

1. Introduction

The current legal requirements for cookies are set out in the Privacy and Electronic Communications Regulations 2003 and the UK GDPR.

Privacy online is of great importance to users. It is also increasingly an important issue for businesses as their data is being commodified. It is not only important from a legal standpoint but also from a business one. By complying with the law, not only is your business safer but you are also likely to engender a greater degree of trust from its customers.

Central to the laws which govern cookies is the issue of consent. The law does not say that you can assume consent. It requires that, in many cases, you must obtain users' permission. Current common practice is to simply inform users that cookies are being taken as consent. This is no longer sufficient. Users must be properly informed, must be given a choice, and must give some kind of explicit indication of their consent.

1.1 Cookies and Similar Technologies

While most guidance focuses on cookies, the law also governs similar technologies commonly collectively referred to as "cookies". The law not only governs cookies but also other similar technologies. A number of these technologies are shared objects (also known as "flash cookies" or "local shared objects") in the browser. References to "cookies" in the law should be taken as also referring to these similar technologies. As technology evolves, the law could not keep up if it limited itself in scope to particular technologies.

1.2 The Law's Purpose

Simply put, the law aims to protect users' privacy. It is important to note that the law does not only govern cookies but also other similar technologies, such as local shared objects, clear gifs, page tags, and web bugs. The law should be taken as also referring to these similar technologies. As technology evolves, the law could not keep up if it limited itself in scope to particular technologies.

Those operating websites within the UK or whose website itself or its operator/owner is based outside of the UK are required to comply with the law.

- 1) Inform users about the purpose of the cookies and their users' computers or devices.
- 2) Obtain users' consent before using cookies.

1.3 Why Have This Law?

It is an inescapable truth that as technologies get stricter, they become more difficult to implement. Indeed, tougher consent requirements stand to not only hinder advertising and the ability to track

A reasonable question to ask is whether users can be relied upon for consent. Users may be more technically aware, or, for the more technically aware users, however, is that many users are not equally sophisticated and the sophistication of devices providing sufficient levels of control over your website, for example, but not from being saved. Even a browser that blocks or blocking all cookies would not be done using first-party cookies

the use of cookies and similar technologies is essential to business. Indeed, tougher consent requirements stand to not only hinder advertising and the ability to track user behaviour of things including behavioural advertising of your website.

built into internet browsers cannot block cookies using browser settings. The problem with such settings, however, is that not all browsers are created equal and the sophistication of devices varies considerably, often not allowing you to stop you from tracking their use of emails and shopping basket contents. Even a browser that blocks or blocking third-party cookies would not be done in this scenario of your tracking

S

A

M

P

L

E

S

2. What Do I Need to Do?

The answer to this question depends on the cookies you use on your website and for what purpose or purposes (e.g. analytics, advertising, remembering preferences, technologies, remember), their frequency of use, and their importance. A thorough cookie audit. This may also provide an opportunity to re-evaluate your use of cookies and their real value to you.

cookies you use on your website and for what purpose or purposes (e.g. analytics, advertising, remembering preferences, technologies, remember), their frequency of use, and their importance. A thorough cookie audit. This may also provide an opportunity to re-evaluate your use of cookies and their real value to you.

2.1 Know Your Cookies

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

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

2.1.1 Strictly Necessary Cookies

A cookie falls into this category if it is necessary for the operation of your website. Strictly necessary cookies may, for example, be used to enable items in a shopping basket, or enable a user to log in.

A cookie falls into this category if it is necessary for the operation of your website. Strictly necessary cookies may, for example, be used to enable items in a shopping basket, or enable a user to log in.

2.1.2 Analytics Cookies

Understanding how users use your website is extremely valuable. Analytics cookies provide insights into many factors, such as what features they are using. Analytics cookies can be set by third parties, but not always. To add to complications, analytics cookies are set by you, if the data collected by them is processed from a data protection perspective.

Understanding how users use your website is extremely valuable. Analytics cookies provide insights into many factors, such as what features they are using. Analytics cookies can be set by third parties, but not always. To add to complications, analytics cookies are set by you, if the data collected by them is processed from a data protection perspective.

