Technologies such as UserReplay work by placing an extra server on your network running what can be described as a 'packet sniffer', which non-intrusively intercepts traffic to and from your servers and logs it to a database. This allows you to gather detailed stats about your website's usage without any client side tagging. And because they see all the values that are passed to and from the server, the user's session can be reconstructed exactly as the user saw them, so you can replay the session and see what the user sees.

Products like UserReplay combine neatly with client side analytics solution such as Google Analytics to provide a full picture of customer behaviour. In circumstances where a significant number of your users have opted out of cookie based tracking, then UserReplay could be employed to keep track of these sessions for reporting purposes.

Conclusion

When the new law covering website privacy comes into effect in May 2012 there will not be a blanket ban on visitor tracking methodologies. A balance needs to be struck between the protection of website visitors' privacy and the benefits of being 'recognised' by favourite websites and receiving personalised content. There will be a requirement for all sites to be much more transparent about the cookies that they store in visitors browsers and they will require some form of explicit consent from the visitor. Third-party cookies such as those used by ad content providers that track visitors across multiple domains are likely to come in for the strongest treatment.

There are quite a few areas to consider when implementing a cookie law compliance solution. On a daily basis new solutions are launched and new guidance and opinion on the subject is asserted. However, as a business it is your responsibility to familiarise yourself with the official guidance ahead of it becoming mandatory and to decide on a solution that works for your business while adhering to the spirit of the directive.

To find out more about
UserReplay call **01483 685420**
or visit **www.userreplay.com**

Further reading

http://www.ico.gov.uk/for_organisations/privacy_and_electronic_communications/the_guide/cookies.aspx

http://www.howstuffworks.com/cookie.htm

http://en.wikipedia.org/wiki/HTTP_cookie

UserReplay®

Customer Experience Replayed

40 Occam Road
Guildford
Surrey GU2 7YG

Telephone **01483 685 420**
Email **info@userreplay.com**

www.userreplay.com