

1. Introduction

The current legal requirements for Privacy and Electronic Communica

Privacy online is of great importance and is also increasingly an important issue as their data is being commodified. It is not only important from a legal standpoint under the law, not only is your business safe but also a degree of trust from its customers.

Central to the laws which govern this area is the issue of consent. The law does not say that you can simply opt out, it requires that, in many cases, you must obtain users' permission. Current common practice is to simply inform users that their data is being taken as consent. This is no longer sufficient. Users must be properly informed, must understand the 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 commonly collectively referred to as cookies. A number of other technologies are also covered, including shared objects (also known as "flash cookies"), web bugs, and 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 due to the far greater definition of "personal data". It may not be immediately obvious that a cookie can identify an individual; however, where a cookie can identify an individual, it qualifies as personal data; however, even if identification can only be made by combining the data in question, it will fall within the definition. The rule of thumb we would suggest, and similar technologies in the same way, such as local storage, clear gifs, page tags, and web bugs, the law could not keep up if it

Those operating websites within the UK (or based outside of the UK) are required to obtain users' permission before placing or using cookies on their website or its operator/owner is required to obtain users' permission before placing or using cookies on their website places and stores on their website places and stores on their website.

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

1.3 Why Have This Law?

S
A
M
P
L
E

It is an inescapable truth that as tracking technologies get stricter, they become more of a burden to business. Indeed, tougher consent requirements stand to neutralise the benefits of advertising and the ability to track user behaviour.

A reasonable question to ask is whether users can be relied upon for consent. Users may be technically aware, or, for the more technically aware, they may be sophisticated, however, is that many users are unaware of their rights, and the equal and the sophistication of devices varies considerably, often not providing sufficient levels of control over their data on your website, for example, but not always being saved. Even a browser setting to block third-party cookies or blocking all cookies would not be sufficient if the tracking was done using first-party cookies.

the use of cookies and similar tracking technologies is essential to business. Indeed, tougher consent requirements stand to neutralise the benefits of advertising and the ability to track user behaviour.

built into internet browsers cannot be relied upon for consent. Users may be technically aware, or, for the more technically aware, they may be sophisticated, however, is that many users are unaware of their rights, and the equal and the sophistication of devices varies considerably, often not providing sufficient levels of control over their data on your website, for example, but not always being saved. Even a browser setting to block third-party cookies or blocking all cookies would not be sufficient if the tracking was done using first-party cookies.

S

A

M

P

L

E

S

2. What Do I Need to Do?

The answer to this question depends on the type of cookies you use and for what purpose or purposes (e.g. analytics, advertising, etc.), their functionality (e.g. essential, analytics, etc.), their frequency (e.g. first-party, third-party), their lifespan (e.g. session, persistent), their importance, their security, and their impact on your users. 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, etc.), their functionality (e.g. essential, analytics, etc.), their frequency (e.g. first-party, third-party), their lifespan (e.g. session, persistent), their importance, their security, and their impact on your users. 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 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

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 use your website, and which parts of it they have used (including which links they have followed). As with analytics cookies, targeting cookies enable you to better understand your users, enabling you to make your advertising more relevant to those users' interests. Targeting cookies are often set by third parties.

It is important to know when and how users use your website, and which parts of it they have used (including which links they have followed). As with analytics cookies, targeting cookies enable you to better understand your users, enabling you to make your advertising more relevant to those users' interests. Targeting cookies are often 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, but by third-party services.

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

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

S

2.1.8 Session Cookies

Any of the cookies listed above...

... Session cookies are temporary and only remain on a user's computer until the point at which they visit your website 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 your computer or device, what personal data is being collected, and whether or not they are being used in compliance with the law.

... used by your website, what those cookies are doing, how long they remain on a user's computer, 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, you can provide a list. Alternatively, a number of online tools (see below) can help you identify the cookies used on your website.

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

2.2.2 What Do My Cookies Do?

For each cookie in your list, make a note of what it does. It is important that you are clear about each cookie's function.

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

2.2.3 What Types of Cookies Am I Using?

Going through the list again, identify the type of cookie each is. Refer back to the list above for guidance on what each type of cookie is. Whether it is a persistent or a session cookie, whether it is strictly necessary, for analytics, functionality, or for targeting.

... are at work on your website. Refer back to the list above for guidance on whether each cookie is first or third-party; 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 for the purpose and shorten that lifespan if it seems excessive.

