Cookie Law Guidance Notes

1. Introduction

The current legal requirements for website cookies and similar technologies stem from the Privacy and Electronic Communications (EC Directive) Regulations 2003 and, as of 25 May 2018, from the European General Data Protection Regulation 2016 ("GDPR").

Privacy online is of great importance, all the more so in light of the GDPR which represents the single greatest step forward in privacy legislation since the Data Protection Act of 1998; a piece of legislation which was crafted before the advent (or at least the rise) of many forms of data collection and usage that are commonplace today, particularly online.

Privacy in general is also increasingly an important issue for internet users who are increasingly concerned that their data is being commodified largely without their permission or knowledge. This is not only important from a legal standpoint, but also from a business one. By complying with the law, not only is your business safe from penalties – particularly the tough ones introduced by the GDPR – but it is also likely to engender a greater degree of trust from its customers.

Central to the laws which govern cookies and similar technologies is the issue of consent. The law does not say that you cannot use cookies, trackers, beacons and so on. Rather, it requires that, in many cases, you must only do so with users' permission. Current common practice is to simply inform users that your website uses cookies with their continued use of the site being taken as consent. As will be seen below, this is no longer sufficient. Users must be properly informed, must be given a genuine choice, and must give some kind of explicit indication of their consent.

1.1 Cookies and Similar Technologies

While most guidance focuses on cookies (indeed, the laws governing such technologies are commonly collectively referred to as "cookie law") it is important to note that the law does not only govern cookies. A number of technologies may be used in a similar way, such as local shared objects (also known as "flash cookies"), web beacons, clear gifs, page tags, and web bugs. References to "cookies" in these Guidance Notes should be taken as also referring to these similar technologies. As technology develops quickly, the law could not keep up if it limited itself in scope to particular terms of art.

1.2 The Law's Purpose

Simply put, the law aims to protect the privacy of internet users. The GDPR extends this protection due to the far greater scope of its definition of "personal data". It may not be immediately obvious that a cookie or the data within it qualifies as personal data; however, where a cookie can identify an individual via their device, even if identification can only be made by combining the data in question with other data, it will fall within the definition. The rule of thumb we would suggest, then, is to err on the side of caution and treat all cookies and similar technologies in the same manner.

Those operating websites within the EU (even if the website itself or its operator/owner is based outside of the EU) are required by law to do the following:

1) Inform users about the purpose of the cookies that their website places and stores on users' computers or devices; and
2) Obtain users' consent before placing and storing those cookies.

1.3 Why Have This Law?

It is an inescapable truth that as regulations limiting the use of cookies and similar technologies get stricter, they become more of an impediment to business. Indeed, tougher consent requirements stand to negatively impact a number of things including behavioural advertising and the ability to track and analyse people's use of your website.

A reasonable question to ask is why the cookie controls built into internet browsers cannot be relied upon for consent. Users are, after all, free to block cookies using browser settings or, for the more technically aware, browser extensions. The problem with such settings, however, is that many users are unaware of them. Furthermore, not all browsers are created equal and the sophistication of cookie and privacy settings varies considerably, often not providing sufficient levels of control. A user might want to stop you from tracking their use of your website, for example, but not prevent their login details and shopping basket contents from being saved. Even a browser that allows users to pick from blocking third-party cookies or blocking all cookies would not provide sufficient control in this scenario of your tracking was done using first-party cookies.

Proposals are afoot to address this state of affairs and were originally planned to come into force alongside the GDPR on 25 May 2018; however, at the time of writing the legislation in question remains in draft form and is still working its way through the European Union legislative process. Of particular interest is a new requirement imposed on the makers of web browsers to incorporate better controls — controls that would, in theory, eliminate the need for the consent mechanisms outlined below — however, until the legislation is finalised and browser makers have been given sufficient time to implement improved controls, the burden remains on the operators of websites to obtain consent from users proactively.

2. What Do I Need to Do?

The answer to this question depends largely upon what cookies you use on your website and for what purpose or purposes. The most effective way of identifying cookies (and similar technologies, remember), their functions, and indeed their importance, is to conduct a thorough cookie audit. This may also provide a useful opportunity to re-evaluate your use of cookies and their real value to your business.

