osano

Cookie Consent Management

Frequently Asked Questions

Introduction

Cookie consent matters. As just one EU country operating with the GDPR and ePrivacy Directive, France used the latter to fine Google and Facebook $170 million and $86 million, respectively, for dropping tracking cookies without consent. This can be confusing because both companies have cookie banners, but France found that their cookie banners were deceptive and didn't allow users to opt out easily enough.

You might be thinking: But that's Google and Facebook! Who's going to pay attention to my little website? In 2021, GDPR-related fines and penalties from data protection authorities within the EU totaled more than $1 billion. And much of that total came from small businesses and individuals. Small size does not preclude receiving a fine.

Also, because it is relatively easy to add cookie consent management to websites, many companies are choosing to add the functionality regardless of whether they are likely to catch the eye of regulators or suffer fines. Especially since everyone else is putting up cookie banners, few companies want to look like outliers.

But there is much more to cookies and consent than just a simple web banner. That's why we've compiled a list of answers to some of the most frequently asked questions we get about cookie consent management: We're here to help you get the information you need about this important topic.

What is a cookie?

A cookie is a small text file that websites pass to your computer through your web browser. Its purpose is to extend the website's functionality and create a better user experience, usually through personalization, session management, and tracking. A cookie might save user inputs, shopping carts, login information, or wish lists. It can also be used for advertising and analytics.

To learn more about how cookies work, watch this short video.

What is cookie consent?

The concept of cookie consent is pretty simple: Before your website places a cookie on a visitor's device, you must get permission. That way, you are always getting authorization and consent for any collection of personal information that might occur when a cookie is dropped onto a user's device and begins communicating back to your website.

However, it's not always that easy in practice, depending on what visitors to your website expect to do. Some cookies are necessary for making your website function correctly, while others are employed explicitly to track users and market to them more effectively. If you only have one binary option — "yes" to cookies or "no" to cookies — you might alienate users who want to use your website but are uncomfortable being tracked.

If you don't ask at all, you run the risk of being reported to some global regulatory agency — or a state's attorney general — if a user can tell that a cookie has been set and is collecting information without their consent.

The best option is to allow them to choose which cookies are OK and which are not. You can allow users to do this every time they visit your site, or you can allow them to set up a profile or otherwise remember their preferences for future visits. This requires some consent management.

What is cookie consent management?

As the term implies, “consent management” allows users to manage their consent to your website when they visit. Via the use of cookies or the creation of a profile, and often with a little of both, users can tell you which cookies they’ll allow you to drop and which they object to, and then your website can remember those preferences when they return for future visits.

This provides benefits to both the user and you, the website operator.

For the user, they don’t have to click an annoying button again every time they visit your website, and they can be confident they are experiencing your website in a way that makes them comfortable.

For you, not only are you assured that visitors to your website are comfortable with the cookies you are setting on their devices, but you also have a record to show to regulators should anyone come to them complaining about your site. You can demonstrate that you have allowed users to manage their consent, and you have the records to prove it.

Further, consent management can go well beyond just cookies! Users might want to manage the consent surrounding your use of their email address, location data, browsing habits, or any number of pieces of personal information they might provide to your website.

While it’s theoretically possible your organization could build a process for this from scratch, coding all of the functionality yourself, most organizations use some kind of consent management platform sold by a third-party vendor (like Osano).

What is a cookie consent management platform?

Consent management platforms come with a range of functionality, but, in general, they ask users of your website for permission to collect and use their personal information.

Some consent management platforms might only manage consent around cookies. Some might only manage consent around email addresses (these are the "unsubscribe" services you're no doubt familiar with). And generally, the pricing for such software rises and falls with the feature set.

The most robust of these consent management platforms collect consent on every kind of personal information a person might provide to your organization — including your employees' information, information supplied to you in a job application, or information supplied to you in the creation of a customer account, etc.

All of them perform the same basic service: they create an account for each user, track the information you have about that user, and track the consent you have attached to each piece of information. For example, a basic file might look something like this:

John Smith

- **Cookies:** Accept all.
- **Email:** Receives Email newsletter. No marketing emails allowed.
- **Phone number:** OK to call about account. No sales calls.
- **Location:** Never OK to track location.
- **Browsing History:** OK to track browsing history on site to suggest other products.
- **Search History:** Never OK to store search history.