... of 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 for the 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. It is more likely now that data used by cookies is considered to be personal data. The obvious – name, email address, IP address – identifiers qualify under the UK GDPR. However, even an anonymised identifier that does not identify an individual on its own but can be combined with other data and used to identify an individual will be processing personal data and must comply with the requirements of the UK GDPR.

... o and in light of the UK GDPR it is more likely now that data used by cookies is considered to be personal data. In addition to the obvious – name, email address, IP address – and other seemingly anonymous identifiers, even an anonymised identifier that does not identify an individual on its own but can be combined with other data and used to identify an individual will be processing personal data, you will need to 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 (and ensure you are complying fully with the UK GDPR). For third-party cookies, control over their use rests (at least to a point) with the third party. If they are still being used on your website, it is therefore important that you ensure they are also complying with the law.

... ortant, and in addition to obtaining consent, if personal data is involved, it is crucial to ensure you are complying fully with the UK GDPR. For third-party cookies, while control over their use 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 they are also complying with the law.

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 when individuals know what data you have and 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 some knowledge about them. Consider, for example, the information similar to that included above in the

Even if you are only using *strictly necessary* cookies, it is important that users are fully informed about what you are doing with their data. If you have a good reason to hide them, it is worth remembering that all. The general rule is, the more precise the information is to keep things simple; the average user does not possess a high degree of technical knowledge so using plain, forward language in your cookie policy is always advisable. Sometimes it is better to go a little overboard with friendly, approachable language, but this should be done without downplaying the perception that cookies are little more than spyware files (usually) really are.

Your cookie information should explain the functions of the various cookies placed by your website, what data is collected, 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 is important to explain how they benefit the user. Your explanation should be positive and helpful. 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 cookie is good for them, rather than why their refusal to accept them is bad.

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

focuses on transparency. Where cookies are used (and include cookies), it is vital that users are fully informed about what you are doing with it. It is only fair to ask for their informed consent.

It is important that users are fully informed about what cookies are and what they do. Many users will have some knowledge about them. Consider, for example, the information similar to that included above in the

It is important that users are fully informed about what cookies are and what they do. Many users will have some knowledge about them. Consider, for example, the information similar to that included above in the

It is important that users are fully informed about what cookies are and what they do. Many users will have some knowledge about them. Consider, for example, the information similar to that included above in the

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

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

S

2.3.2 Where Should I Put My Info

The key word here is “prominence” and, as we have said, the increased importance of transparency and consent under the new rules means that your privacy policy should be similarly prominent.

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

While it is a matter of taste to a certain extent, the prominence of cookie information from your privacy policy is also important. The increased importance of consent and controls plays a part here. It is a good idea to put your privacy policy and cookie information (or at least the links to them) directly to the cookie section of your privacy policy, for example). Not only does this increase its prominence, but it also makes it easier for non-technical users to find it for.

2.3.3 Consent

Consent is one of the key features of the new rules that have been applied. Implied consent, which has been a popular method of obtaining users’ permission to use cookies, is no longer a valid method prior to the UK GDPR was to provide users with information about cookies and ask them that their continued use of the website will be taken as consent to use cookies. Controls have also been put in place to ensure that implied consent is decidedly inconsistent.

This does not necessarily mean that you must have a control over every single cookie that you wish to use. Strictly necessary cookies are an acceptable. The UK GDPR itself in reality says very little about cookies. The Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR) were focused on such matters.

Can I Rely on Implied Consent?

Implied consent is no longer a valid method in the UK GDPR world. Users must now take some affirmative action in order to consent to the use of cookies. Over, this must take place before any cookies are placed.

Can I Rely on Browser Settings?

This is a difficult question at present. As long as there has been that relying solely on users’ browser settings is not a sufficient method. As we have already been noted, many users do not possess sufficient technical knowledge to adjust their browser settings for genuine consent. This, therefore, makes relying on browser settings for genuine consent a poor idea.

There is nothing, of course, to stop you providing additional advice to your users on how to adjust their browser’s privacy settings. Relying on those settings alone is not recommended.

This is a position that may change under the EU’s proposed ePrivacy Regulation which may impose new rules on the use of web browsers to the extent that, eventually, browser settings will be more consistent. Post-Brexit regulatory alignment between the UK and EU could also lead to similar legislation very similar to the

A

M

P

L

E

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 not acceptable to simply tell users that they have to 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 all items in an online shopping cart. You are expected to allow them to be selective. If, for example, your website has analytics, it is essential to its functionality, but not to your users' interests, or your users' interests. Consider, therefore, breaking your cookies 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 essential, but 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. Consider, for example, marketing preferences. Consider, for example, (where possible) reminding them to update their preferences.