2.1 Know Your Cookies

Before we move on to lay out the steps of a cookie audit, it important that you understand the different types of cookie.

2.1.1 Strictly Necessary Cookies
A cookie falls into this category if it is essential to the operation of your website. Strictly necessary cookies may, for example, be required for functions such as logging in, storing items in a shopping basket, or enabling payment transactions.

2.1.2 Analytics Cookies
Understanding how users use your website can be extremely valuable. Analytics cookies provide insights into many factors such as how users are navigating around the site and what features they are using. Analytics cookies may often be set by third parties, but not always. To add to complications, however, even if analytics cookies are set by you, if the data collected by them is processed by a third party, they will be treated differently from a data protection perspective.

2.1.3 Functionality Cookies
Many websites offer some level of personalisation and functionality cookies play a key role here. For auditing purposes, however, it is important not to confuse these with the strictly necessary variety. If the site can be used properly without the cookie, it isn't strictly necessary.

2.1.4 Targeting Cookies
It is important to know when and how often someone visits your website, and which parts of it they have used (including which pages they have visited and which links they have followed). As with analytics cookies, targeting cookies allow you to better understand your users, enabling you to make your site and, more importantly, the advertising on it more relevant to those users' interests. Targeting cookies may often be set by third parties.

2.1.5 First-Party Cookies
As the name suggests, these cookies are placed directly by your website (as opposed to those placed by third-party services, for which see below). Most, if not all, of your strictly necessary and functionality cookies will likely be first-party cookies.

2.1.6 Third-Party Cookies
These cookies are placed by third parties providing services such as advertising and analytics. Analytics and targeting cookies are common types of third-party cookie as such work is often not undertaken in-house.

2.1.7 Persistent Cookies
Any of the cookies listed above may be a persistent cookie. Persistent cookies are those which remain active on a user's computer or device for a predetermined period of time and are activated when that user visits your website.

2.1.8 Session Cookies

Any of the cookies listed above may be a session cookie. Session cookies are temporary and only remain on a user's computer or device from the point at which they visit your website until the web browser is closed, at which point they are removed.

2.2 The Cookie Audit

A cookie audit will help you to identify the cookies that are used by your website, what those cookies are doing, what type of cookies they are, how long they remain on a user's computer or device, what personal data they collect, and whether or not they are being used in compliance with the law.

2.2.1 What Cookies Am I Using?

Begin by listing all of the cookies (yes, and similar technologies) currently used on your website. If you don't know what cookies you are using, your web developer should be able to provide a list. Alternatively, a number of tools – free and otherwise – are available online.

2.2.2 What Do My Cookies Do?

For each cookie in your list, make a note of what it is used for. It is important that you are clear about each cookie's function as this will assist in the next step.

2.2.3 What Types of Cookies Am I Using?

Going through the list again, identify what types of cookie are at work on your website. Refer back to the list above for guidance. Identify whether each cookie is first or third-party; whether it is a persistent or a session cookie; and whether it is strictly necessary, for analytics, functionality, or for targeting.

2.2.4 How Long Do My Persistent Cookies Last?

If you use persistent cookies, it is important to take note of their duration. Persistent cookies are considered to be more privacy-intrusive than session cookies, so for each one, consider whether its lifespan is truly necessary for the cookie's purpose and shorten that lifespan if it seems excessive.

2.2.5 What Data Do My Cookies Collect?

Not all cookies collect and store personal data, but some do and in light of the GDPR it is more likely now that data used by cookies will be defined as "personal data". In addition to the obvious – name, email address etc. – IP addresses and other seemingly anonymous identifiers qualify under the GDPR. As noted above, even an anonymised identifier that does not identify an individual on its own can count as personal data if it can be combined with other data and used to identify someone. If your cookies do use personal data, you will be processing personal data and must, as such, ensure that you comply with the requirements of the GDPR.

2.2.6 Are My Cookies Legal?

Keeping your own first-party cookies under control is important, and in addition to obtaining the correct consent to use them (see below), if any personal data is involved, it is crucial to comply fully with the GDPR. Moreover, if you use third-party cookies, while control over them rests (at least to a point) with the third party providing them, they are still being used on your website. It is therefore important to ensure that the third party or parties involved are also complying with the law.