2.1.3 Functionality Cookies

Many websites offer some level of functionality. Functionality cookies play a key role here. For auditing purposes, however, it is important to confuse these with the strictly necessary variety. If the site cannot function without the cookie, it isn't strictly necessary.

Many websites offer some level of functionality. Functionality cookies play a key role here. For auditing purposes, however, it is important to confuse these with the strictly necessary variety. If the site cannot function without the cookie, it isn't strictly necessary.

2.1.4 Targeting Cookies

It is important to know when and how users have used your website (including which parts they have used (including which links they have followed)). As with analytics cookies, targeting cookies enable you to make your website more relevant to those users' interests. Targeting cookies often be set by third parties.

It is important to know when and how users have used your website (including which parts they have used (including which links they have followed)). As with analytics cookies, targeting cookies enable you to make your website more relevant to those users' interests. Targeting cookies often be set by third parties.

2.1.5 First-Party Cookies

As the name suggests, these cookies are placed by your website (as opposed to those placed by third-party services). Most, if not all, of your strictly necessary and functionality cookies are first-party cookies.

As the name suggests, these cookies are placed by your website (as opposed to those placed by third-party services). Most, if not all, of your strictly necessary and functionality cookies are first-party cookies.

2.1.6 Third-Party Cookies

These cookies are placed by third-party services such as advertising and analytics. Analytics and targeting cookies are often not undertaken in-house.

These cookies are placed by third-party services such as advertising and analytics. Analytics and targeting cookies are often not undertaken in-house.

2.1.7 Persistent Cookies

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

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

A

M

P

L

E

2.1.8 Session Cookies

Any of the cookies listed above may be session cookies. Session cookies are temporary and only remain on a user's computer or device until the web browser is closed. They are removed.

2.2 The Cookie Audit

A cookie audit will help you to identify what cookies are doing, what type of cookies are used, on what computer or device, what personal data is being collected, 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 used on your website. If you don't know what cookies are used, provide a list. Alternatively, a number of online tools can help you identify the cookies currently used on your website.

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 and purpose.

2.2.3 What Types of Cookies Am I Using?

Going through the list again, identify the type of each cookie. Refer back to the list above for guidance on whether it is a persistent or a session cookie, 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 consider their duration. Persistent cookies are considered to be more privacy sensitive than session cookies, so for each one, consider whether its lifespan is truly necessary 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. However, it is more likely now that data used by cookies is considered to be personal data. The obvious – name, email address, IP address – all qualify under the UK GDPR. Even identifiers that do not identify an individual on their own may be used to identify an individual when combined with other data and used to identify an individual. If you are processing personal data as a result of cookies, you must ensure that you comply with the requirements of the UK GDPR.

2.2.6 Are My Cookies Legal?

Keeping your own first-party cookies is legal, but you must obtain the correct consent to use them (or they may be considered to be processing personal data and you must comply fully with the UK GDPR). If you are using third-party cookies, while control over them rests (at least to a point) with the third party, they are still being used on your website. It is therefore important that you ensure that the third party or parties involved are also complying with the law.

S

A

M

P

L

E

2.3 Information and Consent

2.3.1 Informing Users

One of the most important principles when personal data is concerned (and cookies are personal data) is that individuals know what data you have about them after being provided with such information.

It is a good idea to start with a clear explanation of what cookies actually do. Many users will have no idea what they are or what they may not know a great deal about them. Consider, for example, the following explanation of the different cookie types similar to that included above in the sample:

Even if you are only using *strictly necessary* cookies, it is important that users are fully informed about what you are doing with them. Using cookies, but that does not mean you have no reason to hide them, it is worth revealing. The general rule is, the more precise the information, the better. Another general rule is to keep things simple; the average user does not possess a high degree of technical knowledge so using straightforward language in your cookie policy is always advisable. Some users may go a little overboard with friendly, fuzzy, humorous language, but this is not a good idea as it downplays the perception that cookies are little more than spyware. They are useful, innocuous little files that they (usually) really are.