It is undeniable that stricter consent requirements are more onerous for your business, but also for your users. Stricter requirements can often be annoying. However, it is nonetheless 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 easy to find.

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 it is on the Commissioner's part, meaning that it is not currently sufficient.

As already been noted, it is no longer acceptable to simply tell users that they have to accept your cookies. 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 all items in an online shopping cart. You are expected to allow them to be selective. If, for example, your website has analytics, it is essential to its functionality, but not to your users' interests, or your users' interests. Consider, therefore, breaking your cookies 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 essential, but 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. Consider, for example, marketing preferences. Consider, for example, (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. Stricter requirements can often be annoying. However, it is nonetheless 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 easy to find.

S

A

M

P

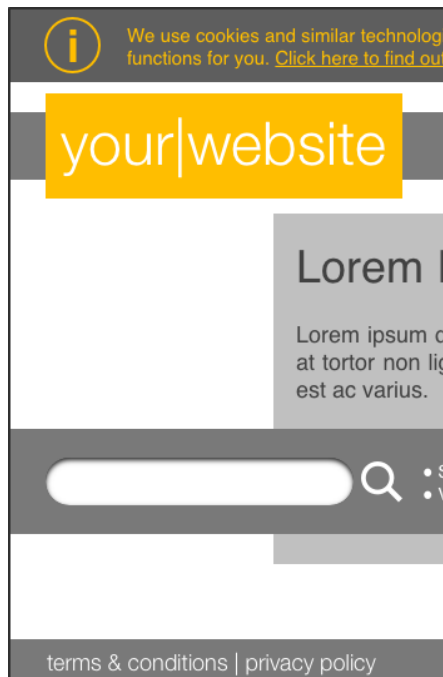
L

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 are more suitable than others, and it is always best to go beyond strictly necessary cookies, you should provide the ability to opt-in or opt-out not only before cookies are set on the user's device, but also at any time after.

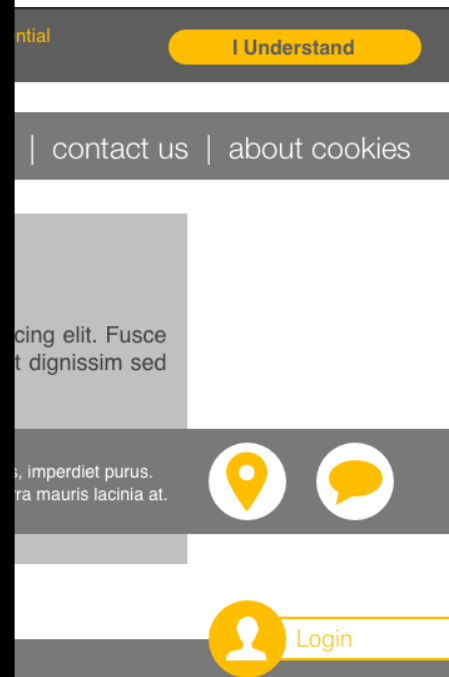
Option 1: Information Banner



This has been one of the most popular options thus far. A simple banner at the top of your (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 providing only information. It is therefore suitable for websites which use strictly necessary cookies alone — those without which the website cannot function correctly for users.

poses you use them for, 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 the ability 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.

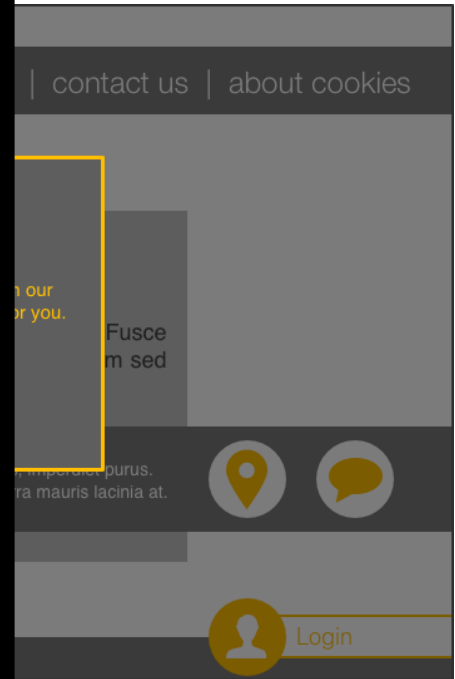
This option does not provide any form of control, but it does provide information which use strictly necessary cookies alone — those without which the website cannot function correctly for users.

