Privacy and Electronic Communications Regulations

Guidance on the rules on use of cookies and similar technologies

ico.
Information Commissioner's Office

Information Commissioner's Office

Contents

Introduction

The Privacy and Electronic Communications (EC Directive) Regulations 2003 (the Regulations) cover the use of cookies and similar technologies for storing information, and accessing information stored, on a user's equipment such as their computer or mobile.

A cookie is a small file, typically of letters and numbers, downloaded on to a device when the user accesses certain websites. Cookies are then sent back to originating website on each subsequent visit. Cookies are useful because they allow a website to recognise a user's device. The Regulations apply to cookies and also to similar technologies for storing information. This could include, for example, Local Shared Objects.

The use of cookies and similar technologies has for some time been commonplace and cookies in particular are important in the provision of many online services. Using such technologies is not, therefore, prohibited by the Regulations but they do require that people are told about cookies and given the choice as to which of their online activities are monitored in this way.

This guidance will explain how the rules apply for those operating websites and using cookies. The guidance uses the term 'cookies' to refer to cookies and similar technologies covered by the Regulations.

Background

The 2003 Regulations implemented a European Directive - 2002/58/EC - which is concerned with the protection of privacy in the electronic communications sector. In 2009 this Directive was amended by Directive 2009/136/EC. This included a change to Article 5(3) of the E-Privacy Directive requiring consent for storage or access to information stored on a subscriber or users terminal equipment – in other words a requirement to obtain consent for cookies and similar technologies.

Governments in Europe had until 25 May 2011 to implement these changes into their own law. The UK introduced the amendments on 25 May 2011 through The Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011.

The rules in this area are essentially designed to protect the privacy of internet users – even where the information being collected about them is not directly personally identifiable. The changes to the Directive in 2009 were prompted in part by concerns about online tracking of individuals and the use of spyware. These are not rules designed to restrict the use of particular technologies as such, they are intended to prevent information being stored on people's computers, and used to recognise them via the device they are using, without their knowledge and agreement.

Consumer understanding of cookies

A clear understanding of users' levels of awareness of what cookies are, what they are used for and how they can be managed, is fundamental to any consideration of the level of detail that needs to be provided about cookies, and the way in which the requirement to obtain consent can be satisfied.

Research into consumers' understanding of the internet and cookies demonstrates that current levels of awareness of the way cookies are used and the options available to manage them is limited. The Department for Culture, Media and Sport commissioned PricewaterhouseCoopers LLP (PWC) to conduct research into the potential impact of cookies regulation[1]. PWC conducted an online survey of over 1000 individuals in February 2011. Despite the report acknowledging that the most intensive internet users are overrepresented in the sample, the results illustrate that significant percentages of these more 'internet savvy' consumers have limited understanding of cookies and how to manage them:

- 41% of those surveyed were unaware of any of the different types of cookies (first party, third party, Flash / Local Storage). Only 50% were aware of first party cookies.
- Only 13% of respondents indicated that they fully understood how cookies work, 37% had heard of internet cookies but did not understand how they work and 2% of people had not heard of internet cookies before participating in the survey.
- 37% said they did not know how to manage cookies on their computer.
- The survey tested respondents' knowledge of cookies, asking them to confirm if a number of statements about cookies were correct or not. Out of the sixteen statements only one was answered correctly by the majority of respondents.

Those who use the internet less regularly, or have a generally lower level of technical awareness, are even less likely to understand the way cookies work and how to manage them. The report concluded that 'broader consumer education about basic online privacy fundamentals could go a long way toward making users feel more comfortable online and also enable them to take more control of their privacy while online' and that 'online businesses will need to evolve their data collection and usage transparency in order to illustrate to consumers the benefits of opting-in.'

Implementing the rules

Implementing these rules requires considerable work in the short term but compliance will get significantly easier with time. The initial effort is where the

[1] http://www.culture.gov.uk/images/consultations/PwC_Internet_Cookies_final.pdf

challenge lies - auditing of cookies, resolving problems with reliance on cookies built into existing systems and websites, making sure the information provided to users is clear and putting in place specific measures to obtain consent. This work takes place in the context of limited consumer awareness and understanding of what cookies do. In time a number of factors are likely to make compliance much more straightforward. New sites and systems and upgrades to existing systems can be designed to facilitate compliance with the rules, those operating websites will be more aware about how they choose to use cookies and enhanced browser options will increasingly allow websites to rely on browser settings to help to satisfy themselves they have consent to set cookies. Most importantly user awareness will be likely to increase as people become used to being prompted to read about cookies and make choices. A variety of consumer initiatives - such as the use of icons to highlight specific uses of cookies will also help in this area.

Work undertaken now will make future compliance much more straightforward. Website operators and their partner organisations need to be confident that their users have a general level of understanding about what is likely to happen on the pages they use. This can only be achieved by implementing changes as soon as it is practical to do so. Some of these changes might be small but can be implemented quickly as part of a more complex long term plan for compliance.

If websites are open and honest about how they work, if the mechanisms for exercising user choices are integrated into the presentation and user experience of the site, the users will be more confident about using the site and more comfortable with how websites collect and use information derived from their online behaviour.

Terminology and definitions

The Regulations apply to cookies and also to similar technologies for storing information. This could include, for example, Local Shared Objects (commonly referred to as "Flash Cookies"), web beacons or bugs (including transparent or clear gifs).

A cookie is a small file, typically 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.

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

Session and persistent cookies

Cookies can expire at the end of a browser session (from when a user opens the browser window to when they exit the browser) or they can be stored for longer. The Regulations apply to both types of cookies:

- **Session cookies** – allow websites to link the actions of a user during a browser session. They may be used for a variety of purposes such as

remembering what a user has put in their shopping basket as they browse around a site. They could also be used for security when a user is accessing internet banking or to facilitate use of webmail. These session cookies expire after a browser session so would not be stored longer term. For this reason session cookies may sometimes be considered less privacy intrusive than persistent cookies.

- **Persistent cookies** – are stored on a users' device in between browser sessions which allows the preferences or actions of the user across a site (or in some cases across different websites) to be remembered. Persistent cookies may be used for a variety of purposes including remembering users' preferences and choices when using a site or to target advertising.