Your cookie information should explain the functions of the various cookies placed by your website, what they do 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, explaining how they benefit the user. Your explanation should be positive. It is thus preferable to say something like:

“By seeing how you use our website, we are better able to understand our customers and improve our services.”

as opposed to:

“If you do not accept our cookies, we will be unable to improve our services as we will be unable to understand our customers around our website.”

Put simply, tell your users why a website is good for them, rather than why their refusal to accept them is bad.

Another useful element to include is a table listing the cookies you use, what each one does, and what terminology as much as possible.

focuses on transparency. Where cookies (include cookies), it is vital that users are fully informed about what you are doing with it. It is only after being provided with such information that you can ask for their informed consent.

of what cookies are and what they do on users, and in particular, what they may not know a great deal about them. Consider, for example, the following explanation of the different cookie types similar to that included above in the sample:

is important that users are fully informed about what you are doing with them. Using cookies, but that does not mean you have no reason to hide them, it is worth revealing. The general rule is, the more precise the information, the better. Another general rule is to keep things simple; the average user does not possess a high degree of technical knowledge so using straightforward language in your cookie policy is always advisable. Some users may go a little overboard with friendly, fuzzy, humorous language, but this is not a good idea as it downplays the perception that cookies are little more than spyware. They are useful, innocuous little files that they (usually) really are.

stand the functions of the various cookies placed by your website, what they do 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, explaining how they benefit the user. Your explanation should be positive. It is thus preferable to say something like:

“By seeing how you use our website, we are better able to understand our customers and improve our services.”

“If you do not accept our cookies, we will be unable to improve our services as we will be unable to understand our customers around our website.”

is good for them, rather than why their refusal to accept them is bad.

table listing the cookies you use, what each one does, and what terminology as much as possible. Again, try to use user-friendly terminology as much as possible.

2.3.2 Where Should I Put My Info

The key word here is “prominence”. It is not the best way to attract a transparent and consent under be similarly prominent.

It is a good idea to bring cookies for consent to use cookies (where detail below. Because your information) should be presented prominent link on every page of your

While it is a matter of taste to a privacy policy is also important. controls plays a part here. It is a information (or at least the links privacy policy, for example). Not easier for non-technical users to find

2.3.3 Consent

Consent is one of the key features have been applied. Implied consent obtaining users’ permission to use provide users with information about website will be taken as consent decidedly inconsistent.

This does not necessarily mean that that you wish to use. Strictly necessary reality says very little about cookies Communications (EC Directive) Regulation

Can I Rely on Implied Consent?

Implied consent is no longer a sufficient some affirmative action in order to any cookies are placed.

Can I Rely on Browser Settings?

This is a difficult question at present users’ browser settings is not a sufficient not possess sufficient technical knowledge browser settings for genuine consent

There is nothing, of course, to stop adjusting their browser’s privacy settings recommended.

This is a position that may change Regulation which may impose new that, eventually, browser settings between the UK and EU could align

S

A

M

P

L

E

n of cookies in your privacy policy aid, the increased importance of ns that your privacy policy should

ers’ attention, along with a request s something we’ll go into in more anisms (also see below for more that it is available at all times. A the preferable route.

of cookie information from your ased importance of consent and ut your privacy policy and cookie ctly to the cookie section of your prominence, but it also makes it for.

n area in which stricter standards time, been a popular method of thod prior to the UK GDPR was to em that their continued use of the cookies. Controls have also been

n control over every single cookie cceptable. The UK GDPR itself in ogies. The Privacy and Electronic e focused on such matters.

DPR world. Users must now take over, this must take place before

as long been that relying solely on eady been noted, many users do This, therefore, makes relying on od.

Additional advice to your users on ce on those settings alone is not

er the EU’s proposed ePrivacy ers of web browsers to the extent Post-Brexit regulatory alignment opts legislation very similar to the

ePrivacy Regulation when it comes to cookies. It is not currently the law and that binds them!

What About Affirmative Consent?

This, if it is not already clear by now, is either on your part, on your users' part, or that it is safest for everyone.

