

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. These are commonly collectively referred to as cookies. A number of other technologies, such as local shared objects (also known as "flash cookies"), clear gifs, page tags, and web bugs. 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. The UK GDPR extends this protection to all personal data. It may not be immediately obvious that a cookie can identify an individual. However, if a cookie can identify an individual, 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, is to treat all cookies with a degree of caution and treat all cookies as personal data.

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 equal and the sophistication of devices varies considerably, often not providing sufficient levels of control over their use of your website, for example, but not from being saved. Even a browser that blocks third-party cookies 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 and the ability to track user behaviour of your website.

built into internet browsers cannot 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 equal and the sophistication of devices varies considerably, often not providing sufficient levels of control over their use of your website, for example, but not from being saved. Even a browser that blocks third-party cookies or blocking all cookies would not be done using first-party cookies

SAMPLE

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. for analytics, advertising, remembering preferences, technologies, remember), their frequency of use, and their importance. A thorough cookie audit. This may also be a good 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. for analytics, advertising, remembering preferences, technologies, remember), their frequency of use, and their importance. A thorough cookie audit. This may also be a good 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 for logging in, storing items in a shopping basket, or enabling a user to navigate through a website.

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

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. For auditing purposes, however, it is necessary to have a variety of cookies. If the site cannot function without the cookie, it isn't strictly necessary.

Many websites offer some level of functionality. For auditing purposes, however, it is necessary to have a variety of cookies. 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.

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.

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.

2.2.3 What Types of Cookies Are They?

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 personal data. The obvious – name, email address, etc. – identifiers qualify under the UK GDPR. Even if a cookie does not identify an individual on its own, it may be 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 must be strictly necessary to comply fully with the UK GDPR). For third-party cookies, while control over their use rests (at least to a point) with the third party, you are still responsible for ensuring they are being used on your website. It is therefore important to ensure that you are also complying with the law.

S

A

M

P

L

E

e. Session cookies are temporary and only remain on a user's computer or device until the point at which they visit your website. They are removed.

used by your website, what those cookies are doing, how long they remain on a user's computer or device, whether or not they are being used in compliance with the law.

technologies) currently used on your website. Your web developer should be able to provide a list. Alternatively – are available online.

ed for. It is important that you are clear about each cookie's function.

are at work on your website. Refer back to the list above for guidance on whether it is strictly necessary, for analytics, functionality, or for targeting.

f 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.

o and in light of the UK GDPR it is more likely now that data used by cookies is considered personal data. The obvious – name, email address, etc. – identifiers qualify under the UK GDPR. Even if a cookie does not identify an individual on its own, it may be 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.

ortant, and in addition to obtaining the correct consent to use them (or they must be strictly necessary to comply fully with the UK GDPR). For third-party cookies, while control over their use rests (at least to a point) with the third party, you are still responsible for ensuring they are being used on your website. It is therefore important to ensure that you are also complying with the law.

2.3 Information and Consent

2.3.1 Informing Users

One of the most important principles when personal data is concerned (and this is true for individuals know what data you have collected 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 about them. Consider, for example, the following information similar to that included above in the sample template:

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 remembering. 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. Sometimes a little overboard with friendly, fuzzy, humorous language, but this can be of downplaying the perception that cookies are little more than spyware than they (usually) really are.

Your cookie information should explain the functions of the various cookies placed by your website, what personal data is involved. In situations where you use cookies to provide useful information to you, such as analytics cookies, you should explain 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 for them.

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

focuses on transparency. Where cookies (include cookies), it is vital that you explain what you are doing with it. It is only after you have given your users their informed consent.

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 remembering. 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. Sometimes a little overboard with friendly, fuzzy, humorous language, but this can be of downplaying the perception that cookies are little more than spyware than they (usually) really are.

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 remembering. 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. Sometimes a little overboard with friendly, fuzzy, humorous language, but this can be of downplaying the perception that cookies are little more than spyware than they (usually) really are.