S
A
M
P
L
E

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

your website only uses strictly legal compliance.

Option 2: Information Popup



In this scenario, a popup takes information banner. Popups can be users' attention as they require at past them and return to the main button or on an area of the screen website behind the popup could popup.

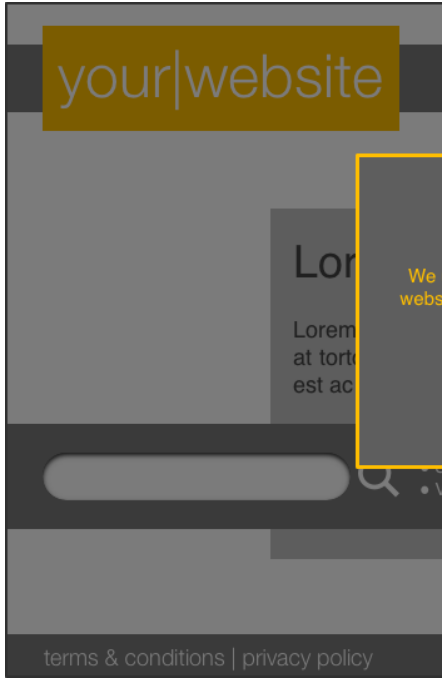
Provides the same details as the banners when it comes to grabbing action from the user in order to get, even if this is only clicking on a's border. In extreme cases, the until the user acknowledges the

As with the information banner, for strictly necessary cookies where y

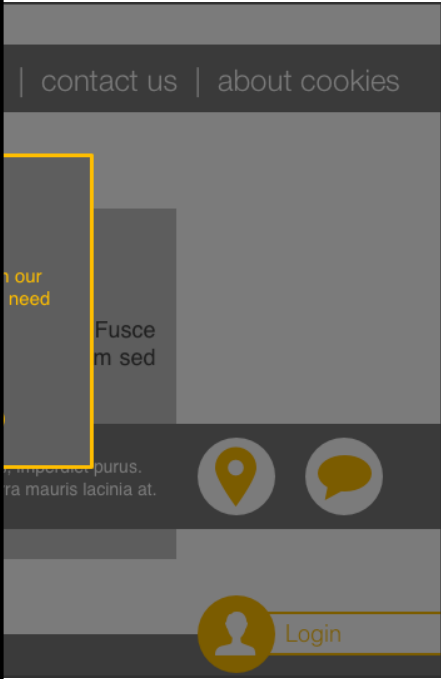
that this option is only suitable for provide controls.

S A M P L E

S



A

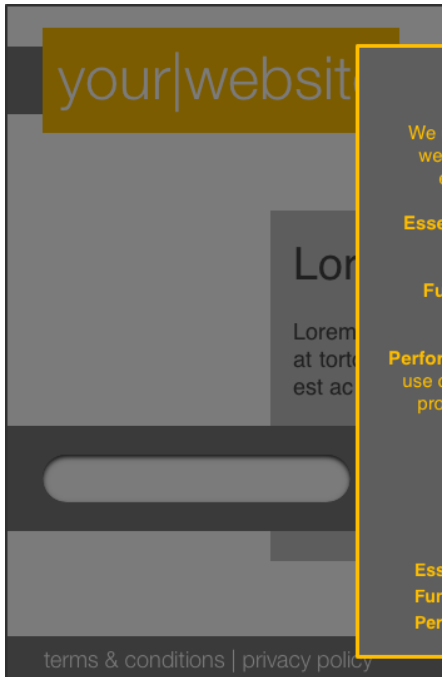


Once again, the popup approach provides a simple opt-in or opt-out choice. However, also as with the information banner, such basic binary controls may often be undesirable.

M

M

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



P



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.