It is important that users are given a choice. It is acceptable to simply tell users that they can accept your cookies. An important concept is "granular consent". In practice, this means giving users control over what their data is used for. You are not expected to enable cookies for everything. You are expected to store items in an online shopping cart, for example, selectively. If, for example, your website is essential to its functionality, but not for analytics, or your users' interests, or your website's interests, Consider, therefore, breaking your website into categories and providing separate opt-in and opt-out controls for each category. It should remain possible for users to use your website without your use of cookies.

It must also be easy for users to change their settings the first time a user visits your site, not just on subsequent visits. A first-visit popup is still a good idea for categories that are not essential to the website, but it must be easy to find on subsequent visits.

A further important point is keeping track of user preferences. It is good practice to apply this not only to cookies, but also to other data stored, for example, in a user's account. This includes marketing preferences. Consider, therefore, sending an email or other message to each user to remind them of their preferences (where possible) reminding them to update their preferences.

It is undeniable that stricter consent requirements are more onerous; not only for you as a business, but also for your users. However, the requirements can often be adjusted to be less onerous. It is nevertheless important to comply with your obligations under the law and to respect your users' rights, even if they might be unaware of them. The key, therefore, is to make the experience as unobtrusive and efficient as possible, while also making it clear that the user can change their preferences at any time.

It is important, however, to note that this is not currently sufficient. Do not rely on this as a legal basis.

It leaves no room for doubt, however, that the Commission's part, meaning that it is not currently sufficient.

As already been noted, it is no longer sufficient to simply tell users that they are agreeing to your website, they are agreeing to your website. UK GDPR is known as "granular consent". In practice, this means giving users control over what their data is used for. You are not expected to enable cookies for everything. You are expected to store items in an online shopping cart, for example, selectively. If, for example, your website is essential to its functionality, but not for analytics, or your users' interests, or your website's interests, Consider, therefore, breaking your website into categories and providing separate opt-in and opt-out controls for each category. It should remain possible for users to use your website without your use of cookies.

It must also be easy for users to change their settings the first time a user visits your site, not just on subsequent visits. A first-visit popup is still a good idea for categories that are not essential to the website, but it must be easy to find on subsequent visits.

A further important point is keeping track of user preferences. It is good practice to apply this not only to cookies, but also to other data stored, for example, in a user's account. This includes marketing preferences. Consider, therefore, sending an email or other message to each user to remind them of their preferences (where possible) reminding them to update their preferences.

It is undeniable that stricter consent requirements are more onerous; not only for you as a business, but also for your users. However, the requirements can often be adjusted to be less onerous. It is nevertheless important to comply with your obligations under the law and to respect your users' rights, even if they might be unaware of them. The key, therefore, is to make the experience as unobtrusive and efficient as possible, while also making it clear that the user can change their preferences at any time.

S

A

M

P

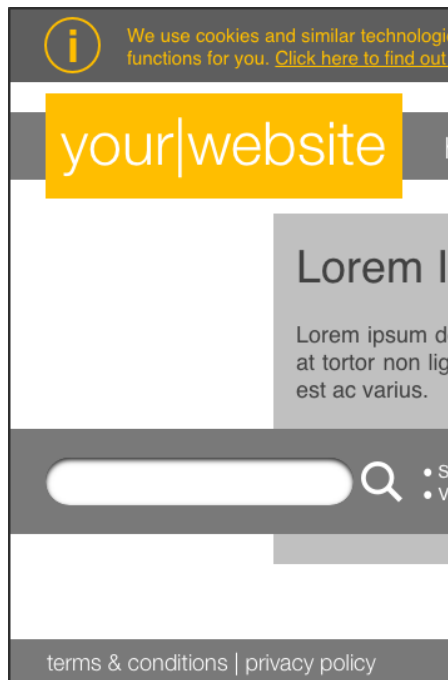
L

E

2.4 How Should I Do It?

Depending upon the types of cookies you use, there are various options that will assist in complying with the law. Some methods will be more suitable than others, and it is always best to go beyond strictly necessary cookies, you should provide users with the ability to opt-in or opt-out not only before cookies are placed on their device, but also at any time after.