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 remembering. 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. Sometimes a little overboard with friendly, fuzzy, humorous language, but this can be of downplaying the perception that cookies are little more than spyware than they (usually) really are.

“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.”

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

Another useful element to include is a table listing the cookies you use, what each one does, and what its purpose is. 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 attention, but transparency and consent under the new rules should be similarly prominent.

It is a good idea to bring cookies to the user's attention for consent to use cookies (where required) in more detail below. Because your information should be presented in a prominent link on every page of your website.

While it is a matter of taste to a large extent, the prominence of your privacy policy is also important. The user interface controls plays a part here. It is a good idea to link to your information (or at least the links to your privacy policy, for example). Not only is it easier for non-technical users to find, but it also makes it

2.3.3 Consent

Consent is one of the key features of the new rules. Implied consent has been applied. Implied consent is obtaining users' permission to use your website without providing users with information about how their website will be taken as consent. This is decidedly inconsistent.

This does not necessarily mean that you wish to use. Strictly necessary cookies are an exception. In reality says very little about cookies. The UK GDPR and the Communications (EC Directive) Regulations 2003.

Can I Rely on Implied Consent?

Implied consent is no longer a valid basis for consent. Some affirmative action in order to obtain consent before any cookies are placed.

Can I Rely on Browser Settings?

This is a difficult question at present. Relying on users' browser settings is not a sufficient basis for consent. Users do not possess sufficient technical knowledge to adjust their browser settings for genuine consent.

There is nothing, of course, to stop users from adjusting their browser's privacy settings. However, this is not recommended.

This is a position that may change under the EU's proposed ePrivacy Regulation which may impose new rules. That, eventually, browser settings will be a sufficient basis for consent between the UK and EU could also be possible.

S

A

M

P

L

E

of cookies in your privacy policy. It is not the best way to attract attention, but the increased importance of transparency and consent under the new rules should be similarly prominent.

users' attention, along with a request for consent to use cookies (where required) in more detail below. Because your information should be presented in a prominent link on every page of your website. That it is available at all times. A prominent link on every page of your website is the preferable route.

of cookie information from your website. The increased importance of consent and the user interface controls plays a part here. It is a good idea to link to your information (or at least the links to your privacy policy, for example). Not only is it easier for non-technical users to find, but it also makes it

an area in which stricter standards have been applied. Implied consent has been applied. Implied consent is obtaining users' permission to use your website without providing users with information about how their website will be taken as consent. This is decidedly inconsistent.

control over every single cookie is not a sufficient basis for consent. Relying on users' browser settings is not a sufficient basis for consent. Users do not possess sufficient technical knowledge to adjust their browser settings for genuine consent.

GDPR world. Users must now take affirmative action in order to obtain consent before any cookies are placed.

as long been that relying solely on users' browser settings is not a sufficient basis for consent. Users do not possess sufficient technical knowledge to adjust their browser settings for genuine consent.

additional advice to your users on adjusting their browser's privacy settings. However, this is not recommended.

er the EU's proposed ePrivacy Regulation which may impose new rules. That, eventually, browser settings will be a sufficient basis for consent between the UK and EU could also be possible.

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 are accepting 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 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 (where possible) reminding them to check their settings.

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 to users how to find the settings to avoid it being missed.

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 the GDPR, is not 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 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 (where possible) reminding them to check their settings.

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 to users how to find the settings to avoid it being missed.