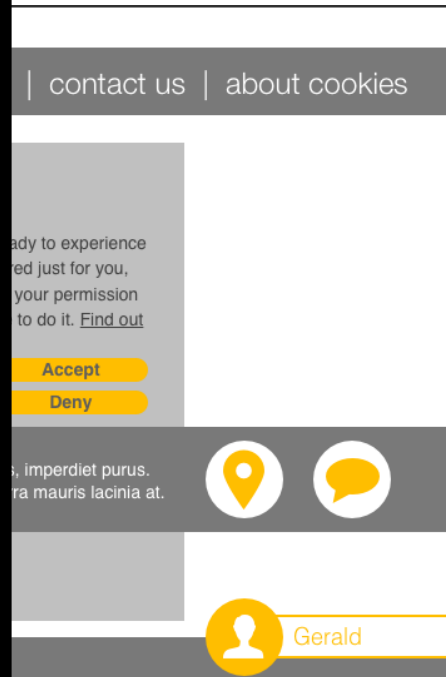
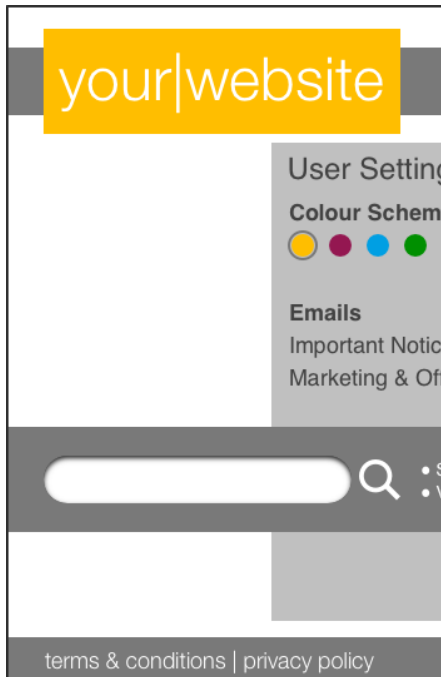
P

L

E

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 has opted in. Information can be provided to users about how to use the relevant features. Despite this, users may not be able to refuse them, even though that may be the case.

Which Option for Me?

There is not necessarily a right answer. It is important to emphasise that user consent to cookies that underpin the vital functions of a website. Consent to cookies before placing them on a device. 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 be achieved if users are given a clear choice.

use cookies from the outset, but users can opt out of non-essential features — personalisation, in this case. At the time that a user wishes to use a feature that may not work without cookies, users may not be able to refuse them, even though that may be the case. If a feature is strictly necessary, users must remain free to refuse them, even though that may be the case.

In this question, however it remains unclear whether some basic, strictly necessary cookies are essential to get users' express consent. In any event, 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 be achieved if users are given a clear choice.

S

A

M

P

L

E

S

3. A Word On Advertising and A

Many analytics and advertising se and similar technologies in orde provided with its own privacy con regulatory programme with hundre up by AdChoices include controls

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

The online advertising and tracking some that the UK GDPR, and th could herald a significant shift in someone’s permission to “track” th

state of flux and it is expected by sis on consent and transparency, work, not least because asking for tising is unlikely to go down well.

Wherever possible, the importanc when a user first arrives on your s at all. At the very least, a detailed users’ activity around your site Analytics, explain the benefits to explain the benefits of allowing be that are more relevant to their inte

be remembered. Placing cookies n after the fact is not true consent n should be provided. If you track ses using, for example, Google f your site serves up advertising, too — namely that users see ads annoying and intrusive.

4. Conclusion

The collective bundle of requirem thorn in the side for website ope came into force in 2011, many particularly complained about c complaint was more down to a la was down to users being happ understand a great deal about th agree” button and continuing to us the scale, with the rise in the av and steps by companies like App by default, many users are quite c or their personal data to any deg your website. Some try to fight a argue that it is perhaps prefera existence rather than trying to di meet with success for long any workarounds).

Law” represents something of a e so called “EU Cookie Law” first e unhappy, arguing that nobody t, however, is that the lack of nderstanding among users than it that many still do not know or clicking the close button or the “I n. Meanwhile, at the other end of of pro-privacy browser extensions ng technologies in their browsers u or your cookies into their system plutely necessary for them to use ser-centric controls, but we would d address the reasons for their rse of action which is unlikely to quently update them to address

The current state of play, it must consent alone is set to make thing interruptions will be necessary to more before getting on with the b again in the future, but for now, t despite such annoyances, have individuals’ rights to privacy and u complying than by resisting.

Indeed, the increased emphasis on site operators and for users. More d users will need to read and do website. Things are set to change should be taken. These rules do, seeking to increase and protect ed, there is more to be gained by

A

M

P

L

E