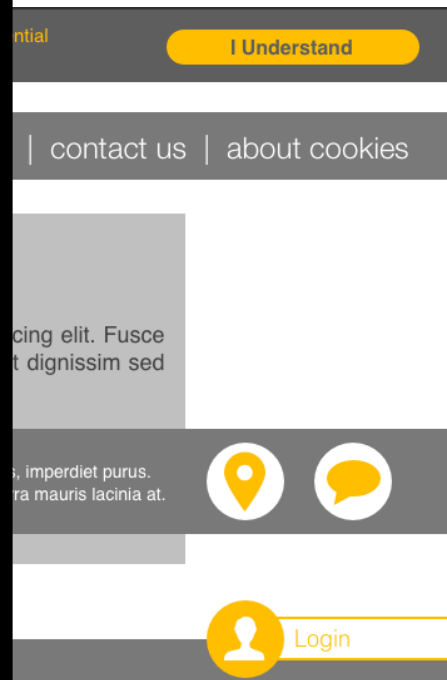
Option 1: Information Banner



This has been one of the most popular methods for providing cookie information to users thus far. A simple banner at the top of the (visible) web page provides a brief outline of your use of cookies and a link to more detailed information. Note also the “about cookies” link.

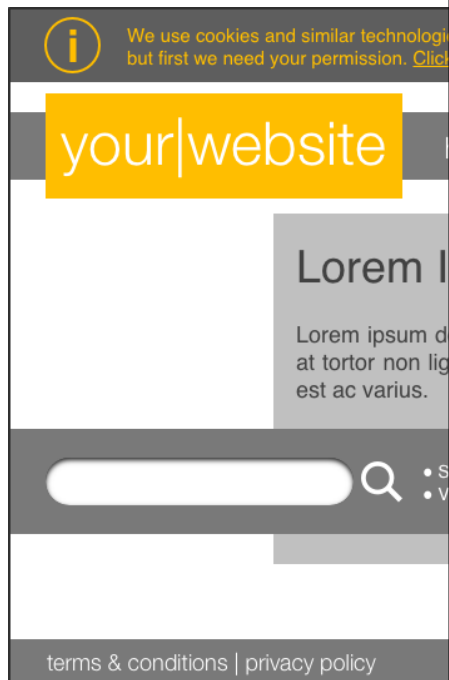
This option has the benefit of simplicity, but it only provides information. It is therefore not sufficient for cookies which use strictly necessary cookies alone — those without which the website cannot function correctly for users.

When you use cookies, you have a choice. Some methods will be more suitable than others, and it is always best to go beyond strictly necessary cookies, you should provide users with the ability to opt-in or opt-out not only before cookies are placed on their device, but also at any time after.



This has been one of the most popular methods for providing cookie information to users thus far. A simple banner at the top of the (visible) web page provides a brief outline of your use of cookies and a link to more detailed information. Note also the “about cookies” link.

This option has the benefit of simplicity, but it only provides information. It is therefore not sufficient for cookies which use strictly necessary cookies alone — those without which the website cannot function correctly for users.

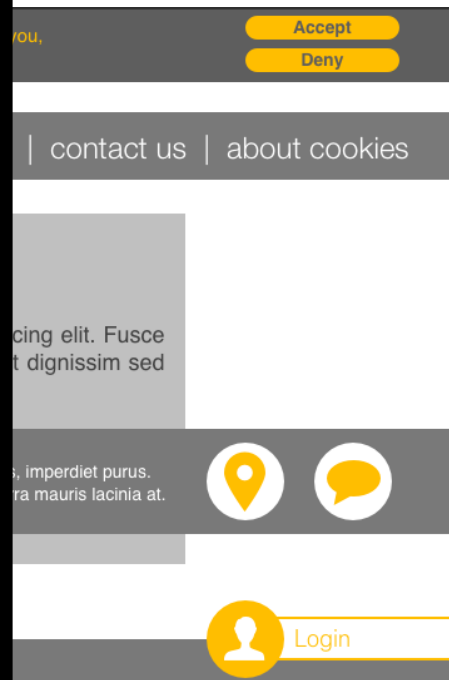


This version of the banner adds only a few cookies are used, but nevertheless be taken with simple are still useful to them in order to forego useful functions such as the “about cookies” link, helping to provide your website.