- **First and third party cookies** – Whether a cookie is 'first' or 'third' party refers to the website or domain placing the cookie. First party cookies in basic terms are cookies set by a website visited by the user - the website displayed in the URL window. Third party cookies are cookies that are set by a domain other than the one being visited by the user. If a user visits a website and a separate company sets a cookie through that website this would be a third party cookie.

Subscriber

This means a person who is a party to a contract with a provider of public electronic communications services for the supply of such services. In this context the person who pays the bill for the internet connection (that is, the person legally responsible for the charges)

User

This means any individual using a public electronic communications service. In this context a user would be the person sat at a computer or using a mobile device to browse the internet.

Terminal equipment

The device a cookie is placed on – usually a computer or mobile device

Consent

The Regulations require that users or subscribers consent. Directive 95/46/EC (the Data Protection Directive on which the UK Data Protection Act 1998 (the DPA) is based) defines 'the data subject's consent' as:

'any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed'.

Consent must involve some form of communication where the individual knowingly indicates their acceptance. This may involve clicking an icon, sending

an email or subscribing to a service. The crucial consideration is that the individual must fully understand that by the action in question they will be giving consent.

'Prior' consent

It has been suggested that the fact the Regulations do not specifically refer to 'prior' consent suggests that consent can be obtained after the activity consent is needed for has occurred (in this instance after the cookie has been set).

It is difficult to see that a good argument could be made that agreement to an action could be obtained after the activity the agreement is needed for has already occurred. This is not the generally accepted way in which consent works in other areas, and is not what users will expect. Setting cookies before users have had the opportunity to look at the information provided about cookies, and make a choice about those cookies, is likely to lead to compliance problems. The Information Commissioner does however recognise that currently many websites set cookies as soon as a user accesses the site. This makes obtaining consent before the cookie is set difficult. Wherever possible the setting of cookies should be delayed until users have had the opportunity to understand what cookies are being used and make their choice. Where this is not possible at present websites should be able to demonstrate that they are doing as much as possible to reduce the amount of time before the user receives information about cookies and is provided with options. A key point here is ensuring that the information you provide is not just clear and comprehensive but also readily available.

You should also consider whether users who might make a one-off visit to your site would have a persistent cookie set on their device. If this is the case, you could mitigate any risk that they would object to this by shortening the lifespan of these cookies or, where possible given the purpose for using them, making them session cookies.

Implied consent as a basis for compliance with the Privacy and Electronic Communications Regulations.

Much of the debate around the so-called "consent for cookies" rule has focussed on the nature of the consent required for compliance. Implied consent has always been a reasonable proposition in the context of data protection law and privacy regulation and it remains so in the context of storage of information or access to information using cookies and similar devices. While explicit consent might allow for regulatory certainty and might be the most appropriate way to comply in some circumstances this does not mean that implied consent cannot be compliant. Website operators need to remember that where their activities result in the collection of sensitive personal data such as information about an identifiable individual's health then data protection law might require them to obtain explicit consent.

Early reporting on the new rule led some to believe that an explicit, opt-in style consent would be required for every cookie each time it was set. The

Information Commissioner's guidance made it clear that although an explicit opt-in mechanism might provide regulatory certainty it was not the only means of gaining consent. In some circumstances those seeking consent might consider implied consent as an option that was perhaps more practical than the explicit opt-in model.

Implied consent is certainly a valid form of consent but those who seek to rely on it should not see it as an easy way out or use the term as a euphemism for "doing nothing". In many cases, to create a situation in which implied consent is acceptable to subscribers, users and the regulator it would still be necessary to follow the steps set out in the Information Commissioner's existing guidance.

To explain further it might be useful to unpack what we actually mean by the term "implied consent" remembering throughout that consent (whether it is implied or express) has to be a freely given, specific and informed indication of the individual's wishes. For implied consent to work there has to be some action taken by the consenting individual from which their consent can be inferred. This might for example be visiting a website, moving from one page to another or clicking on a particular button. The key point, however, is that when taking this action the individual has to have a reasonable understanding that by doing so they are agreeing to cookies being set.

1. "Specific and informed"

It has been suggested that the fact that a visitor has arrived at a webpage should be sufficient evidence that they consent to cookies being set or information being accessed on their device. The key here is that the visitor should understand that this is the case. It is important to note that it would be extremely difficult to demonstrate compliance simply by showing that a user visited a particular site or was served a particular advertisement unless it could also be demonstrated that they were aware this would result in cookies being set.

In compliance terms this difficulty arises because although the person setting the cookie may think that there is an inference of consent, without information being given to the user, it is unlikely that they will understand that they are giving any sort of agreement. This remains the case if information is provided to the user but only as part of a privacy notice that is hard to find, difficult to understand or rarely read. This is why the "do nothing" approach is not enough. The understanding is all on the website operator's side and the user "giving" consent is unaware that their actions are being interpreted in this way. The user is not informed so in the context of the Regulations, this is not valid consent.

Many users will have some general notion that websites and third parties will collect information about how sites are used but it is difficult to take these rather vague notions and assume that all users will have sufficient knowledge to allow the person setting the cookie to infer consent simply because the user's browser requested the content or the user searched for the service.

By analogy, if a patient visits a doctor this act alone would not be taken as indication that the patient consents to examination, treatment or the recording of health information. The patient and doctor would hold a conversation during which the doctor might offer an invitation to the patient to lie down on an examination couch. In the context of this exchange the doctor might now be able to infer consent from the patient's actions based on the fact that there is a shared understanding of what is happening.

To rely on implied consent for cookies, then, it is important that the person seeking consent can satisfy themselves that the user's actions are not only an explicit request for content or services but also an indirect expression of the user's agreement that in addition to providing such content or services the provider may store or access information on the user's device.

To be confident in this regard the provider must ensure that clear and relevant information is readily available to users explaining what is likely to happen while the user is accessing the site and what choices the user has in terms of controlling what happens. Exactly how this information is provided is a matter for the person seeking consent and it is not the Information Commissioner's role to provide precise wording or impose particular methods of communication. Certainly, the existing guidance does contain some examples of how this information might be provided to users but these should be seen as suggestions on how to reach a desired outcome rather than prescriptive and exclusive lists of compliant activity.