With this consent management in place, your organization should know how to interact with John Smith and be confident in avoiding privacy violations.

As you get more sophisticated in privacy and consent management, you'll see that there are rules around how you collect consent based on the type of information you're collecting, where the user is living, and many more variables. As just one example, pre-checked boxes that a user has to uncheck to opt out are not acceptable in many places. And it is not OK in many jurisdictions to deny service to a user if they do not provide consent for personal data collection.

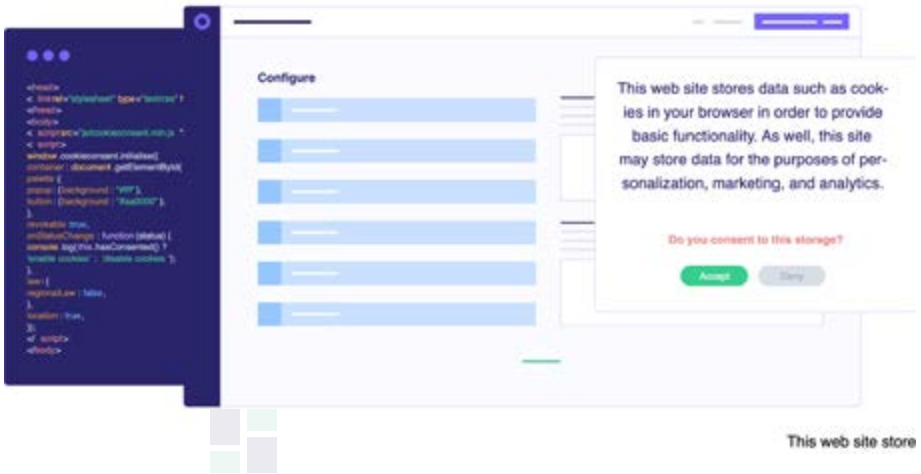
It's important to consult with lawyers specializing in the privacy field if you have specific questions about the laws surrounding consent and the collection your organization would like to do. However, many consent management platforms (including Osano) come with helpful information about laws and regulations or have consultancy as part of their product offering.

What is cookie consent program?

A cookie consent program is simply a simplified consent management program that only looks at the way your organization handles consent related to cookies. Because cookies are sometimes regulated separately from other forms of personal information — in the EU, for example, the GDPR regulates data protection as a whole, but the ePrivacy Directive regulates cookies specifically — it can be helpful to have a separate management program that looks just at cookies.

Also, because cookies are actively placed on users' devices and aren't just related to the collection of information, it can be helpful to have software designed specifically to deal with the regulation of which cookies are placed on which users' machines.
This program will separate cookies into categories, allow users to make choices based on the category of cookie and then make sure to either remember those selections when a user returns or ask for consent if encountering what it perceives as a new user.

A good cookie consent program and implementation should make this process as unobtrusive as possible and try not to give users a negative first impression of the website.



How do you set up a cookie consent program?

A relatively large industry of cookie consent management solutions has sprung up in the last decade or so, responding to the need to comply with brand-new or developing privacy laws around the world. While it is possible to code a solution on your own, and your IT or infosec teams might offer to make it happen, it's unlikely they will be able to provide something that meets the industry's current standards.

These software solutions will have a variety of ways they go about implementation, but many of them are as simple as inserting a bit of code in the header of your website's pages. The "out-of-the-box" solution is often enough to keep you compliant with the law and at least cover the bases if you feel you are behind and don't yet have a strategic approach.

However, most solutions will allow you to tailor your user experience and decide what you will let users select. Every organization defines what "cookies required for website functionality" actually means, for example, and you might decide you want other categories of cookies beyond simply "functionality," "tracking," and "third-party," which are the standard buckets with which people generally begin.

By working with your privacy compliance team, your IT team, your marketing team, and anyone else who might be involved (including people like UX developers and others), you should be able to analyze your risk tolerance, your compliance obligations, and your necessary functionality to come to an agreement on the user experience you'd like to deliver.