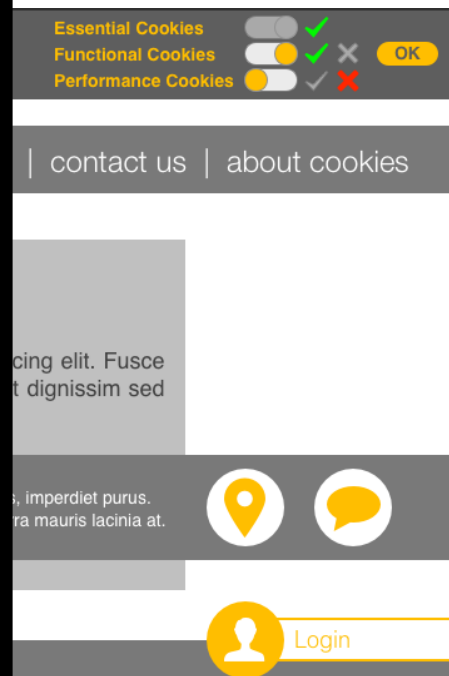


The approach taken here in this *granular approach* referred to above, with a link to more details, also necessary cookies are noted, but off; and performance cookies (a

SAMPLE



controls. This may be suitable where the same category. Care should be taken in forcing users to disable functions that they do not like; and forcing you to note the presence of the “about cookies” link, helping to provide your website.

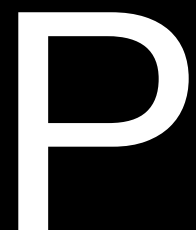


This banner incorporates the so-called *granular approach* referred to above, with a link to more details, also necessary cookies are noted, but off; and performance cookies (a

S

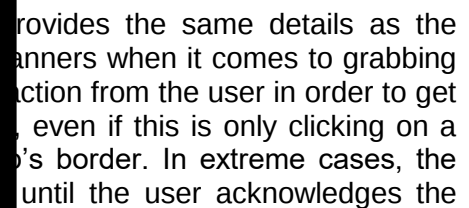
A

M

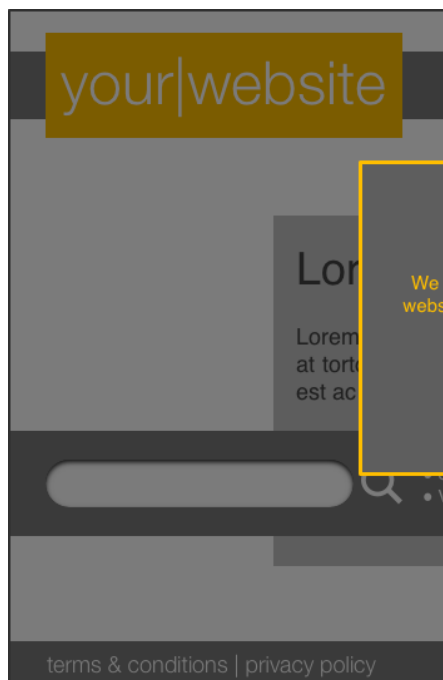


L

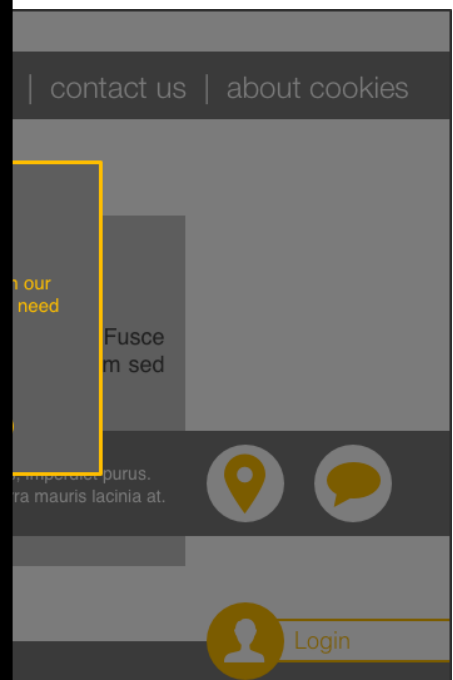
E

[illegible]