S

A

M

P

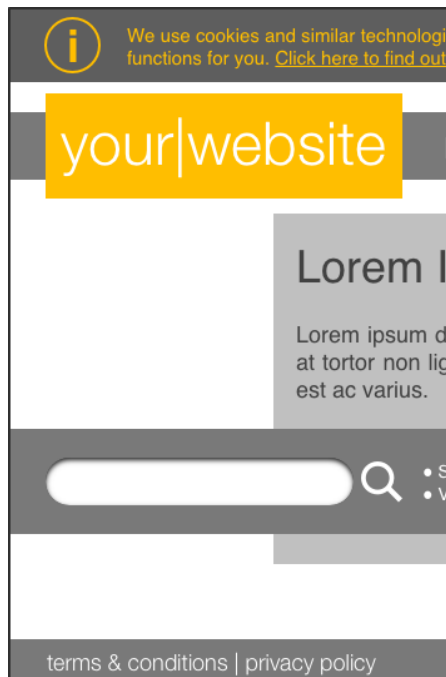
L

E

2.4 How Should I Do It?

Depending upon the types of cookies you use, there are various options that will assist in compliance. Some methods will be more suitable than others, and it is always best to use more than strictly necessary cookies, you should provide a way to opt-in or opt-out not only before cookies are set on the user's device, but also at any time after.

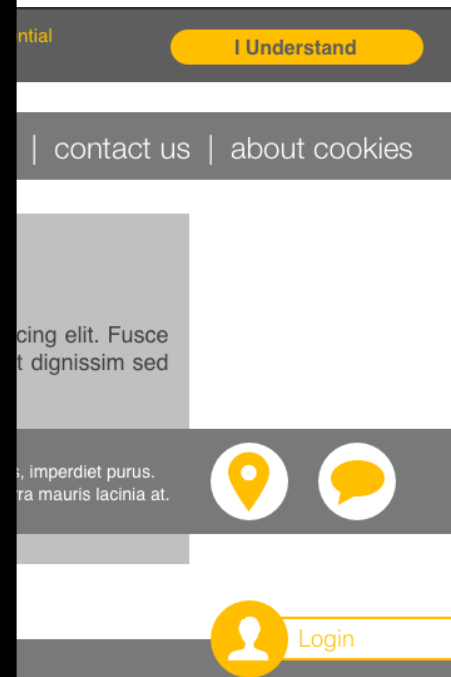
Option 1: Information Banner



This has been one of the most popular methods 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.

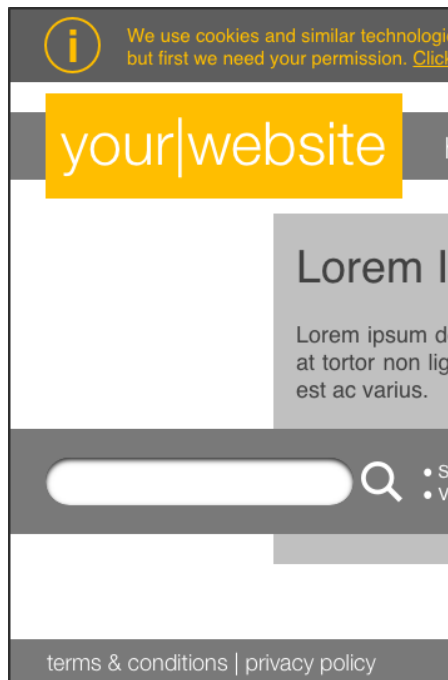
When you use cookies, you have a legal obligation to inform users. Some methods will be more suitable than others, and it is always best to use more than strictly necessary cookies, you should provide a way to opt-in or opt-out not only before cookies are set on the user's device, but also at any time after.



Providing cookie information to users (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.