Important factors to bear in mind might include:

- The nature of the intended audience of the site. Some sites might be aimed at an audience who are technically aware enough to have a reasonable understanding of what is going on. These sites would not necessarily need to provide very basic information about what cookies are but they might still want to give their users detailed explanation of how the site uses cookies and similar technology.

- The way in which users expect to receive information from and on the site. The more the information about cookies fits with the rest of the site the more likely users are to read it and, in turn, the more likely the website operator is able to assume that users understand and accept how the site works.

- Making sure that the language used is appropriate for the audience. Website operators are not expected to teach users exactly how the internet and World Wide Web work and it would be counterproductive to bombard the uninitiated with unnecessary levels of detail in highly technical language. For further advice on what to say and how to say it, see the advice provided by the International Chambers of Commerce.

Whatever the context in which cookies are being set it is helpful to see implied consent as coming out of a shared understanding between websites and users. The more users see prominent notices giving clear and relevant information

about cookies, the more they will develop an understanding about cookie use. Sites will then be able to assume that users have some basic understanding and will therefore know that some actions will have specific consequences in relation to the setting of cookies.

2. "An indication of wishes"

Where consent is required in the offline world individuals can do this in a number of ways. It can be given orally, in writing or it might be implied via the taking of a particular course of action which, although it is not an explicit statement of consent or agreement, makes the individual's wishes known. How far a course of action can indicate the individual's wishes will depend to a large extent on the context in which the action is taken.

To return to a medical analogy, in everyday life and taken in isolation, the rolling up of a sleeve might not signify a great deal; in the doctor's surgery, in the context of the doctor-patient relationship and in the light of information received and given by both parties, the rolling up of a sleeve might constitute an action which implies the patient's consent to having their blood pressure taken. A range of factors starting with the environment in which the action is taken and including the provision of information have allowed the doctor to infer consent.

In the context of cookies, similar consent might be inferred from a series of user actions which do not in isolation constitute a direct expression of the user's thoughts about cookies – they have not, in effect, ticked a box accepting cookies – but which in context act as a strong enough indication that they agree to cookies being set.

User actions can only give a strong enough indication if there is a shared understanding of what is happening. An example might be that the user is given a clear and unavoidable notice that cookies will be used and on that basis decides to click through and continue to use the site. Without such a clear notice it is difficult for the person seeking consent to interpret the user's actions as being any meaningful indication that the user was happy for cookies to be set. This is why the Information Commissioner has been keen to stress the importance of providing more and better information to users about cookies.

This is especially important with regard to commonly used features such as web analytics. It is clearly the case that the majority of websites undertake some form of analytics activity and most of those will use cookies to facilitate some if not all of that activity. The Information Commissioner recognises that gaining explicit opt-in consent for analytics cookies is difficult and that implied consent might be the most practical and user-friendly option. In light of this, website operators, developers and analytics vendors need to recognise that while analytics are, for them, an integral and entirely ordinary part of how the web has developed, for users the picture is rather less clear.

While many users might know enough to suppose that websites must make some use of statistics generated by their users it is unlikely that the majority of

those users would make the link between this supposition and the cookies being set on their device. Put simply, there is a gap between the range and complexity of the practices employed to provide, maintain and improve online services and the level of understanding users have about those practices. In particular, users are unaware of how much depends on their device and their activity being used to facilitate the provision of online services. The key to the validity of implied consent in this context is the narrowing of this gap. The more it becomes second nature for users to appreciate that on most sites they visit certain things are more likely than not going to happen then the more it will become acceptable for their actions – setting their browser up in a particular way, using the site in a particular way – to be interpreted as an indication that they understand what is happening and, by extension, that they consent to cookies. Alongside this of course should be the facility for users to make choices about whether and the extent to which their device is used to store and read cookies and information to support those choices. Whether those choices are at browser level or site specific it must always be possible for the user to decline to accept cookies even if it means a site's functionality is limited for the user as a result.

Consent from the user or subscriber

The Regulations state that consent for a cookie should be obtained from the subscriber or user. The subscriber means the person who pays the bill for the use of the line. The user is the person using the computer or other device to access a website.

In practice the owner of a website may well not be able to distinguish between consent provided by the subscriber or the user. The key then is that valid consent has been provided by one of the parties.

The Regulations do not specify whose wishes should take precedence if they are different. Other references in the legislation to a subscriber's ability to make decisions in this area, such as around browser settings, might suggest the subscriber's indications may in the first instance take priority. There may well be cases where a subscriber, for example, an employer, provides an employee with a terminal at work along with access to certain services to carry out a particular task, where to effectively complete the task depends on using a cookie type device. In these cases, it would not seem unreasonable for the employer's wishes to take precedence. There are other areas of the legislation, around browser settings where the subscriber clearly has the ability to make a decision on behalf of any users. However, there will be circumstances where a user's wish should take precedence. To continue the above example, an employer's wish to accept such a device should not take precedence where this will involve the unwarranted collection of personal data of that employee.

In a domestic context there will usually be a subscriber (the person in the household paying the bill) and potentially several other users. If a user complained that a website they visited was setting cookies without their consent the website could demonstrate they had complied with the Regulations if they

could show that consent had previously been obtained from the subscriber. The key to resolving problems in practice is to ensure information about cookies and mechanisms for making choices are as easily accessible as possible.

The Law

This is what the law requires:

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.

Regulation 6 of the Privacy and Electronic Communications Regulations 2003 (PECR)

Those setting cookies must:

- **tell people that the cookies are there,**
- **explain what the cookies are doing, and**
- **obtain their consent to store a cookie on their device.**

Since 2003 anyone using cookies has been required to provide clear information about those cookies. In May 2011 the existing rules were amended. Under the revised Regulations the requirement is not just to provide clear information about the cookies but also to obtain consent from users or subscribers to store a cookie on their device.

	2003 rule	2011 rule
Requirement to provide information	You must provide clear and comprehensive information about any cookies you are using	You must provide clear and comprehensive information about any cookies you are using

Requirement to provide choice	You must provide the option for people to opt out of cookies being stored on their devices	You must obtain consent to store a cookie on a user or subscribers device

Exceptions from the requirement to provide information and obtain consent

There is an exception to the requirement to provide information about cookies and obtain consent where the use of the cookie is:

(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.