2.3 Information and Consent

2.3.1 Informing Users

One of the most important principles of the GDPR focuses on transparency. Where personal data is concerned (and remember, this can include cookies), it is vital that individuals know what data you hold about them and what you are doing with it. It is only after being provided with such information that users can give you their informed consent.

It is a good idea to start with a clear, simple explanation of what cookies are and what they actually do. Many users will have heard of cookies, but they may not know a great deal about them. Consider, for example, including an explanation of the different cookie types similar to that included above in these Guidance Notes.

Even if you are only using *strictly necessary* cookies, it is important that users are fully informed about what you are doing. You may not need consent to place strictly necessary cookies, but that does not mean that you can avoid telling users about them. If you have reason to hide them, it is worth re-evaluating whether they are in fact *strictly necessary* after all. The general rule is, the more prominent your information, the better. Another general rule is to keep things simple; the average internet user does not possess a high degree of technical knowledge so using user-friendly, straightforward language in your cookie information is always advisable. Some websites tend to go a little overboard with friendly, fuzzy, humorous language, but this does have the benefit of downplaying the perception that cookies are little more than spyware rather than being the useful, innocuous little files that they (usually) really are.

Your cookie information should enable users to fully understand the functions of the various cookies placed by your website, what effect they will have on users, and in particular, what personal data is involved. In situations where cookies are used to provide useful information to you, such as analytics cookies, it may also be worth explaining how they benefit the user. Your explanation should be positive rather than negative. It is thus preferable to say something like:

> *"By seeing how you use our website using analytics cookies, we are better able to understand our customers and continually improve our services."*

as opposed to:

> *"If you do not accept our analytics cookies we will not be able to improve our services as we will be unable to track your movement and activity around our website."*

Put simply, tell your users why accepting your cookies is good for them, rather than why their refusal to accept them is bad for you.

Another useful element to include in your information is a table listing the cookies you use, what each one does, and what information it collects. Again, try to use user-friendly terminology as much as possible.

2.3.2 Where Should I Put My Information?

The key word here is “prominence”. Burying a brief mention of cookies in your privacy policy is not the best way to attract attention. That being said, the increased importance of transparency and consent under the GDPR also means that your privacy policy should be similarly prominent.

It is a good idea to bring cookies directly to first-time visitors’ attention, along with a request for consent to use cookies (where appropriate) and this is something we’ll go into in more detail below. Because your information and consent mechanisms (also see below for more information) should be presented together, it is important that it is available at all times. A prominent link on every page of your website, therefore, is the preferable route.

While it is a matter of taste to an extent, the separation of cookie information from your privacy policy is also important. Once again, the increased importance of consent and controls plays a part here. It is advisable to separate out your privacy policy and cookie information (or at least the links to them by linking directly to the cookie section of your privacy policy, for example). Not only does this help with prominence, but it also makes it easier for non-technical users to find what they are looking for.

2.3.3 Consent

Consent is one of the key features of the GDPR and an area in which stricter standards have been applied. Implied consent has, for quite some time, been a popular method of obtaining users’ permission to use cookies. A common method prior to the GDPR has been to provide users with information about cookies, informing them that their continued use of the website will be taken as consent to the use of those cookies. Controls have also been decidedly inconsistent.

This does not necessarily mean that users must be given control over every single cookie that you wish to use. Strictly necessary cookies are still acceptable. The GDPR itself in reality says very little about cookies and related technologies. The Privacy and Electronic Communications (EC Directive) Regulations 2003 are more focused on such matters, as is the forthcoming Regulation on Privacy and Electronic Communications (commonly referred to as the “ePrivacy Regulation”). It is important to note that, at the time of writing, the ePrivacy Regulation remains in draft form and is still being debated and amended by the various EU lawmaking bodies. It is intended to come into force at the same time as the GDPR (25 May 2018) however this is currently thought to be quite unlikely with some legal experts suggesting that it may not see the light of day until 2019. These Guidance Notes will be updated as more information becomes available. It is nevertheless helpful to be aware of the Regulation as it provides some insight, even as a draft, into what will and will not be acceptable in the future. Under the most recent draft available, if a cookie (or related technology) is “necessary for providing an information society service requested by the end-user” (i.e. your website or the service it provides), it is acceptable.

