Changes to the rules on using cookies and similar technologies for storing information

The law which applies to how you use cookies and similar technologies for storing information on a user's equipment such as their computer or mobile device changed on 26 May 2011. This document sets out these changes and explains what steps you need to take to ensure you comply.

It is aimed at those organisations which are starting to think about how they will comply with the new rules. It is a starting point for getting compliant rather than a definitive guide.

These changes apply to storage or gaining access to information stored, in the device of a subscriber or user. This means the use of cookies and similar technologies for storing information.

A cookie is a small file of letters and numbers downloaded on to a device when the user accesses certain websites. Cookies allow a website to recognise a user's device.

The Regulations also apply to similar technologies for storing information. This could include, for example, Local Shared Objects (commonly referred to as "Flash Cookies").

For more information see: http://www.allaboutcookies.org/

We will use the term cookies through this document to refer to cookies and similar technologies covered by the Regulations.

As explained below, you will need a user's consent if you want to store a cookie on their device. The ICO recognises that cookies perform a number of legitimate functions. We also recognise that gaining consent will, in many cases, be a challenge. However, it is important to remember that that these rules give you the opportunity to check how well you explain how your web pages work to the people who visit them. Complying with the new rules will allow you to be confident that your users have a better and clearer understanding of what you do and how you do it.

What is changing?

The previous rule on using cookies for storing information was that you had to:

- tell people how you use cookies, and
- tell them how they could 'opt out' if they objected.

Many websites did this by putting information about cookies in their privacy policies and giving people the possibility of 'opting out'.

This rule was set out in Regulation 6 of the Privacy and Electronic Communications Regulations 2003 (PECR):

> ***6.*** *(1) Subject to paragraph (4), a person shall not use an electronic communications network to store information, or to gain access to information stored, in the terminal equipment of a subscriber or user unless the requirements of paragraph (2) are met.*
>
> *(2) The requirements are that the subscriber or user of that terminal equipment -*
>
> *(a) is provided with clear and comprehensive information about the purposes of the storage of, or access to, that information; and*
>
> *(b) is given the opportunity to refuse the storage of or access to that information*

What do the new rules say?

The new requirement is essentially that cookies can only be placed on machines where the user or subscriber has given their consent.

> *6 (1) Subject to paragraph (4), a person shall not store or gain access to information stored, in the terminal equipment of a subscriber or user unless the requirements of paragraph (2) are met.*
>
> *(2) The requirements are that the subscriber or user of that terminal equipment--*
>
> *(a) is provided with clear and comprehensive information about the purposes of the storage of, or access to, that information; and*
>
> *(b) has given his or her consent.*
>
> *(3) Where an electronic communications network is used by the same person to store or access information in the terminal equipment of a subscriber or user on more than one occasion, it is sufficient for*

the purposes of this regulation that the requirements of paragraph (2) are met in respect of the initial use.

"(3A) For the purposes of paragraph (2), consent may be signified by a subscriber who amends or sets controls on the internet browser which the subscriber uses or by using another application or programme to signify consent.

(4) Paragraph (1) shall not apply to the technical storage of, or access to, information--

(a) for the sole purpose of carrying out the transmission of a communication over an electronic communications network; or

(b) where such storage or access is strictly necessary for the provision of an information society service requested by the subscriber or user.

Why is this rule changing?

The European Directive on which the Regulations are based has been revised. UK law has to change to implement that changed Directive.

Does this consent rule apply to every type of cookie?

The only exception to this rule is if what you are doing is 'strictly necessary' for a service requested by the user. This exception is a narrow one but might apply, for example, to a cookie you use to ensure that when a user of your site has chosen the goods they wish to buy and clicks the 'add to basket' or 'proceed to checkout' button, your site 'remembers' what they chose on a previous page. You would not need to get consent for this type of activity.

This exception needs to be interpreted quite narrowly because the use of the phrase "strictly necessary" means its application has to be limited to a small range of activities and because your use of the cookie must be related to the service requested by the user. Indeed, the relevant recital in the Directive on which these Regulations are based refers to services "explicitly requested" by the user. As a result our interpretation of this exception therefore has to bear in mind the narrowing effect of the word "explicitly". The exception would not apply, for example, just because you have decided that your website is more attractive if you remember users' preferences or if you decide to use a cookie to collect statistical information about the use of your website.

When are the rules changing?

The new legislation comes into force on 26 May 2011.

You need to take steps now to prepare and ensure you are ready to comply.