In defining an 'information society service' the Electronic Commerce (EC Directive) Regulations 2002 refer to 'any service normally provided for remuneration, at a distance, by means of electronic equipment for the processing (including digital compression) and storage of data, and at the individual request of a recipient of a service'.

The term 'strictly necessary' means that such storage of or access to information should be essential, rather than reasonably necessary, for this exemption to apply. However, it will also be restricted to what is essential to provide the service requested by the user, rather than what might be essential for any other uses the service provider might wish to make of that data. It will also include what is required to comply with any other legislation the person using the cookie might be subject to, for example, the security requirements of the seventh data protection principle.

Where the setting of a cookie is deemed 'important' rather than 'strictly necessary', those collecting the information are still obliged to provide information about the device to the potential service recipient and obtain consent.

This exception is likely to apply, for example, to a cookie used to ensure that when a user of a site has chosen the goods they wish to buy and clicks the 'add to basket' or 'proceed to checkout' button, the site 'remembers' what they chose on a previous page. This cookie is strictly necessary to provide the service the

user requests (taking the purchase they want to make to the checkout) and so the exception would apply and no consent would be required.

The Information Commissioner is aware that there has been discussion in Europe about the scope of this exception. The argument has been made in some areas that cookies that are used for resource planning, capacity planning and the operation of the website, for example, could come within the scope of the exemption. The difficulty with this argument is that it could equally be made for advertising and marketing cookies (whose activities help to fund websites). The intention of the legislation was clearly that this exemption is a narrow one and the Commissioner intends to continue to take the approach he has outlined clearly in published guidance since the 2003 Regulations were introduced.

Activities likely to fall within the exception	**Activities unlikely to fall within the exception**
A cookie used to remember the goods a user wishes to buy when they proceed to the checkout or add goods to their shopping basket	Cookies used for analytical purposes to count the number of unique visits to a website for example
Certain cookies providing security that is essential to comply with the security requirements of the seventh data protection principle for an activity the user has requested – for example in connection with online banking services	First and third party advertising cookies
Some cookies help ensure that the content of your page loads quickly and effectively by distributing the workload across numerous computers.	Cookies used to recognise a user when they return to a website so that the greeting they receive can be tailored

Responsibility for compliance

The Regulations do not define who should be responsible for complying with the requirement to provide information about cookies and obtain consent. Where a person operates an online service and any use of cookies will be for their purposes, it is clear that that person will be responsible for complying with this Regulation.

The person setting the cookie is therefore primarily responsible for compliance with the requirements of the law. Where third party cookies are set through a website both parties will have a responsibility for ensuring users are clearly informed about cookies and for obtaining consent. In practice it is obviously considerably more difficult for a third party who has no direct interface with the user to achieve this. It is also important to remember that users are likely to

address any concerns or complaints they have to the person they can identify or have the relationship with – the company running the website. It is therefore in both parties' interests to work together.

The key point is not who obtains the consent but that valid, well informed consent is obtained.

Third parties setting cookies, or providing a product that requires the setting of cookies, may wish to consider putting a contractual obligation into agreements with web publishers to satisfy themselves that appropriate steps will be taken to provide information about the third party cookies and obtain consent.

Companies who design and develop websites or other technologies for other people, must also carefully consider the requirements of these Regulations and make sure the systems they design allow their clients to comply with the law. The Information Commissioner would expect that any development of new software, or upgrades to existing software, would take into account the need to ensure products are compliant with these rules and broader data protection requirements. Privacy by Design is an approach whereby privacy and data protection compliance is designed into systems right from the start, rather than being bolted on afterwards or ignored. For more information on privacy by design see our website www.ico.org.uk.

An organisation based in the UK is likely to be subject to the requirements of the Regulations even if their website is technically hosted overseas. Organisations based outside of Europe with websites designed for the European market, or providing products or services to customers in Europe, should consider that their users in the UK and Europe will clearly expect information and choices about cookies to be provided.

Browser settings

Both the Directive on which the Regulations are based, and the Regulations themselves, suggest browser settings may be one means of obtaining consent if they can be used in a way that allows the subscriber to indicate their agreement to cookies being set.

> '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.'

In other words, if the user visits a website, the website 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 can be confident that in setting A, B and C they have the users consent to do so. They would not set cookie D.

At present, most browser settings are not sophisticated enough for websites to assume that consent has been given to allow the site to set a cookie. For consent to be clearly signified by the browser settings it would need to be clear that subscribers had been prompted to consider their current browser settings and, had either indicated in some way they were happy with the default, or have made the decision to change the settings. The other difficulty is that not everyone accessing websites will do so with a traditional web browser.

Government is working with the major browser manufacturers to establish which browser level solutions will be available and when. In future many websites may well be able to rely on the user's browser settings as part, or all, of the mechanism for satisfying themselves of consent to set cookies. For now relying solely on browser settings will not be sufficient and even when browser options are improved it is likely not all website visitors will instantly have the most up-to-date browser with these enhanced privacy settings.

Practical advice for those wishing to comply

The Information Commissioner wants to provide as much flexibility as possible for organisations to design solutions that meet their business needs and provide users with the choices they require.

It is not enough simply to continue to comply with the 2003 requirement to tell users about cookies and allow them to opt out. The law has changed and whatever solution an organisation implements has to do more than comply with the previous requirements in this area.

First steps

If you have not started work on complying with these rules it is important to do so now. First steps should be to:

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. Where you need consent - 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

You should already know what cookies you are using but it would be sensible to recheck that at this point. 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 web pages

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

Although the law makes no distinction between different types of cookie it is intended to add to the level of protection afforded to the privacy of internet users. Therefore it follows 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.

The Information Commissioner recognises that 'how intrusive' an activity will depend to an extent on the view taken by the user so it can be difficult to judge. This difficulty, however, should not be a barrier to making a sensible judgement about which of your activities might cause users concern and which will not.

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.