Can I Rely on Implied Consent?

Implied consent is no longer a sensible option in a GDPR world. Users must now take some affirmative action in order to indicate consent. Moreover, this must take place before any cookies are placed.

Can I Rely on Browser Settings?

This is a difficult question at present. The general advice has long been that relying solely on users’ browser settings is not a sensible idea. As has already been noted, many users do

not possess sufficient technical knowledge or awareness. This, therefore, makes relying on browser settings for genuine consent a highly flawed method.

There is nothing, of course, to stop you from providing additional advice to your users on adjusting their browser's privacy settings; however, reliance on those settings alone is not recommended.

This is a position that may change in the future under the aforementioned ePrivacy Regulation which is currently designed to impose new obligations on the makers of web browsers to the extent that, eventually, browser settings could be sufficient. It is very important, however, to note that this is not currently the law and that browser settings are not currently sufficient. Do not rely on them!

What About Affirmative Consent?

This, if it is not already clear by now, is by far the best way. It leaves no room for doubt, either on your part, on your users' part, or on the Information Commissioner's part, meaning that it is safest for everyone.

It is important that users are given a real choice. As has already been noted, it is no longer acceptable to simply tell users that by continuing to use your website, they are agreeing to accept your cookies. An important concept under the GDPR is known as "granular consent". In practice, this means giving users more finite control over what their data is used for. You are not expected to enable users to prevent your website from letting them log in, store items in an online shopping basket etc. but you are expected to allow them to be selective. If, for example, your website offers additional personalisation features that are not essential to its functionality, but still make for a better user experience, it is not in your interests, or your users' interests, to turn these off alongside, say, analytics cookies. Consider, therefore, breaking your cookies down into categories and providing separate opt-in and opt-out controls for each category. It is also important to keep in mind that it should remain possible for users to use your website in some way, even if they do not consent to your use of cookies.

It must also be easy for users to change their preferences later on. A popup that appears the first time a user visits your site, never to be seen again, is unlikely to deliver here. A first-visit popup is still a good idea for catching users' attention, however the settings must remain easy to find on subsequent visits.

A further important point is keeping users aware of their privacy settings. It is good practice to apply this not only to cookies, but also to other user data such as personal information stored, for example, in a user's account or profile on your website, and with respect to direct marketing preferences. Consider, therefore, a yearly email or other message to each user (where possible) reminding them to check their settings, including cookies.

It is undeniable that stricter consent requirements will be more onerous; not only for you as a business, but also for your users. Popups laden with information and asking for controls to be adjusted can often be annoying to users, but it is nonetheless important to comply with your obligations under the law and to help safeguard users' rights, even if they might be unaware of them. The key, therefore, is to make the whole experience as unobtrusive and efficient as possible, while also maintaining sufficient prominence to avoid it being missed.

2.4 How Should I Do It?

Depending upon the types of cookies you use, and the purposes you use them for, you have various options that will assist in complying with the law. Some methods will be more suitable than others, and it is always important to remember that if you use anything more than strictly necessary cookies, you will need to give users a genuine choice and the ability to opt-in or opt-out not only before your website places any cookies on the user's computer or device, but also at any time afterwards.

Option 1: Information Banner

This has been one of the most popular methods of providing cookie information to users thus far. A simple banner at the top or bottom of the (visible) web page provides a brief outline of your use of cookies and similar technologies along with a link to more detailed information. Note also the "about cookies" link in the navigation.

