TOUGH COOKIES

While the value of businesses tracking their website visitors is clear, the law on how to demonstrate the legal basis for this tracking certainly isn't.

It’s important for businesses to strike the right balance: you want to place cookies on as many of your visitors’ devices as possible in order to optimize their experience, but you also must ensure they have provided sufficient consent in the eyes of the law.

So, what are your options?

Well, we’re certainly not lawyers - and the responsibility for implementing tracking consent mechanisms for your visitors rests on your shoulders - but we’ve put together a guide to give our expert opinion and push you in the right direction.

We’ll cover the different types of cookie banners, explain some of the jargon, and lay out what the law says when it comes to consent.

Let’s get started!

Glossary

First thing's first; let's get you clued up about some of the jargon involved in cookie consent.

First party cookies

These cookies can ONLY be placed and read from the website the user is actively visiting. For example, since you've visited canddi.com, information about your browsing activity can only be accessed by canddi.com. This is generally used for website analytics, or to personalize the experience for the visitor.

CANDDi has always used first party tracking exclusively, so our platform isn't in any danger of being affected by upcoming data privacy laws which tend to focus on third-party tracking.

Third party cookies

These cookies can be read across multiple websites. Ever looked at a nice pair of trainers on asos.com, then seen ads for the same trainers on different websites across the web? Third party cookies are how this happens, and have probably wreaked havoc on your wallet over the years.

GDPR

The General Data Protection Regulation (GDPR) is a set of EU regulations which require companies (or any data controller) to be clear about the data they are processing about any data subject.

Since the nation states of the EU implement these laws separately, differing interpretations (especially in regards to what constitutes "informed consent" and "legitimate interest") have led to inconsistencies in the enforcement of GDPR.

The legislation is not (by itself) concerned with tracking, or indeed the actual mechanism of data capture. Rather, it's more concerned about a data subject's (your visitors') ability to access, amend, and control their data, and the legal basis under which a data controller (you) chooses to capture and use this data.

In short: what data are you capturing, and why are you holding it?

PECR

The Privacy and Electronic Communications Regulations is UK law (based off an EU directive) which concern how an organisation can electronically communicate with an individual.

Special category data

Special category data is defined as part of the GDPR. Specifically, it refers to data which is sensitive and should be controlled more carefully.

This includes (but is not limited to) items such as

- Health data
- Criminal convictions
- Data regarding any child aged under 13

GDPR is clear that any Special Category should only be handled with explicit consent.

What does the law say?

At the time of writing (February 2020) there is very little legal guidance regarding what online tracking compliance should look like in practice. In the UK this falls between the following legislations:

- GDPR (https://en.wikipedia.org/wiki/General_Data_Protection_Regulation)
- PECR (https://en.wikipedia.org/wiki/Privacy_and_Electronic_Communications_(EC_Directive)_Regulations_2003)

It's thought that the upcoming ePrivacy Regulation will clear up most of the confusion, however this has been repeatedly pushed back and there is no current date for it's final implementation.

Current references (correct as at Feb 2020) from the ICO:

- ICO guide to cookies
- PECR guidance on cookies
- ICO guide on complying with cookie rules

The PECR states that the user of that terminal equipment

a) Is provided with clear information about the purposes of storage, or access to, that information; and
b) Has given his or her consent

Confusingly, there is no definition given in PECR of what consent actually means. Under GDPR, however, it has the following specific definition:

"any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her"

If you're still wondering just how unclear the law is on all of this, the fact that even the ICO's compliance guide advises you "to look at the methods other online services already use" for inspiration pretty much says it all.

So, let's look at what options are available to you.