Conducting a cookies audit

An audit of cookies could involve the following steps and considerations:

- Identify which cookies are operating on or through your website
- Confirm the purpose(s) of each of these cookies
- Confirm whether you link cookies to other information held about users - such as usernames

- Identify what data each cookie holds
- Confirm the type of cookie – session or persistent
- If it is a persistent cookie how long is its lifespan?
- Is it a first or third party cookie? If it is a third party cookie who is setting it?
- Double check that your privacy policy provides accurate and clear information about each cookie

Providing information about cookies

The Regulations are not prescriptive about the sort of information that should be provided, but the text should be sufficiently full and intelligible to allow individuals to clearly understand the potential consequences of allowing the cookies should they wish to do so. This is comparable with the transparency requirements of the first data protection principle. At present, levels of user understanding are likely to be low and so those using cookies will need to make a particular effort to explain the activities of cookies in a way that people will understand.

Long tables or detailed lists of all the cookies operating on the site may be the type of information that some users will want to consider. For most users it may be helpful to provide a broader explanation of the way cookies operate and the categories of cookies that you use on your website. A description of the types of things analytical cookies are used for on the site will be more likely to satisfy the requirements than simply listing all the cookies you use with basic references to their function.

For example

Our website uses four cookies. A cookie is a small file of letters and numbers that we put on your computer if you agree. These cookies allow us to distinguish you from other users of the website which helps us to provide you with a good experience when you browse our website and also allows us to improve our site.

The cookies we use are 'analytical' cookies. They allow us to recognise and count the number of visitors and to see how visitors move around the site when they're using it. This helps us to improve the way our website works, for example by making sure users are finding what they need easily. Read more about the individual analytical cookies we use and how to recognise them [link]

At present information about cookies is generally provided in a privacy policy accessed through a link at the bottom of a webpage. Making sure users will see clear information about cookies is important for compliance with the information requirements of the Regulations, to ensure that consent is valid and more broadly to increase levels of user awareness. Possible ways of making information about cookies more prominent include:

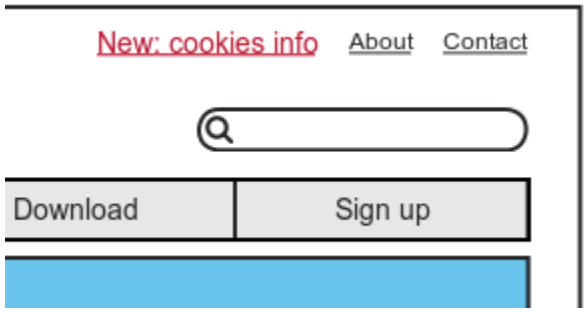
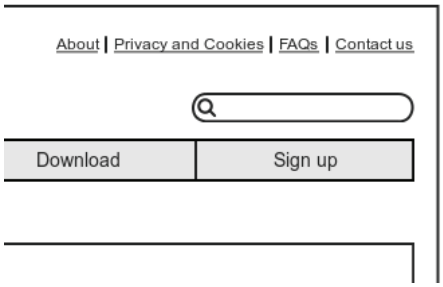


Figure 1: Highlighting cookies information

Other methods of increasing the prominence of cookies information:

- Simple formatting can help - this might include changing the size of the link to the information or using a different font. The key is whether the link to this important information is distinguishable from "normal text" and other links.



- Positioning is important – simply moving the link from the footer of the page to somewhere more likely to catch attention is an easy but effective thing to try.

- Making the hyperlink more than simply "privacy policy" : this could involve a link through some explanatory text ("Find out more about how our site works and how we put you in control")

You might consider other techniques such as mouse over highlights that make the link stand out as being important or using a clickable image or icon to encourage people to seek more information. Many organisations use features such as blogposts or news headlines to draw attention to certain content so you could do this in relation to explaining how the site works. Clearly, this is not a permanent feature but could increase your confidence that regular users have seen the relevant information.

These examples are all straightforward and easy to implement suggestions. They are not intended to be complex techniques that will solve everything. They are included in this advice to illustrate that there are 'quick wins' to be had that will increase the likelihood that users see your information about cookies.

Getting consent in practice

Which method will be appropriate to get consent for cookies will depend in the first instance on what the cookies you use are doing and to some extent on the relationship you have with users.

When considering how to provide information about cookies and how to obtain consent it may be helpful to look at the methods most websites already use to draw users' attention to information or choices they want to highlight.

Many websites make use of different techniques to highlight things they want users to see, such as promotions, special offers, or customer satisfaction surveys. Websites also commonly obtain agreement or consent from individuals in other contexts, such as verification of minimum age requirements, changes in terms and conditions and to double check whether customers definitely want to proceed with a purchase. Providing users with information and obtaining their agreement is not a new feature of the internet. The approach you take for cookies can build on these existing mechanisms.

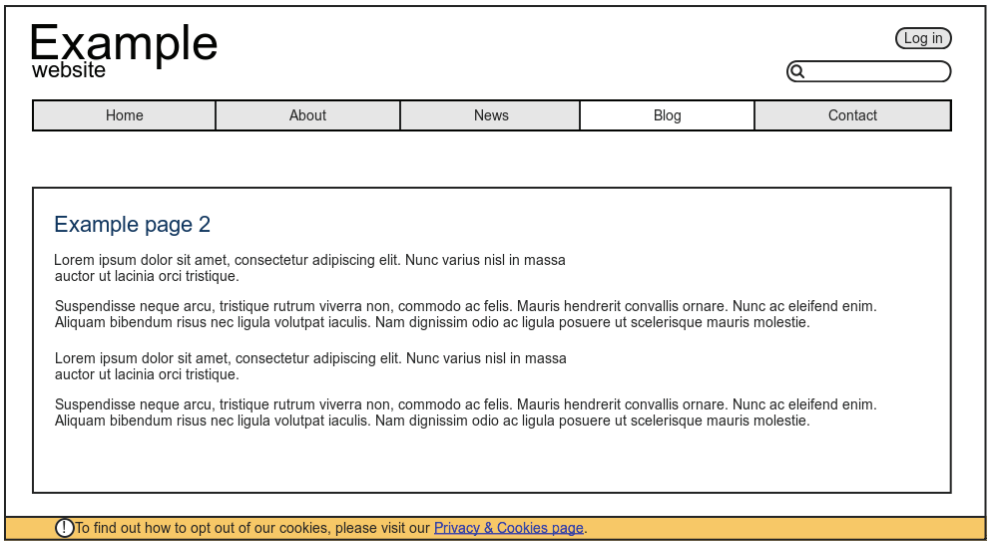
Pop ups and similar techniques

Pop-ups or similar techniques such as message bars or header bars 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 not implemented carefully.