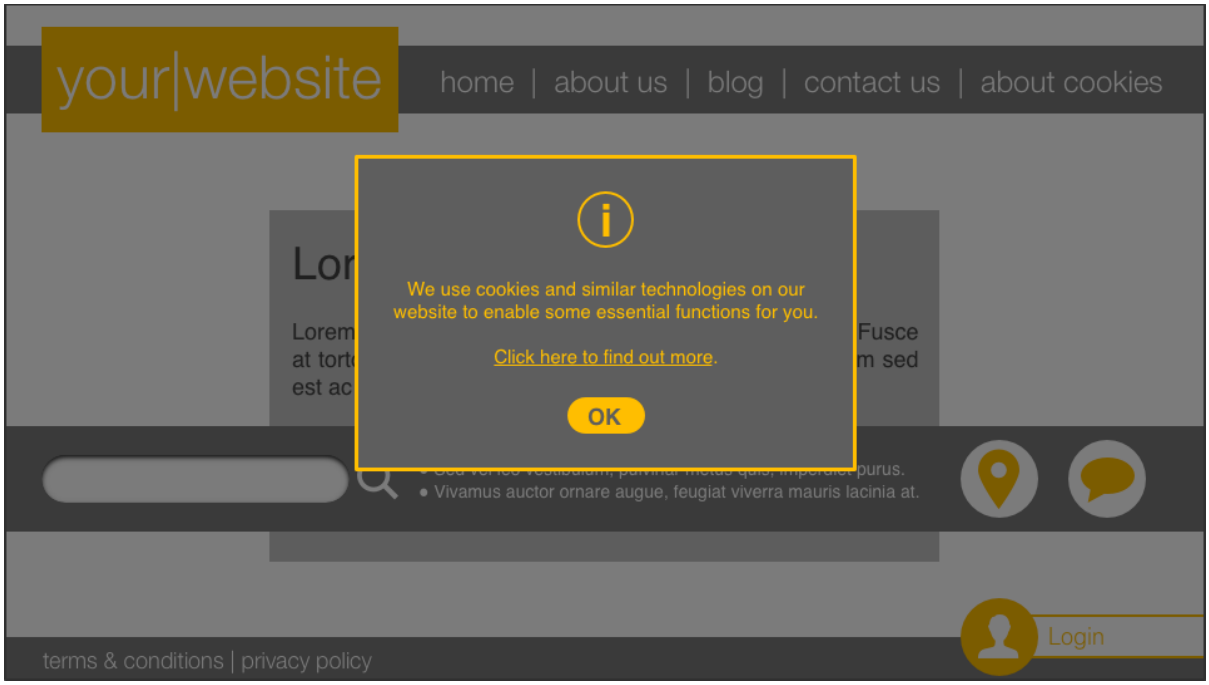
This option has the benefit of simplicity; however, it does not provide any form of control, only information. It is therefore only suitable for websites which use strictly necessary cookies alone — those without which the website would not function correctly for users.

This version of the banner adds simple opt-in / opt-out controls. This may be suitable where only a few cookies are used, particularly if they are of the same category. Care should nevertheless be taken with simple controls as they risk forcing users to disable functions that are still useful to them in order to disable those that they do not like; and forcing you to forego useful functions such as analytics. As above, note the presence of the “about cookies” link, helping to provide the ease of controlling cookies as users continue to use your website.

The approach taken here in this third evolution of the banner incorporates the so-called *granular approach* referred to above. Users are given essential information about cookies, with a link to more details, along with controls over each category of cookie. Strictly necessary cookies are noted, but no control is given; functional cookies can be turned on or off; and performance cookies (a friendlier name for analytics, in most cases) can also be