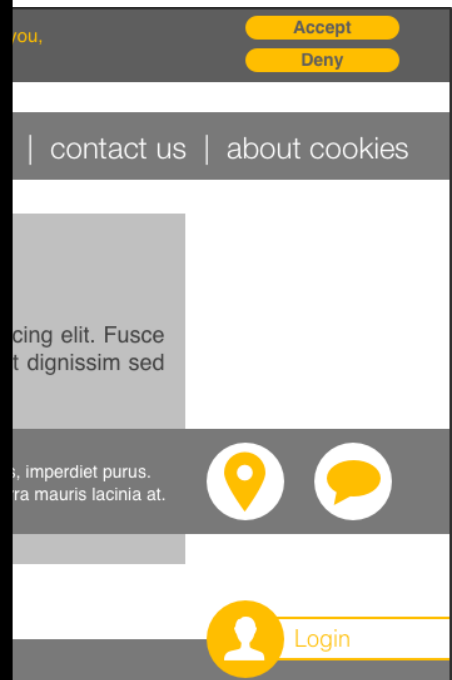
SAMPLE



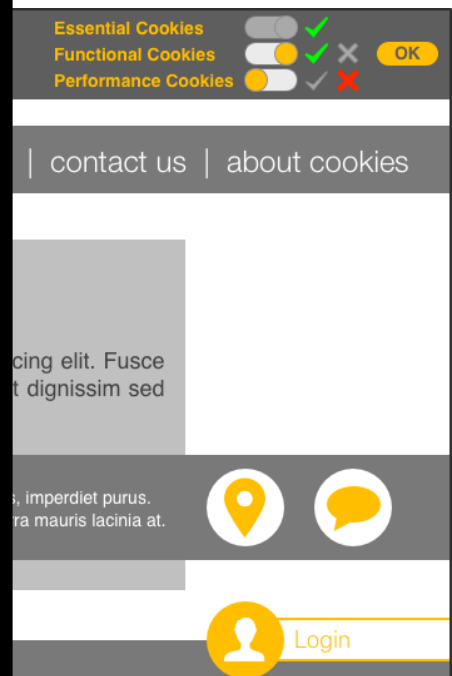
This version of the banner adds only a few cookies are used, pa nevertheless be taken with simple are still useful to them in order t forego useful functions such as cookies” link, helping to provide your website.



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



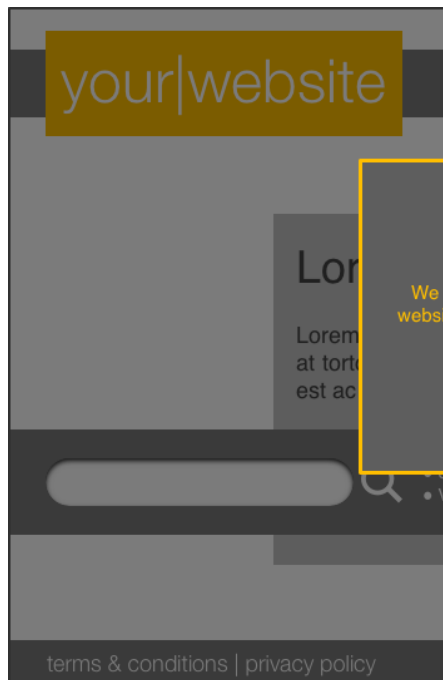
controls. This may be suitable where the same category. Care should ing users to disable functions that y do not like; and forcing you to ote the presence of the “about cookies as users continue to use



banner incorporates the so-called essential information about cookies, each category of cookie. Strictly ional cookies can be turned on or ics, in most cases) can also be

turned on or off. Of the three necessary cookies, this should be

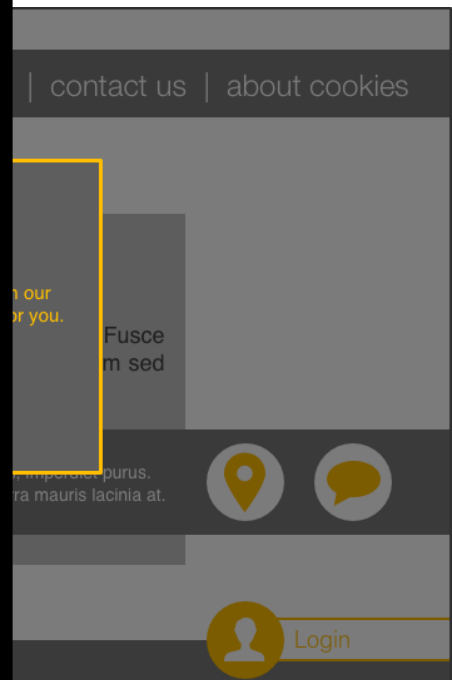
Option 2: Information Popup



In this scenario, a popup takes the place of an information banner. Popups can be more effective than banners as they require user attention as they require a user to click on a button or on an area of the screen to close the popup. The website behind the popup could be partially obscured.