Then, it should be a relatively simple matter of configuring the software to match your preferences.

How do you add a cookie consent pop-up to your website?

In terms of the actual implementation, cookie consent management software (like Osano) should be a relatively light lift. You simply add some code to your website headers and then log into a cloud-based account where you can configure the shape, color, and text that users will encounter when they visit.

When shopping for software that fits your cookie consent management needs, the range of options you have for the user experience may be one of your points of differentiation. While functionality is important, you don't want a visual experience that detracts from your branding and overall aesthetic.

Also, while just about every site these days has third-party cookies that exist because of plug-ins for social media integration, video players, and other web features, not every cookie-consent solution automatically scans for them and blocks them by default until users make the choice to allow them.

How do users revoke their consent?

Many jurisdictions require that users be able to revoke their consent for you to collect and process their personal data at any time. Your cookie consent management platform should allow users to change their preferences at any time. That change of preference should trigger the deletion of the cookies on their device or give them directions for clearing their cookies.

If your management platform has data discovery functionality, it may also be able to keep a record across multiple databases where collected personal information has been stored or moved for easier information deletion.

Regardless, if a user expresses that they no longer want their browsing habits tracked across sites, for example, you will need to be able to identify that user in your database and delete the information you have stored about them.

How your cookie consent platform manages that can mean the difference between a lot of manual labor and relatively simple automation.

How do I comply with the GDPR's cookie consent?

Technically, the GDPR (the General Data Protection Regulation in the European Union) does not solely regulate cookies. Much of that power is held by the ePrivacy Directive, also known as the Cookie Directive.

However, they work in tandem, and the details aren't overly important. While the Cookie Directive governs the actual placement and removal of the cookies from user devices, the use of the personal data gathered via cookies is governed by the GDPR.

Suppose you are simply using cookies that make your website function, and you don't gather any explicit personal information about your users through the use of cookies. In that case, the GDPR technically won't apply to your use of cookies — but you will be subject to the GDPR for other collection of personal information if you have employees or users in the EU, simply by the fact of them filling out paperwork and buying things from you.

If you are collecting significant amounts of personal information from people in the EU, you should have someone whose job it is — either external counsel or an internal professional like a Data Protection Officer — to examine how you collect and use that data and make sure that you are compliant with the law. If you are not the DPO, you should be collaborating with the DPO (or making sure you have one, if you are subject to the GDPR).

From a cookie perspective, though, which law is in play doesn't really matter. If you're dealing with people who live in Europe on a regular basis, you should make sure you are not placing cookies on their machines before they consent to it, other than the most basic of functionality cookies that allow the site to perform its basic purpose.

You will likely be compliant in the European Union (disclaimer: we're not lawyers!) if you do the following:

- ✔ Get consent before you drop cookies other than purely functional ones.
- ✔ Explain in plain language what every cookie does at the point where you're asking for consent.
- ✔ Keep a record of that consent.
- ✔ Don't make consenting to the cookies necessary for using the site.
- ✔ Allow users to easily withdraw their consent if they want.

But I'm in the US! Why should I add cookie consent to my site?

For most US websites, adding a cookie consent banner is mostly a case of following that old adage: Better safe than sorry. With many US states and countries around the world passing new privacy laws, and the difficulty of knowing where visitors to your website are coming from, companies across the United States are taking steps to make sure they have permission to collect personal information before they collect it.

Cookies are often a way that companies collect personal information, sometimes without people understanding how much or how often. And many new privacy laws issue harsh penalties for collecting personal information without permission.

For example, California's Consumer Privacy Act (aka the CCPA) and the European Union's General Data Protection Regulation (the GDPR) and "ePrivacy Directive" strictly regulate the collection of personal information. If you don't follow the rules, California can impose fines of up to $2,500 per violation – $7,500 if proven you intentionally ignored the law.

When should I ask for tracking consent and show the cookie policy?

With all cookies that are "optional" — i.e., not necessary for the basic performance of the website — it's best to get consent before placing them on a user's device. While consent is only strictly necessary if the user is residing in California or in a variety of locations outside the United States, privacy laws move at a rapid pace, and it can be difficult to know from where your users are coming.