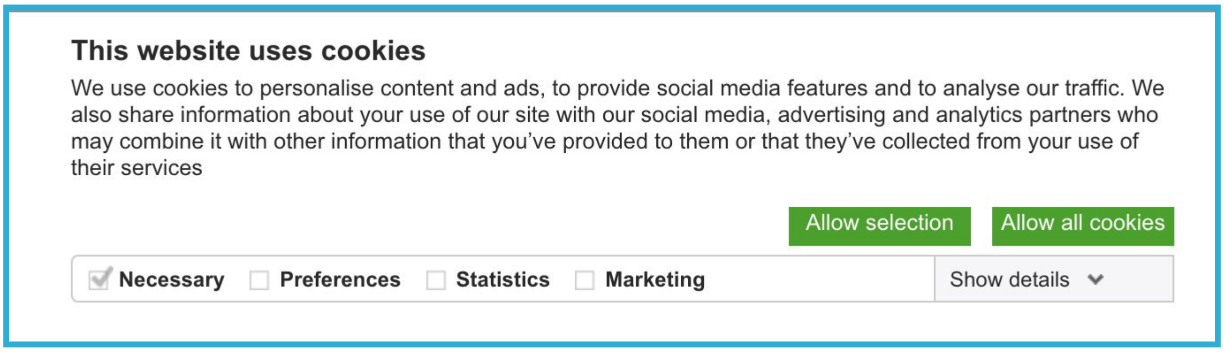
Different types of consent forms

Regardless of the gaps in legislation, one thing is clear: some kind of consent form is required in order to track individuals online.

We believe there are four broad categories of consent forms, for each of which we've provided an example as well as advantages and disadvantages.

Full explicit consent

This is the whiter-than-white approach. The site displays a consent pop-up with all of the tracking options unticked. This means that if the user just simply presses "okay", no tracking will be performed.



This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services

Here is an example from https://www.cookiebot.com/en/:

In this example, nothing is ticked by default. The user has equal ability to select "Allow selection" (no cookies by default) or "Allow all cookies".

Positives

- The website can confirm beyond all doubt that any consent is informed and freely given
- This is a perfect option for special category data which must be handled with extra care

Negatives

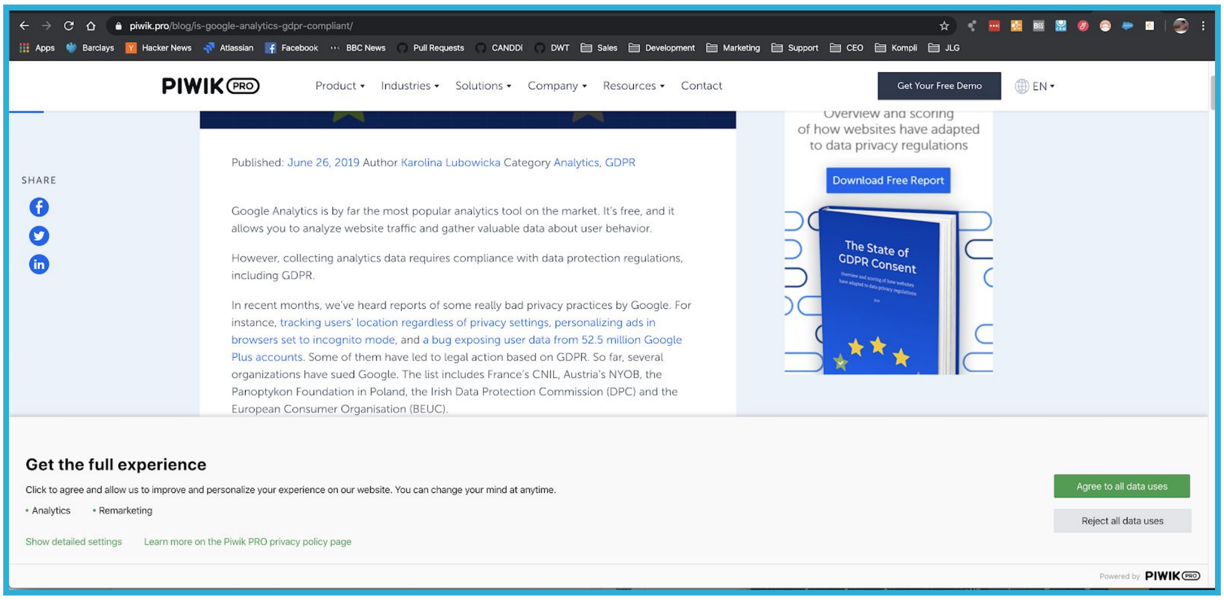
- Users are likely to either be confused, or simply not read the banner and opt for no tracking. This means their activity can not be personalized or tracked, helping neither the visitor or the business.