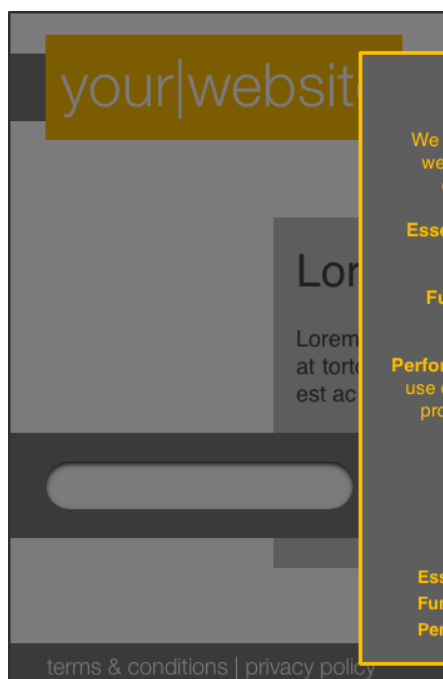
SAMPLE



Once again, the popup approach provides a simple opt-in or opt-out choice. However, also as with the information banner, such basic binary controls may often be undesirable.



of catching users' attention. In addition, as with the information banner, such basic binary controls may often be undesirable.

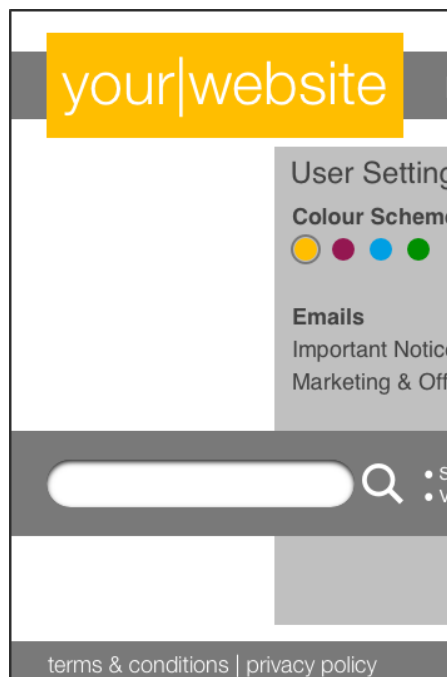


As with the information banner version, this choice has the benefit of granularity. Users are given more control over how cookies and, by extension, their data, are used. As a banner, this option also has the advantage of more space in which to present the information. Of the popup options, unless your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



Of the popup options, unless your website only uses strictly necessary cookies, this may be the preferred option for legal compliance.

Option 3: Settings or Feature-led



This approach may be attractive instead only uses them when a user wants to use the relevant features. Despite this, users may not work without cookies, unless they can be reasonably expected to refuse them, even though that may

Which Option for Me?

There is not necessarily a right answer, but it is important to emphasise that using cookies that underpin the vital functions of a website requires user consent to cookies before placing them. The definition of “personal data” considered under the Data Protection Act 1998 regime. Instead of attempting to determine whether or not a particular feature falls within the remit, it is, we would argue, preferable to seek user permission to use them. Even if some features are strictly necessary, compliance with the spirit of the law user-led consent can surely only serve