What will happen to me if I don't do anything?

The government's view is that there should be a phased approach to the implementation of these changes. In light of this if the ICO were to receive a complaint about a website, we would expect an organisation's response to set out how they have considered the points above and that they have a realistic plan to achieve compliance. We would handle this sort of response very differently to one from an organisation which decides to avoid making any change to current practice. The key point is that you cannot ignore these rules.

The ICO will be issuing separate guidance on how we intend to enforce these Regulations.

So what do I need to do now?

We advise you to now take the following steps:

1. Check what type of cookies and similar technologies you use and how you use them.
2. Assess how intrusive your use of cookies is.
3. Decide what solution to obtain consent will be best in your circumstances.

1. Check what type of cookies you use and how you use them

This might have to be a comprehensive audit of your website or it could be as simple as checking what data files are placed on user terminals and why.

You should analyse which cookies are strictly necessary and might not need consent. You might also use this as an opportunity to 'clean up' your webpages and stop using any cookies that are unnecessary or which have been superseded as your site has evolved.

2. Assess how intrusive your use of these cookies is

The new rule is intended to add to the level of protection afforded to the privacy of internet users. It follows therefore that the more

intrusive your use of cookies is, the more priority you will need to give to considering changing how you use it.

Some of the things you do will have no privacy impact at all and may even help users keep their information safe. Other technologies will simply allow you to improve your website based on information such as which links are used most frequently or which pages get fewest unique views. However, some uses of cookies can involve creating detailed profiles of an individual's browsing activity. If you are doing this, or allowing it to happen, on your website or across a range of sites, it is clear that you are doing something that could be quite intrusive – the more privacy intrusive your activity, the more priority you will need to give to getting meaningful consent.

It might be useful to think of this in terms of a sliding scale, with privacy neutral cookies at one end of the scale and more intrusive uses of the technology at the other. You can then focus your efforts on achieving compliance appropriately providing more information and offering more detailed choices at the intrusive end of the scale.

3. Decide what solution to obtain consent will be best in your circumstances

Once you know what you do, how you do it and for what purpose, you need to think about the best method for gaining consent. The more privacy intrusive your activity, the more you will need to do to get meaningful consent.

I have heard that browser settings can be used to indicate consent – can I rely on that?

One of the suggestions in the new Directive is that the user's browser settings are one possible means to get user consent. In other words, if the user visits your website, you can identify that their browser is set up to allow cookies of types A, B and C but not of type D and as a result you can be confident that in setting A, B and C you have his consent to do so. You would not set cookie D.

At present, most browser settings are not sophisticated enough to allow you to assume that the user has given their consent to allow your website to set a cookie. Also, not everyone who visits your site will do so using a browser. They may, for example, have used an application on their mobile device. So, for now we are advising organisations which use cookies or other means of storing information on a user's equipment that they have to gain consent some other way.

If I can't rely on browser settings what other options are there?

In future many websites may well be able to rely on the user's browser settings to demonstrate that they had the user's agreement to set all sorts of cookies. We are aware that the government is working with the major browser manufacturers to establish which browser level solutions will be available and when. For now, though, you will need to consider other methods of getting user consent. What is appropriate for you will depend on what you are doing. You should also consider the fact that not all of your website visitors will have the most up-to-date browser with these enhanced privacy settings. You would still need to gain consent for those users.

You need to provide information about cookies and obtain consent before a cookie is set for the first time. Provided you get consent at that point you do not need to do so again for the same person each time you use the same cookie (for the same purpose) in future.

- **Pop ups and similar techniques**

Some have suggested using pop-ups to ask for consent. This might initially seem an easy option to achieve compliance – you are asking someone directly if they agree to you putting something on their computer and if they click yes, you have their consent - but it's also one which might well spoil the experience of using a website if you use several cookies.

However, you might still consider gaining consent in this way if you think it will make the position absolutely clear for you and your users. Many websites routinely and regularly use pop ups or 'splash pages' to make users aware of changes to the site or to ask for user feedback. Similar techniques could, if designed well enough, be a useful way of informing users of the techniques you use and the choices they have. It is important to remember though that gaining consent in this potentially frustrating way is not the only option.

- **Terms and conditions**

There are already lots of examples of gaining consent online using the terms of use or terms and conditions to which the user agrees when they first register or sign up. Where users open an online account or sign in to use the services you offer, they will be giving their consent to allow you to operate the account and

offer the service and there is no reason why consent for the purposes of complying with the new rules on cookies cannot be gained in the same way.