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 highlighting the use of cookies and obtaining consent.

Figure 2: Website with header bar

Using this technique you could ensure you are compliant by not switching on any cookies unless the person clicks I agree. Some users might not click on either of the options available and go straight through to another part of the site. If they do, you might decide that you could set a cookie and infer consent from the fact that the user has seen a clear notice and actively indicated that they are comfortable with cookies by clicking through and using the site. This is an option that relies on the user being aware that the consequence of using the site is the setting of cookies. If you choose this option you might want the reassurance of a notice appearing elsewhere on the site which reminds users that you are setting cookies.



Terms and conditions

It is not uncommon for consent to be gained online using the terms of use or terms and conditions to which the user agrees when they 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. There is no reason why consent for the 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. Consent has to be specific and informed. To satisfy the 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.

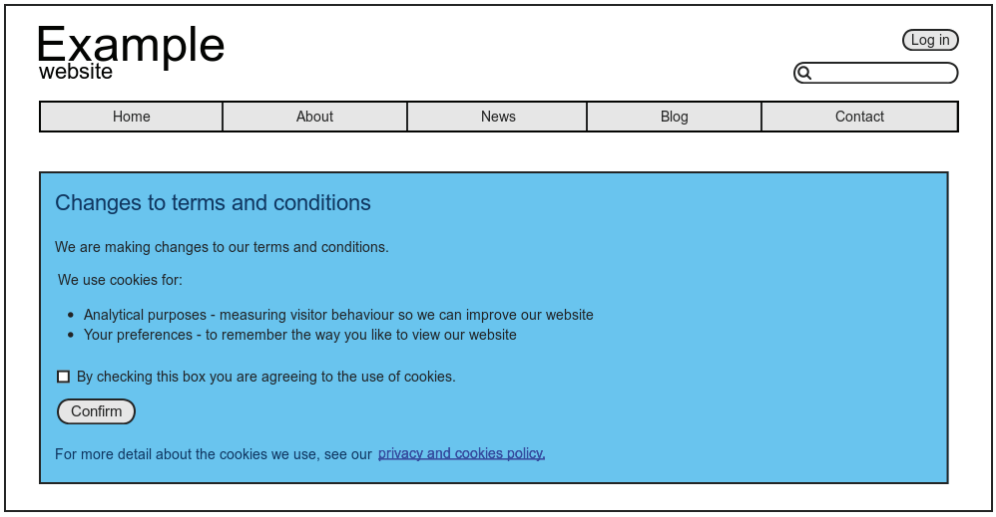


Figure 3: Cookies consent through terms and conditions

1. 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 a 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. Agreement for the cookie could therefore be seamlessly integrated with the choice the user is already making.

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.

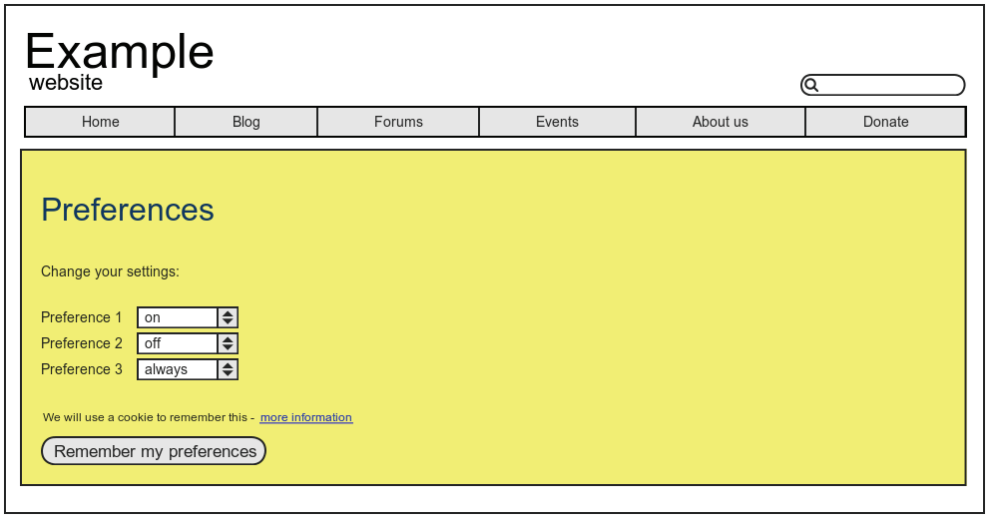


Figure 4: Consent to use cookies to remember preferences

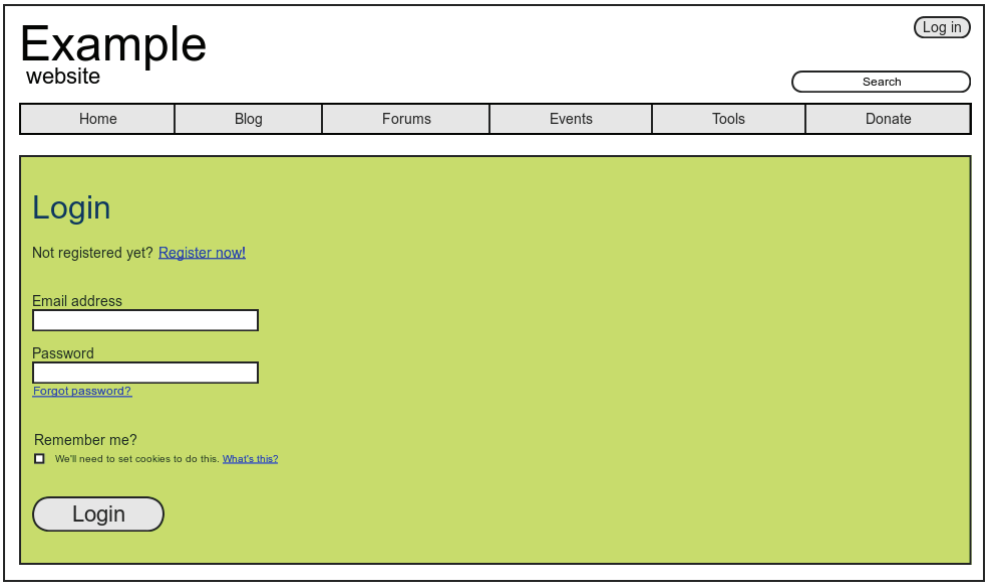


Figure 5: Using cookies to remember preferences

2. 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 and analytical uses

You will often collect information about how people access and use your site. This work is often done 'in the background' and not at the request of the user. A first party 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. You must also think about giving people more details about what you do so that users can make an informed choice about what they will allow.