As with the information banner, this option is only suitable for strictly necessary cookies where you have a legitimate interest.

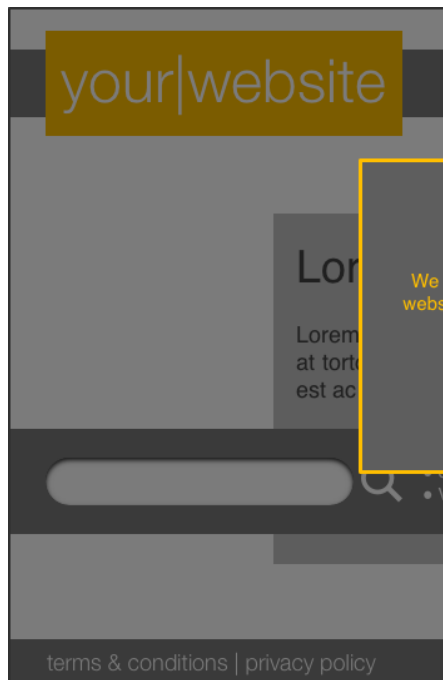
your website only uses strictly necessary cookies for legal compliance.



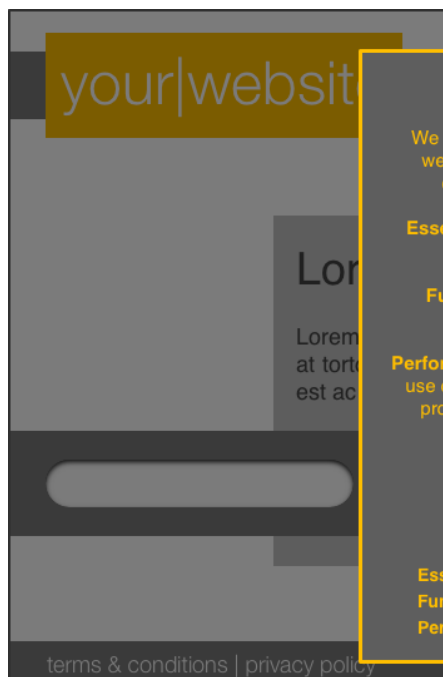
This option provides the same details as the information banner when it comes to grabbing user attention. It requires action from the user in order to get past the popup, even if this is only clicking on a button or on an area of the screen's border. In extreme cases, the popup could prevent the user from interacting with the website until the user acknowledges the popup.

As with the information banner, this option is only suitable for strictly necessary cookies where you have a legitimate interest.

SAMPLE

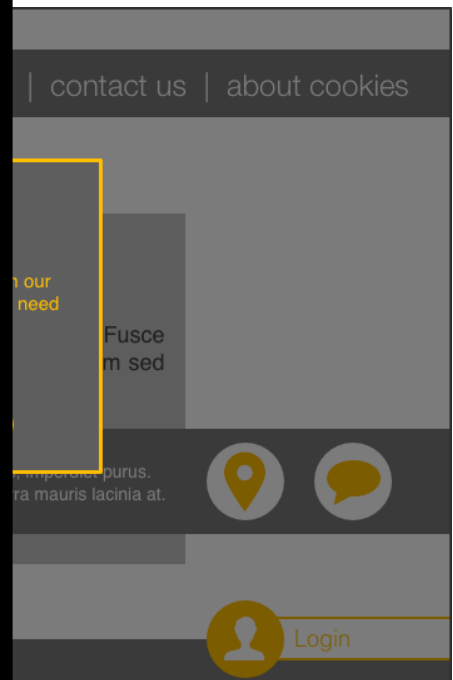


Once again, the popup approach provides a simple opt-in or opt-out choice. However, also as with the information banner, this approach can often be undesirable.