However, it is important to note that changing the terms of use alone to include consent for cookies would not be good enough even if the user had previously consented to the overarching terms. To satisfy the new rules on cookies, you have to make users aware of the changes and specifically that the changes refer to your use of cookies. You then need to gain a positive indication that users understand and agree to the changes. This is most commonly obtained by asking the user to tick a box to indicate that they consent to the new terms.

The key point is that you should be upfront with your users about how your website operates. You must gain consent by giving the user specific information about what they are agreeing to and providing them with a way to show their acceptance. Any attempt to gain consent that relies on users' ignorance about what they are agreeing to is unlikely to be compliant.

- **Settings-led consent**

Some cookies are deployed when a user makes a choice about how the site works for them. In these cases, consent could be gained as part of the process by which the user confirms what they want to do or how they want the site to work.

For example, some websites 'remember' which version a user wants to access such as version of a site in a particular language. If this feature is enabled by the storage of a cookie, then you could explain this to the user and that it will mean you won't ask them every time they visit the site. You can explain to them that by allowing you to remember their choice they are giving you consent to set the cookie.

This would apply to any feature where you tell the user that you can remember certain settings they have chosen. It might be the size of the text they want to have displayed, the colour scheme they like or even the 'personalised greeting' they see each time they visit the site.

- **Feature-led consent**

Some objects are stored when a user chooses to use a particular feature of the site such as watching a video clip or when the site remembers what they have done on previous visits in order to personalise the content the user is served. In these cases, presuming that the user is taking some action to tell the webpage what they want to happen – either opening a link, clicking a button or agreeing to the functionality being 'switched on' – then you can ask for their consent to set a cookie at this point. Provided you make it clear to the user that by choosing to take a particular action then certain things will happen you may interpret this as their consent. The more complex or intrusive the activity the more information you will have to provide.

Where the feature is provided by a third party you may need to make users aware of this and point them to information on how the third party might use cookies and similar technologies so that the user is able to make an informed choice.

- **Functional uses**

You will often collect information about how people access and use your site and this work is often done 'in the background' and not at the request of the user. An analytic cookie might not appear to be as intrusive as others that might track a user across multiple sites but you still need consent. You should consider how you currently explain your policies to users and make that information more prominent, particularly in the period immediately following implementation of the new Regulations. You must also think about giving people more details about what you do – perhaps a list of cookies used with a description of how they work – so that users can make an informed choice about what they will allow.

One possible solution might be to place some text in the footer or header of the web page which is highlighted or which turns into a scrolling piece of text when you want to set a cookie on the user's device. This could prompt the user to read further information (perhaps served via the privacy pages of the site) and make any appropriate choices that are available to them.

If the information collected about website use is passed to a third party you should make this absolutely clear to the user. You should review what this third party does with the information about your website visitors. You may be able to alter the settings of your account to limit the sharing of your visitor information. Similarly, any options the user has should be prominently displayed and not hidden away.

- **Third party cookies**

Some websites allow third parties to set cookies on a user's device. If your website displays content from a third party (eg from an advertising network or a streaming video service) this third party may read and write their own cookies or similar technologies onto "your" users' devices. Obviously, the process of getting consent for these cookies is more complex and our view is that everyone has a part to play in making sure that the user is aware of what is being collected and by whom. There are a number of initiatives that seek to ensure that users are given more and better information about how their information might be used. These will no doubt adapt to achieve compliance with the new rule but we would advise anyone whose website allows or uses third party cookies to make sure that they are doing everything they can to get the right information to users and that they are allowing users to make informed choices about what is stored on their device.

This may be the most challenging area in which to achieve compliance with the new rules and we are working with industry and other European data protection authorities to assist in addressing complexities and finding the right answers.

Will the ICO be producing more specific guidance on what I need to do in future?

We will be keeping the situation under review and will consider issuing more detailed advice if appropriate in future. In particular, we may supplement this advice with further examples of how to gain consent for particular types of cookies.

However, we do not intend to issue prescriptive lists on how to comply. You are best placed to work out how to get information to your users, what they will understand and how they would like to show that they consent to what you intend to do. What is clear is that the more directly the use of a cookie or similar technology relates to the user's personal information, the more carefully you need to think about how you get consent.

We are keen to ensure any future guidance we produce in this area reflects real world practice and that it can continue to be used as technologies develop.