Full implicit consent

This method provides only two main options: “accept everything” or “reject everything”.

Clearly, the user will be steered towards the green “accept everything” button, though it’s very easy for data-conscious individuals to open up a more detailed interface to explicitly opt in to different types of tracking.

Here is an example from https://piwik.pro/:



Published: June 26, 2019 Author Karolina Lubowicka Category Analytics, GDPR

Google Analytics is by far the most popular analytics tool on the market. It's free, and it allows you to analyze website traffic and gather valuable data about user behavior.

However, collecting analytics data requires compliance with data protection regulations, including GDPR.

In recent months, we've heard reports of some really bad privacy practices by Google. For instance, tracking users' location regardless of privacy settings, personalizing ads in browsers set to incognito mode, and a bug exposing user data from 52.5 million Google Plus accounts. Some of them have led to legal action based on GDPR. So far, several organizations have sued Google. The list includes France's CNIL, Austria's NYOB, the Panoptykon Foundation in Poland, the Irish Data Protection Commission (DPC) and the European Consumer Organisation (BEUC).

Get the full experience

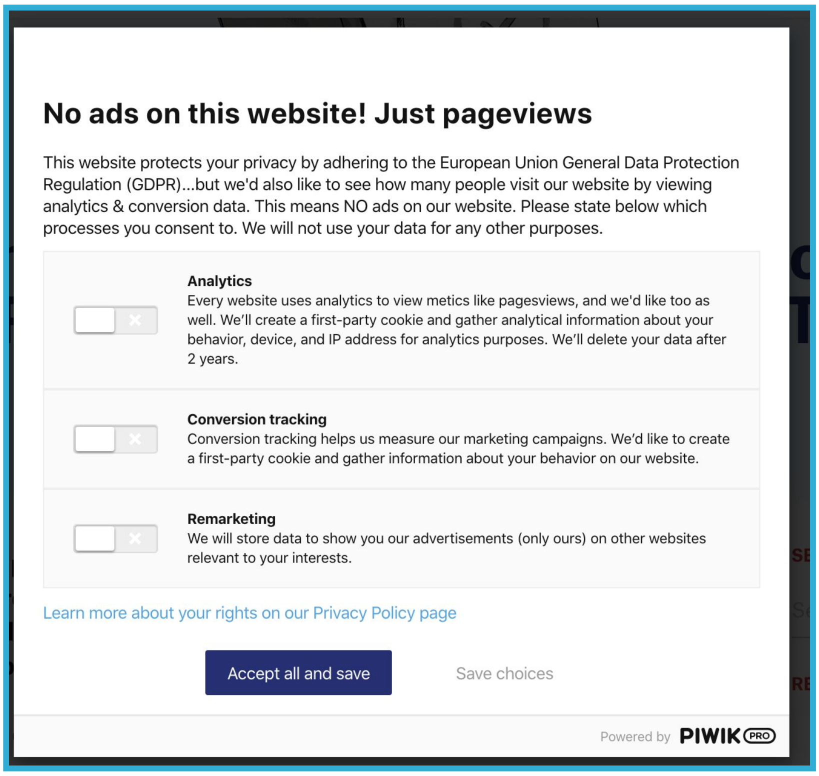
Click to agree and allow us to improve and personalize your experience on our website. You can change your mind at anytime.