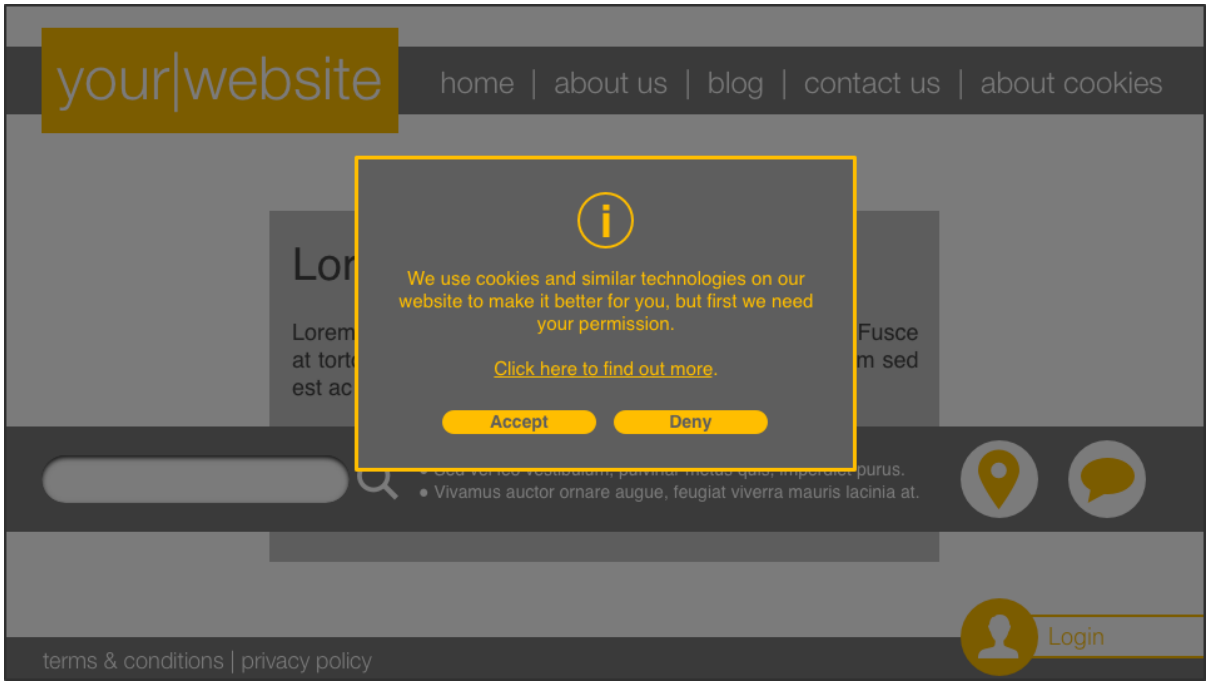
turned on or off. Of the three banner options, unless your website only uses strictly necessary cookies, this should be the preferred option for legal compliance.