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. An advantage of more space in which to present the information is that the website only uses strictly necessary cookies for legal compliance.

SAMPLE

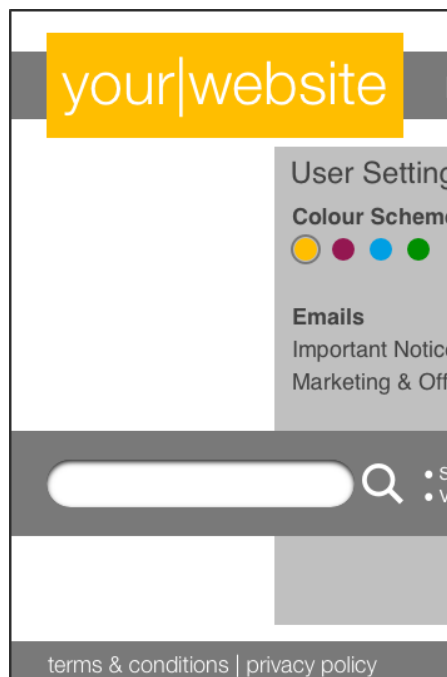


of catching users' attention. In addition, as with the information banner, this approach provides a simple opt-in or opt-out choice. However, also as with the information banner, this approach can often be undesirable.



Of the popup options, unless your website only uses strictly necessary cookies for legal compliance, this choice has the benefit of granularity. Users are given more control over how cookies and, by extension, their data, are used. An advantage of more space in which to present the information is that the website only uses strictly necessary cookies 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. It is important to emphasise that under the UK GDPR, cookies that underpin the vital functions of a website must be placed without consent to cookies before placing them. The definition of “personal data” considered under the old Data Protection Act 1998 regime. Instead of attempting to determine whether or not a particular cookie falls within the remit, it is, we would argue, preferable to seek the user's permission to use them. Even if some cookies are strictly necessary, compliance with the spirit of the law through user-led consent can surely only serve

S

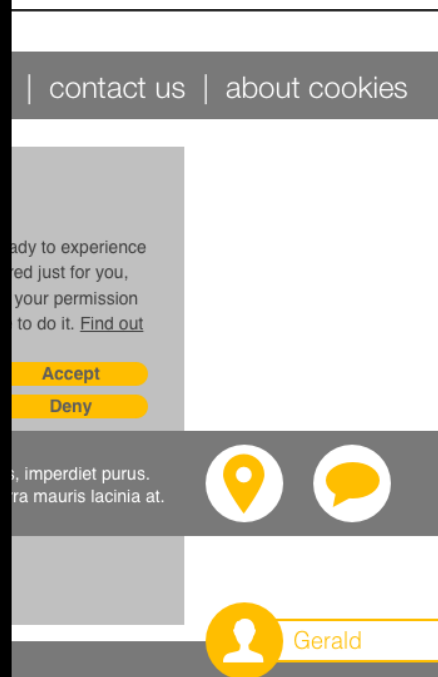
A

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. If certain features may not work without cookies, and they are strictly necessary, users must remain free to refuse them, even though that may

In this question, however it remains important to emphasise that under the UK GDPR, cookies that underpin the vital functions of a website must be placed without consent to cookies before placing them. The definition of “personal data” considered under the old Data Protection Act 1998 regime. Instead of attempting to determine whether or not a particular cookie falls within the remit, it is, we would argue, preferable to seek the user's permission to use them. Even if some cookies are strictly necessary, compliance with the spirit of the law through user-led consent can surely only serve

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 the user 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 the user's attention 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 controlled 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 the user 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 the user's attention 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.