- Analytics
- Remarketing

Show detailed settings   Learn more on the Piwik PRO privacy policy page

Agree to all data uses

Reject all data uses



No ads on this website! Just pageviews

This website protects your privacy by adhering to the European Union General Data Protection Regulation (GDPR)...but we'd also like to see how many people visit our website by viewing analytics & conversion data. This means NO ads on our website. Please state below which processes you consent to. We will not use your data for any other purposes.

Analytics
Every website uses analytics to view metics like pagesviews, and we'd like too as well. We'll create a first-party cookie and gather analytical information about your behavior, device, and IP address for analytics purposes. We'll delete your data after 2 years.

Conversion tracking
Conversion tracking helps us measure our marketing campaigns. We'd like to create a first-party cookie and gather information about your behavior on our website.

Remarketing
We will store data to show you our advertisements (only ours) on other websites relevant to your interests.

Learn more about your rights on our Privacy Policy page

The first image shows the initial banner, while the second shows the more detailed window available to those who want it.

Positives

- Provides a privacy-aware user with the ability to select precisely what they want to consent to
- Provides the average user an ability to say yes and get on with browsing the site
- Allows the user to change their preferences at a later time

Negatives

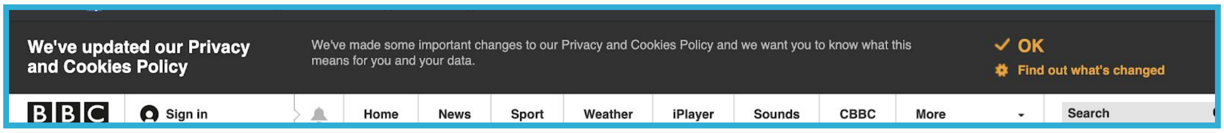
- Since most users will simply click the big green button without fully reading the form, it can be argued that this does not provide explicit informed consent. As such, this isn't suitable for websites which handle special category data.

Aggregate implicit consent with website settings

This option is a little more subtle than the full implicit consent banner.

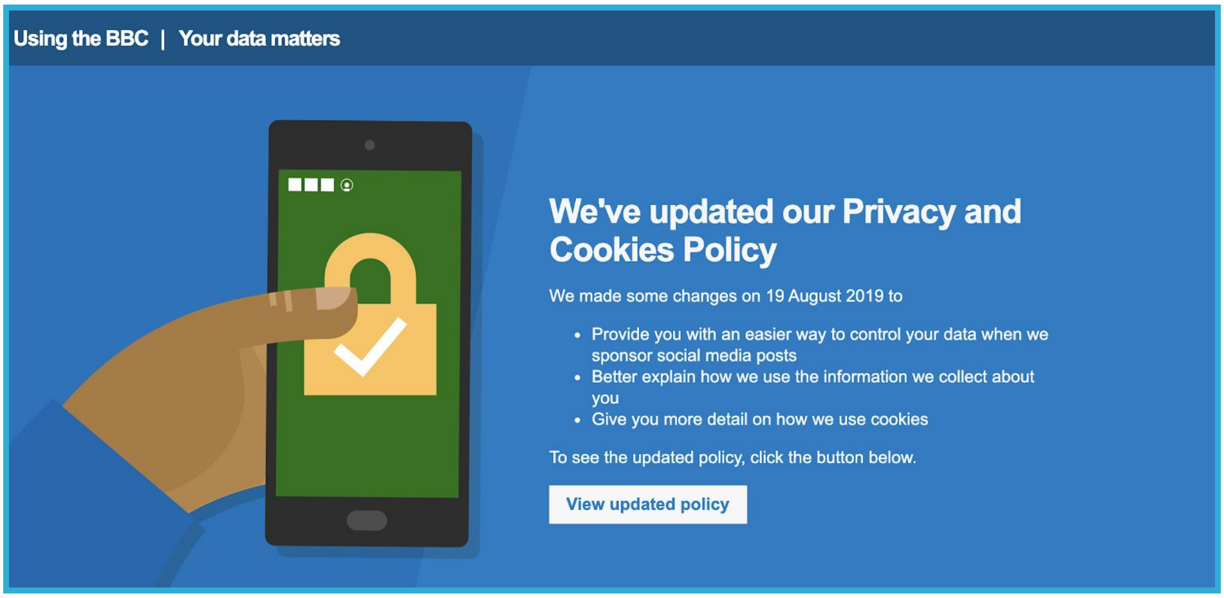
Here, the user simply has an option to say yes; if they want to find out more they can go to a settings page (note: there isn't a "no" option on the main banner).