Option 2: Information Popup

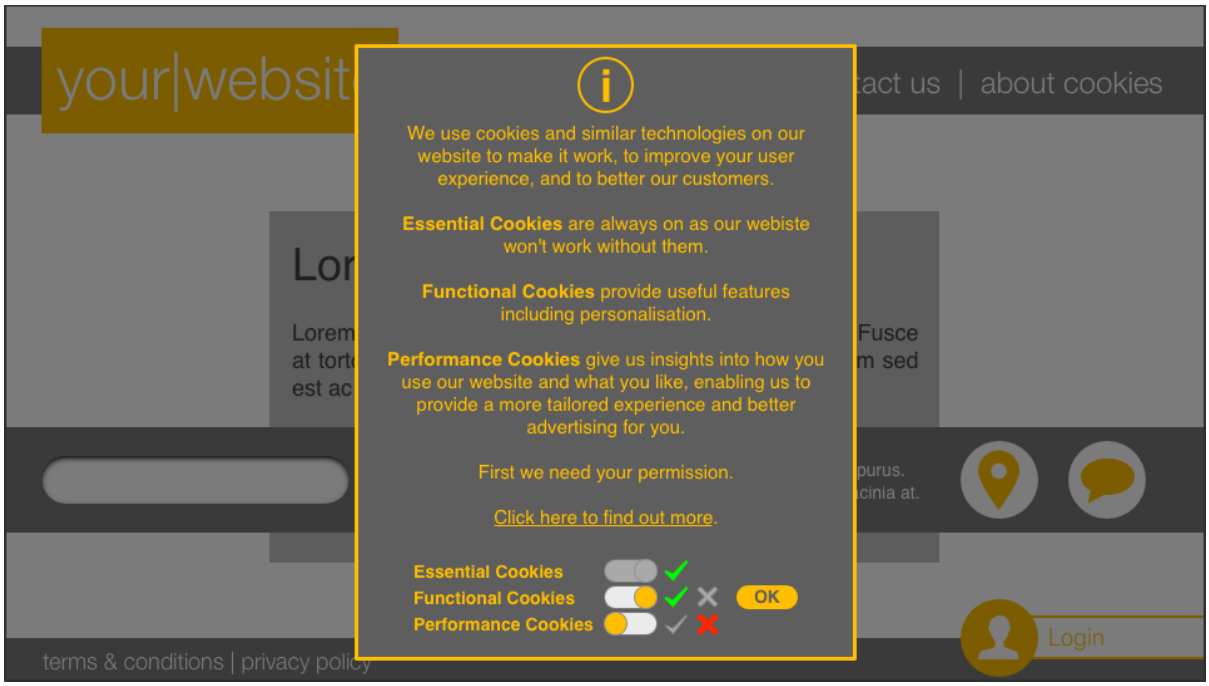


In this scenario, a popup takes over the screen and provides the same details as the information banner. Popups can be more effective than banners when it comes to grabbing users' attention as they require at least some kind of interaction from the user in order to get past them and return to the main features of the website, even if this is only clicking on a button or on an area of the screen outside of the popup's border. In extreme cases, the website behind the popup could be effectively disabled until the user acknowledges the popup.

As with the information banner, however, keep in mind that this option is only suitable for strictly necessary cookies where you are not required to provide controls.

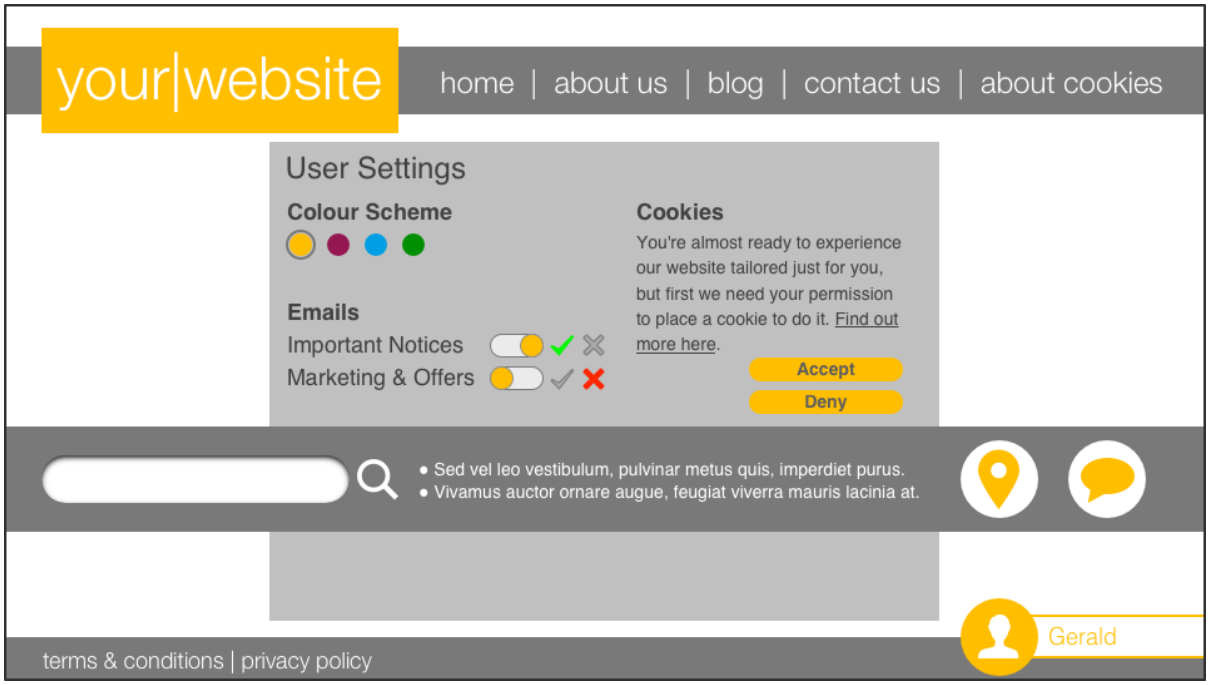


Once again, the popup approach here has the benefit of catching users' attention. In addition, as with the information banner with controls, it provides a simple opt-in or opt-out choice. However, also as with the banner approach, offering such basic binary controls may often be undesirable.



As with the information banner with sophisticated controls, this choice has the benefit of granularity. Users are given more information and more control over how cookies and, by extension, their data, are used. As a popup, rather than a banner, this option also has the advantage of more space in which to provide information. Of the popup options, unless your website only uses strictly necessary cookies, this should be the preferred option for legal compliance.