S

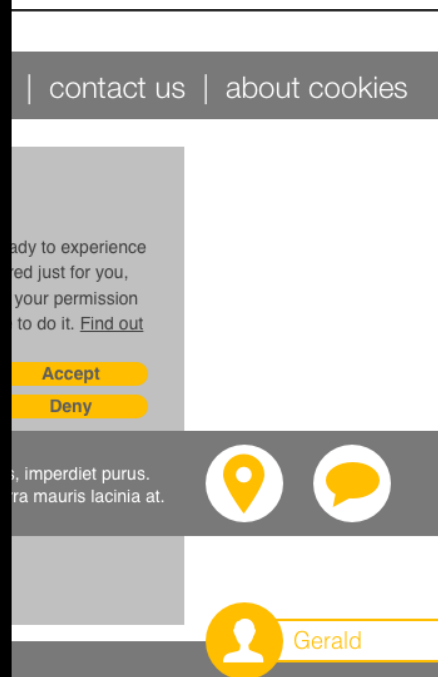
A

M

P

L

E



use cookies from the outset, but for certain features — personalisation, in this case — at the time that a user wishes to use them, certain features may not work without cookies, and, if strictly necessary, users must remain free to refuse to use certain features.

On this question, however it remains important to emphasise that using some basic, strictly necessary cookies is essential to get users' express consent. However, the UK GDPR expands the definition of “personal data” considered under the old Data Protection Act 1998 regime. Instead of attempting to determine whether or not a particular feature falls within the remit, it is, we would argue, preferable to seek user permission to use them. Even if some features are strictly necessary, compliance with the spirit of the law user-led consent can surely only serve to ensure that the letter of the law may not appear to be a wash for improved transparency and user-led consent can surely only serve to ensure that the letter of the law may not appear to be a wash for improved transparency and

3. A Word On Advertising and A

Many analytics and advertising services and similar technologies in order to be provided with its own privacy controls. The regulatory programme with hundreds of controls up by AdChoices include controls

The online advertising and tracking industry is in a state of flux and it is expected by some that the UK GDPR, and the new ePrivacy Directive, could herald a significant shift in the way that someone's permission to "track" their

Wherever possible, the importance of consent when a user first arrives on your site should be at all. At the very least, a detailed explanation of users' activity around your site using Google Analytics, explain the benefits to you and explain the benefits of allowing behaviour that are more relevant to their interests.

4. Conclusion

The collective bundle of requirements has become a thorn in the side for website operators. Since it came into force in 2011, many complaints have been made, particularly complained about cookies. The complaint was more down to a lack of understanding than was down to users being happy to give consent. They understand a great deal about the "I agree" button and continuing to use the website. At the scale, with the rise in the average number of steps by companies like Apple and Google, by default, many users are quite happy to give their personal data to any degree to use your website. Some try to fight against it, but we would argue that it is perhaps preferable to accept its existence rather than trying to eliminate it (which will meet with success for long any of the many workarounds).

The current state of play, it must be said, is that consent alone is set to make things worse. More interruptions will be necessary to get consent, and more before getting on with the business. This is again in the future, but for now, the industry, despite such annoyances, have accepted the reality of individuals' rights to privacy and the need to comply rather than by resisting.

third parties and many use cookies. In some cases, advertising is often now served by AdChoices, for example, is a self-regulatory programme for major advertisers. Ads served by AdChoices use related cookies.

The online advertising and tracking industry is in a state of flux and it is expected by some that the UK GDPR, and the new ePrivacy Directive, could herald a significant shift in the way that someone's permission to "track" their

Wherever possible, the importance of consent when a user first arrives on your site should be at all. At the very least, a detailed explanation of users' activity around your site using Google Analytics, explain the benefits to you and explain the benefits of allowing behaviour that are more relevant to their interests.

The "EU Cookie Law" represents something of a change. The so called "EU Cookie Law" first came into force in 2011, many complaints have been made, particularly complained about cookies. The complaint was more down to a lack of understanding than was down to users being happy to give consent. They understand a great deal about the "I agree" button and continuing to use the website. At the scale, with the rise in the average number of steps by companies like Apple and Google, by default, many users are quite happy to give their personal data to any degree to use your website. Some try to fight against it, but we would argue that it is perhaps preferable to accept its existence rather than trying to eliminate it (which will meet with success for long any of the many workarounds).

Indeed, the increased emphasis on consent alone is set to make things worse. More interruptions will be necessary to get consent, and more before getting on with the business. This is again in the future, but for now, the industry, despite such annoyances, have accepted the reality of individuals' rights to privacy and the need to comply rather than by resisting.