This is the approach that the BBC takes, as you can see below:



We've updated our Privacy and Cookies Policy

We've made some important changes to our Privacy and Cookies Policy and we want you to know what this means for you and your data.

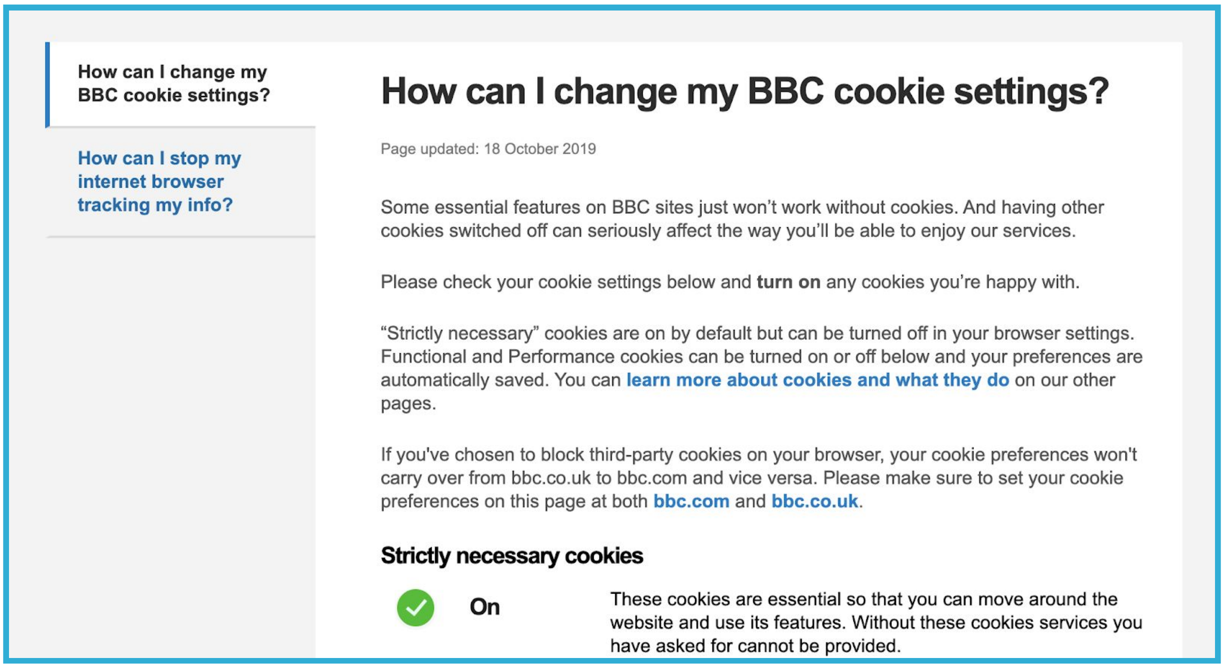


We've updated our Privacy and Cookies Policy

We made some changes on 19 August 2019 to

- Provide you with an easier way to control your data when we sponsor social media posts
- Better explain how we use the information we collect about you
- Give you more detail on how we use cookies

To see the updated policy, click the button below.



How can I change my BBC cookie settings?
How can I stop my internet browser tracking my info?

How can I change my BBC cookie settings?

Page updated: 18 October 2019

Some essential features on BBC sites just won't work without cookies. And having other cookies switched off can seriously affect the way you'll be able to enjoy our services.