Option 3: Settings or Feature-led Consent



This approach may be attractive if your website does not use cookies from the outset, but instead only uses them when a user wishes to use certain features — personalisation, in this case. Information can be provided and consent obtained at the time that a user wishes to use the relevant features. Despite the fact that such features may not work without cookies, unless they can be reasonably categorised as *strictly necessary*, users must remain free to refuse them, even though that may mean missing out on certain features.

Which Option for Me?

There is not necessarily a right or wrong answer to this question, however it remains important to emphasise that unless you are only using some basic, strictly necessary cookies that underpin the vital functions of your website, it is essential to get users' express consent to cookies before placing them. As noted above, the GDPR expands the definition of "personal data" considerably over and above that under the Data Protection Act 1998. Data contained in cookies and similar technologies that might not qualify as personal data under the 1998 Act, or even by any conventional understanding, may well be caught by the GDPR. Instead of attempting to engage in a complex decision-making exercise to determine whether or not a particular cookie does or does not fall under the GDPR's remit, it is, we would argue, preferable to treat all cookies alike and get users' prior express permission to use them. Even if strict compliance with the letter of the law may not appear necessary, compliance with the spirit of the law and its push for improved transparency and user-led consent can surely only stand your business in good stead.

3. A Word On Advertising and Analytics

Many analytics and advertising services are provided by third parties and many use cookies and similar technologies in order to function. In many cases, advertising is often now provided with its own privacy controls and opt-out tools. AdChoices, for example, is a self-regulatory programme with hundreds of participants including major advertisers. Ads served up by AdChoices include controls enabling users to control related cookies.

The online advertising and tracking world is in a constant state of flux and it is expected by some that the GDPR, and the accompanying emphasis on consent and transparency, could herald a significant shift in how such technologies work, not least because asking for someone's permission to "track" them and feed them advertising is unlikely to go down well.

Wherever possible, the importance of prior consent must be remembered. Placing cookies when a user first arrives on your site and getting permission after the fact is not true consent at all. At the very least, a detailed, user-friendly explanation should be provided. If you track users' activity around your site for performance purposes using, for example, Google Analytics, explain the benefits to you and to your users. If your site serves up advertising, explain the benefits of allowing behavioural tracking here too — namely that users see ads that are more relevant to their interests and, therefore, less annoying and intrusive.

As the new world of the GDPR settles into reality (not to mention the forthcoming new world of the aforementioned ePrivacy Regulation) it is likely that providers of third-party services such as analytics and advertising will change the way in which their services work. For now, as the owner and/or operator of a website that employs such services, your job is to ensure that you are doing whatever you can to comply with the law and, at the risk of excessive repetition, this means keeping users as informed as possible, and getting their consent to use cookies and similar technologies that go beyond the *strictly necessary* category.

4. Conclusion

The collective bundle of requirements known as "Cookie Law" represents something of a thorn in the side for website operators. Indeed, when the so called "EU Cookie Law" first came into force in 2011, many website operators were unhappy, arguing that nobody particularly complained about cookies. What is evident, however, is that the lack of complaint was more down to a lack of knowledge and understanding among users than it was down to users being happy. It is quite possible that many still do not know or understand a great deal about the technology — simply clicking the close button or the "I agree" button and continuing to use the website in question. Meanwhile, at the other end of the scale, with the rise in the availability and popularity of browser extensions such as *AdBlock* and *Ghostery*, the more tech savvy user is quite clearly unwilling to let you or your cookies into their system or their personal data to any degree greater than is absolutely necessary for them to use your website. Some try to fight against these forms of user-centric controls, but we would argue that it is perhaps preferable to take the hint and address the reasons for their existence rather than trying to disable their effect (a course of action which is unlikely to meet with success for long anyway as the developers of such extensions frequently update them to address workarounds).

The current state of play, it must be said, is not perfect. Indeed, the increased emphasis on consent alone is set to make things more onerous for website operators and for users. More interruptions will be necessary to the user experience and users will need to read and do more before getting on with the business of using your website. Things are set to change again in the future, but for now, this is the approach that should be taken. These rules do, despite such annoyances, have honourable roots in seeking to increase and protect

individuals' rights to privacy and ultimately, it is to be hoped, there is more to be gained by complying than by resisting.