Where a user logs into a website, or chooses to download a particular service that uses cookies, it should be relatively straightforward to put in place a mechanism to obtain consent for analytical and functional cookies at the point

the user logs in. Clear information about the activities of these cookies can be provided and the user can be prompted to make a specific and informed choice before logging on to signify their agreement.

It is likely to be more difficult to obtain consent for this type of cookie where you do not have any direct relationship with a user – for example where users just visit a site to browse. In this case websites should ensure the information they provide to users about cookies in this area is absolutely clear and is highlighted in a prominent place (not just included through a general privacy policy link). As far as possible measures should be put in place to highlight the use of cookies and to try to obtain agreement to set these cookies. There are various ways in which information about cookies can be — see Providing information about cookies.

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 is one of the most challenging areas in which to achieve compliance with the rules. The Information Commissioner continues to work with industry and other European data protection authorities to assist in addressing complexities and finding the right answers.

Possible mechanisms for gaining consent

Relationship with user or subscriber	Type of cookie	Possible mechanisms for gaining consent
Registered user of online	First party analytical	Highlighting the cookies

banking services	cookies (session) and first party cookies used to tailor advertising on log in pages (persistent)	and asking for consent from the user as they log into their account. Once this consent is obtained the option will not have to be provided on subsequent visits.
Occasional visitor to an online magazine	Cookie to remember and tailor preferences for viewing and set up of the site (persistent)	The mechanism for the user to select or tailor their preferences 'Would you like us to remember your…' is amended to specifically flag that this process involves agreeing to a cookie. If the user selects the option to request that their preferences are remembered – having clearly had highlighted the role of the cookie in that process – the consent requirements would be satisfied.
User wanting to download a game or application	First party cookie used to personalise the gaming experience (persistent)	In most cases the user will already be agreeing to terms and conditions to download the game or app. The way in which cookies are used is clearly and specifically highlighted in a prominent place in the process of agreement to these conditions (for example next to the 'I agree' box). Once this consent is obtained the option will not have to be provided each time the game is used.

In many cases a combination of solutions will be appropriate and different solutions will work in different contexts. In some cases a website may use a combination of factors to satisfy themselves an individual has consented, for example, the user has used an updated version of a browser that clearly allowed and prompted them to make appropriate choices about cookies, there is clear information about cookies prominently displayed on the webpage and the cookies being set are first party analytical cookies with a low level of intrusiveness.

Consent for cookies on more than one site

An organisation with several connected websites could in theory obtain consent for cookies set on each site in one place, for example when the user logged in on one site. In order for this consent to be valid it would have to be absolutely clear which websites the cookies in question were set on, what those cookies were used for and exactly what the user was agreeing to.

Changes to cookies use after consent has been obtained

Provided a valid consent has been obtained once it does not need to be obtained again each time a user visits. Clearly if the purposes of the cookies you use changes significantly after consent has been obtained you will need to make users aware of the changes and allow them to make the choice about those activities. Consent does not have to be gained separately for each individual cookie, provided you have explained the purpose of the cookies clearly a user could provide consent to cookies performing a set of functions.

Withdrawing consent for cookies

Once consent has been obtained users or subscribers may choose to withdraw that consent at any time. You should ensure you provide information about how consent can be withdrawn, and cookies that have already been set removed, in your privacy policy. You may wish to explain any consequences of withdrawing that consent, for example, impacts on the functionality of the website.

Alternatives to cookies and the broader privacy context

In some areas it is possible for functions usually performed by a cookie to be achieved through other means. This could include, for example, using certain characteristics to identify devices so that you can analyse visits to a website (this is sometimes known as 'device fingerprinting'). When considering alternatives to cookies it is important to look at the broader privacy context. Focusing solely on cookies is missing the point. Even where the clear cookies rules do not apply you must consider the DPA whenever you are collecting information that builds up a picture that could allow you to identify an individual. You should tell people what you are collecting and how you are using this information.

Cookies and personal data

Although the Regulations do not just apply where personal data is being processed activities involving processing of personal data give rise to greater privacy and security implications.

Where the setting of a cookie does involve the processing of personal data, those using them will need to make sure they comply with the additional requirements of the DPA.

Phased implementation

Prior to the introduction of the Regulations, government expressed the view that there should be a phased approach to the implementation of these changes. The Information Commissioner agreed that businesses would need time to implement solutions. He therefore confirmed that he would exercise his discretion and allow organisations a 'lead in' period of 12 months to put in place the measures needed to comply.

During this period the Information Commissioner has made clear he expects organisations to be taking steps to be in a position to comply with the rules. If he were to receive a complaint about a website during the 12 month lead in period, he would expect an organisation's response to set out a realistic plan to achieve compliance. See our statement on enforcing the revised Privacy and Electronic Communications Regulations for more information.

Enforcement and penalties

The Information Commissioner's aim is to ensure organisations comply with the law. In cases where organisations refuse or fail to comply voluntarily the Information Commissioner has a range of options to available to him to take formal action where this is necessary.

The main options are:

• **Information notice**: this requires organisations to provide the Information Commissioner with specified information within a certain time period.

• **Undertaking:** this commits an organisation to a particular course of action in order to improve its compliance.

• **Enforcement notice**: this compels an organisation to take the action specified in the notice to bring about compliance with the Regulations. For example, a notice may be served to compel an organisation to start gaining consent for cookies. Failure to comply with an enforcement notice can be a criminal offence.