Please check your cookie settings below and **turn on** any cookies you're happy with.

"Strictly necessary" cookies are on by default but can be turned off in your browser settings. Functional and Performance cookies can be turned on or off below and your preferences are automatically saved. You can **learn more about cookies and what they do** on our other pages.

If you've chosen to block third-party cookies on your browser, your cookie preferences won't carry over from bbc.co.uk to bbc.com and vice versa. Please make sure to set your cookie preferences on this page at both **bbc.com** and **bbc.co.uk**.

Strictly necessary cookies

✓ On

These cookies are essential so that you can move around the website and use its features. Without these cookies services you have asked for cannot be provided.

It takes three clicks to navigate to the second window. Needless to say, this means it isn't particularly easy to change which tracking you consent to, or indeed to opt-out of the cookies altogether.

Positives

- Very simple for users to opt-in
- Flexible options do exist for privacy-conscious individuals

Negatives

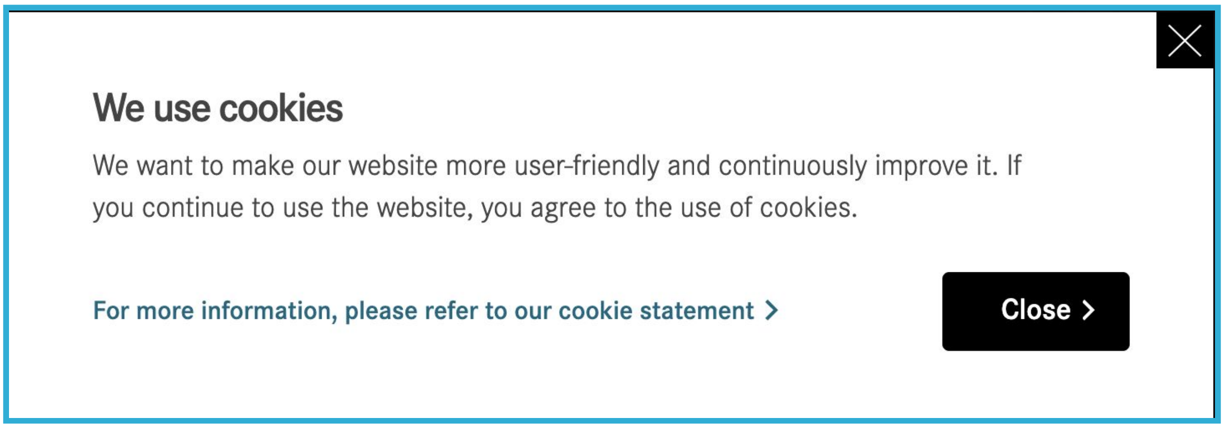
- It can be argued that the relatively hard-to-find options window actually obfuscates the entire consent process. This option is certainly not suitable for websites which handle special category data.

Aggregate implicit consent with browser settings

With this approach, the cookie consent banner contains an "accept" button and appears when the visitor first lands on a website. There is a link to that website's privacy page for those who want to learn more about the nature of the tracking being used.

The key thing to note here is that the only way a visitor can opt out of this tracking is by clearing the cache on their browser.

The below example is from Daimler:

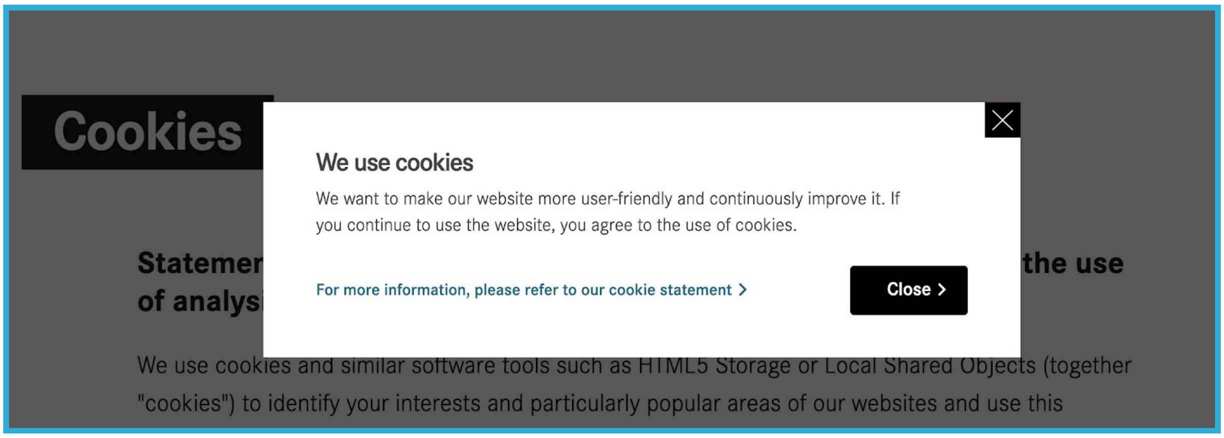


We use cookies

We want to make our website more user-friendly and continuously improve it. If you continue to use the website, you agree to the use of cookies.

For more information, please refer to our cookie statement >

Note: anyone who clicks the option for more information will get sent to Daimler's privacy page, but the banner will not disappear until they click "close".



We use cookies

We want to make our website more user-friendly and continuously improve it. If you continue to use the website, you agree to the use of cookies.

For more information, please refer to our cookie statement >

We use cookies and similar software tools such as HTML5 Storage or Local Shared Objects (together "cookies") to identify your interests and particularly popular areas of our websites and use this

Positives

- Avoids all of the messiness of users having to choose the cookies they want

Negatives

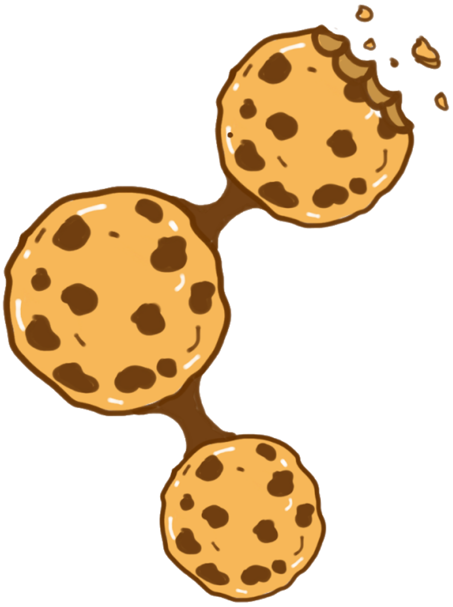
- It would be hard to justify that a user has actually given informed consent. This is especially true if, like Daimler, you force the user to accept before allowing them to access the website.

Other potential risks

So we've established that it's important to be aware of the legal implications of how you choose to acquire tracking consent. But it's also important to be aware of how the technical implementation of this choice can factor in.

For example, a well known consent plugin for wordpress websites was recently found to have a major bug which meant it may not have been correctly capturing users' consent. This not only renders the entire consent process useless, but also opens up websites to data privacy litigation.

What does CANDDi recommend?



Clearly, tracking consent currently exists in what can only be described as a very large and very gray area of the law. As such, it's important that you determine your own approach to gathering consent on your website.

That said, we can certainly recommend that any organisation which processes any form of special category data must obtain full explicit consent.

As for typical B2B businesses, the full explicit consent approach is likely overkill. While it's true that regulations may change in the future, there's no need to prematurely jump to the "whitest" solution possible. We've seen the negative effects of this already, when thousands of B2B organisations destroyed their perfectly viable email lists in the mistaken belief that the then-upcoming GDPR legislation would make them unusable.

Keeping all of this in mind, we'd recommend most of our customers offer aggregate implicit consent with website settings. This balances the interests of the user and the interest of your company, leading to informed consent which benefits both parties and improves the relationship between them.