For third-party tracking cookies, or your own cookies that may track what a user does or what other sites they might visit after leaving your site, the risk is a little higher, as that information can get "sensitive" and thus reach a higher risk level for collecting, should users visit medical sites or other web pages that indicate they're in a protected class.

For these sorts of tracking cookies, best practice is starting to move toward opt-in consent prior to placing them on a device and explaining what they do while you ask for that consent. That's certainly the way it is in the GDPR.

However, it's still true that many companies operating in the United States and unworried about the EU collect these all under an "I agree" button that doesn't necessarily explain every cookie that's being placed unless a user clicks through for more information. It remains to be seen whether that fully satisfies California's evolving privacy laws.

You should consult with your team and potentially legal counsel to see what's right for you.

How to update a cookie list for GDPR cookie consent?

Regarding cookies and the GDPR, you should have two lists:

1. A list of every cookie you're placing on a machine, how the cookie is categorized, and a description of what that cookie actually does. This is usually in a table that users can quickly access right from where they are being asked for consent.

2. A list of every user who has consented to the placement of cookies. You have this to prove to anyone who asks that you do, indeed, have consent and supply it to a user if they ask. It also makes it possible for that user to revoke their consent easily in the future. This list might not actually have names, etc., but may simply be a list of IP addresses or unique identifiers that you can link to a device. In many ways, unless you need the name information or other data, having less personal information provides you with less risk.

   With a cookie management platform like Osano, this should be relatively automated. If you are creating a bespoke solution, this can be a fairly large amount of manual work.

   If you are subject to the GDPR, your Data Protection Officer likely oversees this effort.

How to update a cookie list for GDPR cookie consent?

A list of people and the consent that they have provided to you can, itself, be considered personal information. Therefore, your consent list should be protected like any other personal data.

- ✔ Access to the list should be limited to those who need to access the information.
- ✔ The list should be encrypted at rest and require a username and password to access, at a minimum.
- ✔ The list should be regularly updated to make sure that data you no longer need (such as consent that has expired) is deleted.
- ✔ The list should allow you to access it and delete data upon request by the user.
- ✔ The list should allow you to easily produce a record of consent for a user upon request or proof of consent for all of your users upon request by a government regulator.

If you are using a consent management platform like Osano, this is maintained as part of the platform's abilities.

What happens if I don't use a cookie consent policy on my website?

The answer to this depends on the answers to many other questions:

- Do the users of your website come from the European Union, California, or other areas of the world that have privacy laws in place that govern the use of cookies and the collection of consent?
- Is your company large enough, or do the sorts of business with sensitive data that would trigger the requirements of certain privacy laws?
- Are you placing cookies that collect large amounts of personal data, or do the cookies simply make it so your website works right?
- Would your users be surprised — or annoyed! — if they found out the cookies you were dropping on their devices were collecting their personal information or tracking their behavior?

If your users are in the EU, your cookies collect sensitive data, and your users would be upset enough about it to contact their privacy regulator, some very bad things could happen, indeed. The EU can fine you up to 4% of your overall revenue for the year and even force you to stop collecting information altogether.

If your users are in California and you're found to have willfully failed to get consent, they can fine you up to $7,500 for every visitor to your site.

Every business plan and risk appetite will be different; if you're concerned about consequences, you should err on the side of caution and collect consent or consult with an industry-specific attorney who can advise you on your best course of action.

Why use Osano?

Osano provides the most popular cookie consent management application in the world, with over 750,000 active deployments.

We're here to help you implement top-notch privacy compliance wither you're a privacy expert or new to privacy and just looking to protect your organization.

We'll help you:

- Comply with 40+ privacy laws with 1 line of JavaScript
- Show the correct language and cookie banner automatically
- Log every consent via 1-way encryption in our private quantum ledger
- Keep DSARs secure and compliant with a dedicated messaging portal
- Sleep soundly protected by the industry's only No Fines, No Penalties Pledge

To see Osano in action

Schedule a Demo

or visit www.osano.com for more information.