• **Monetary penalty notice:** a monetary penalty notice requires an organisation to pay a monetary penalty of an amount determined by the ICO, up to a maximum of £500,000. This power can be used in the most serious of cases

and if specific criteria are met, if any person has seriously contravened the Regulations and if the contravention was of a kind likely to cause substantial damage or substantial distress. In addition the contravention must either have been deliberate or the person must have known or ought to have known that there was a risk that a contravention would occur and failed to take reasonable steps to prevent it.

More guidance on the circumstances in which the Information Commissioner will use this power, including what is considered a 'serious breach', can be found in the monetary penalties guidance: www.ico.org.uk

Enforcement of the cookies rules

The Information Commissioner will take a practical and proportionate approach to enforcing the rules on cookies. He has to enforce the law, but he does have some discretion in how he exercises his formal enforcement powers.

The options set out above are powers to enforce all the provisions of the Regulations (which also cover marketing by electronic means) they are not specific to the rules about cookies. The Information Commissioner made clear when the rules on cookies were introduced in May 2011 that he would be unlikely to take formal action against those who were taking steps to comply with the rules during a 12 month lead in period. At the end of this period in May 2012 the Information Commissioner will consider complaints about cookies in line with his normal approach to complaint handling under the Regulations. This will involve in most cases contacting the organisation responsible for setting the cookies in the first instance and asking them to respond to the complaint and explain what steps they have taken to comply with these rules.

Where formal action is considered, perhaps because an organisation refuses to take steps to comply or has been involved in a particularly privacy intrusive use of cookies without telling individuals or obtaining consent, any use of formal regulatory powers would be considered in line with the factors set out in the published Data Protection Regulatory Action Policy and Guidance on the issuing of monetary penalties: www.ico.org.uk

As the lead in period comes to an end organisations will need to be able to demonstrate they have taken sensible, measured action to move to compliance. If a website has not achieved full compliance at the end of the period the Information Commissioner will expect a specific and clear explanation of why it was not possible to comply in time, a clear timescale for when compliance will be achieved and details of specifically what work is being done to make that happen.

Where, for example, compliance is delayed because cookies are embedded in existing software (which would be expensive to upgrade) the Information Commissioner would expect these costs to be carefully weighed up against how intrusive the cookies in question are and how long it will be before the software

will be upgraded in any event. The Information Commissioner would expect this analysis to be available with clear timescales. He would not accept simply that a website cannot remove a cookie because it is too expensive, particularly where no other measures have been put in place to mitigate risks to users.

The Regulatory Action Strategy makes clear that any formal action must be a proportionate response to the issue it seeks to address and that monetary penalties will be reserved for the most serious of breaches of the Regulations meeting the criteria set out above. Although the Information Commissioner cannot completely exclude the possibility of formal action in any area, it is highly unlikely that priority for any formal action would be given to focusing on uses of cookies where there is a low level of intrusiveness and risk of harm to individuals, if an organisation can demonstrate they have done everything they can clearly to inform users about the cookies in question and to provide them clear details of how to make choices. Whilst he does not consider they are exempt from the rules the Commissioner is therefore unlikely to prioritise, for example, first party cookies used for analytical purposes and cookies that support the accessibility of sites and services, in any consideration of regulatory action.

Your questions answered

Will the Information Commissioner 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. 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 setting 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.

Can I wait for browser settings options to be changed?

No, as explained above this will take some time and it is not clear that even when the necessary changes are achieved you could rely on all users instantly using the most up to date version of any browser. Browser settings are part of the solution and you will increasingly be able to rely on these as part of the mechanism for satisfying yourself that you have a users consent to set cookies. For now, you will need to work on implementing another solution.

How do these rules apply to intranets?

In our view the rules do not apply in the same way to intranets. The Regulations require that consent is obtained from the user or subscriber. A 'user' is defined as any individual using a public electronic communications service. An intranet is unlikely to be a public electronic communications service. Although the

Regulations would not therefore apply in the same way to cookies that are set on an intranet it is important to remember that the requirements of the DPA are likely to apply if your use of cookies is for the purposes of monitoring performance at work, for example. Wherever an organisation collects personally identifiable information using cookies then the normal fairness requirements of the DPA will apply.

People say this law just isn't practical – what happens if I do nothing and wait for it all to go away?

This isn't going away. It's the law. The UK Regulations come from a European Directive that was passed in 2009. The requirements cannot easily be changed and cannot just be ignored. Many organisations are making a lot of effort to comply. The Information Commissioner has been clear that he will take a practical and proportionate approach to enforcing these rules where organisations are making the effort to comply.

Does the law apply in the same way for mobile devices?

Yes, the requirements apply to cookies set on mobile devices and other terminal equipment such as internet enabled televisions and games consoles.

Can I copy the Information Commissioner's solution?

The Information Commissioner's website www.ico.org.uk uses a banner that informs users about cookies and gives them the chance to consent. Whilst we have no objection to organisations seeing if this option would work for them any solution has to be appropriate to an organisation's own needs. We will review the use of the banner in future and may consider other options ourselves.

Nobody complains about cookies – why are you expecting people to spend lots of time complying with these rules?

Consumer research indicates that at this point in time individuals generally have a low understanding of what cookies are, how they work and how to exercise choice over those cookies. You cannot rely on the fact that people don't complain where levels of understanding of an activity are very low. One of the purposes of these rules is to increase individual's awareness and understanding so they can decide whether they object to cookies or not. Those who use cookies have a part to play in educating consumers and making the case to individuals with concerns about why cookies you want to use are beneficial.

We only use analytical cookies – if nobody consents that will seriously restrict the amount of information we can get to improve and develop our website

The Regulations do not distinguish between cookies used for analytical activities and those used for other purposes. We do not consider analytical cookies fall within the 'strictly necessary' exception criteria. This means in theory websites need to tell people about analytical cookies and gain their consent.

In practice we would expect you to provide clear information to users about analytical cookies and take what steps you can to seek their agreement. This is likely to involve making the argument to show users why these cookies are useful. Although the Information Commissioner cannot completely exclude the possibility of formal action in any area, it is highly unlikely that priority for any formal action would be given to focusing on uses of cookies where there is a low level of intrusiveness and risk of harm to individuals. Provided clear information is given about their activities we are highly unlikely to prioritise first party cookies used only for analytical purposes in any consideration of regulatory action.