

# Your 7-Step Cookie Governance Checklist

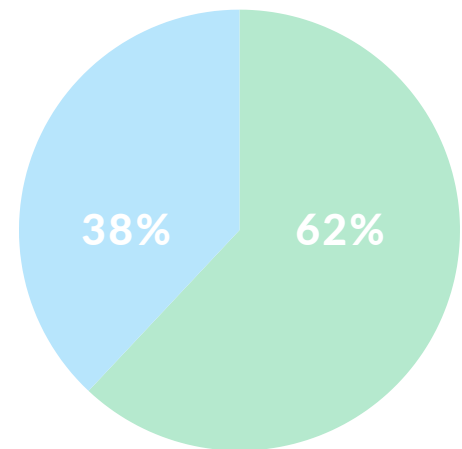
Good cookie governance is what differentiates the inefficient from the efficient when it comes to cookie consent management. Once you master the cookie governance lifecycle, many downstream compliance activities become much, much easier. In this article, we'll walk you through the steps to robust cookie governance.

## 1. Submit a New Cookie Request

In organizations with poor cookie governance, this step is usually skipped. Nobody “requests” to add new cookies to the site; they just go ahead and do it. That can cause a whole lot of problems down the line with consent management, privacy notices, subject rights requests, and more. Ideally, you should have a standardized procedure for receiving new cookie requests.

New cookie requests will typically come from internal stakeholders, such as members of the marketing or development teams. Sometimes, such a request might come from third-party service providers and vendors,

as well. Cookie requests should include information on the purpose of the cookie, the types of data it will collect, the intended duration of storage, and other criteria as needed. If the cookie is associated with a new vendor, you'll also want to conduct a thorough risk assessment.



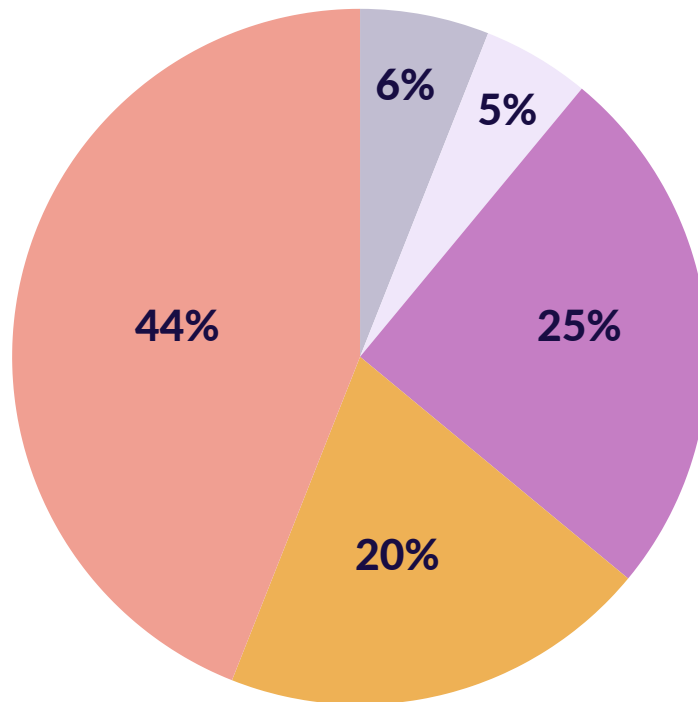
Sixty-two percent of survey respondents use automated methods for cookie consent/discovery scanning as opposed to manual methods. (Source: IAPP-EY 2023).

## 2. Conduct a Privacy Impact Assessment

If the cookie request is associated with a new vendor or if substantially changes how your organization collects and processes personal data, you'll want to conduct a privacy impact assessment (PIA).

PIAs help you determine the impact that a data processing activity will have on consumer privacy and data protection rights. A PIA in this circumstance should take into account the type of data collected, the purpose of collection, and the risks associated. Not only does this exercise help you identify when a vendor and/or cookie presents unacceptable compliance risk, but it also provides documentation proving that you were accountable for your data privacy compliance obligations.

■ Not Required   ■ Not Performed   ■ Ad Hoc  
■ Regularly Conducted, But Triggers Undefined  
■ Regularly Conducted Based on Established Triggers



Frequency at which respondents conducted PIAs. Respondents either were not required to conduct PIAs (6%), did not perform PIAs regularly (5%), conducted PIAs on an ad hoc basis (25%), conducted them regularly but without defined triggers such as the addition of a new cookie (20%), or conducted them regularly based on triggers such as the introduction of a new cookie (44%; Source: IAPP-EY 2023).

The biggest challenge associated with this step is often a lack of resources. Make sure you familiarize yourself with the privacy assessment process before you need to conduct an assessment, so you're not scrambling to meet deadlines when the time comes. Often, data privacy platforms will include automated and streamlined assessment workflows to help you speed up and scale the assessment process, too.

### 3. Add Cookie to Staging Environment

Next, you'll want to add the cookie to your website staging environment—this allows you to verify its functionality without affecting the live site.

Depending on the nature of the cookie, you might test to see if it's collecting the appropriate information, if it fires or is blocked based on user consent preferences, or if it interferes with the functionality of any other scripts or cookies when it fires or is blocked.

At this stage, you'll also want to make sure it's accurately classified in your consent management solution, whether that's a homegrown approach, an integration with your tag manager, or a consent management platform (CMP). Since certain jurisdictions require businesses to provide consumers with granular control over which categories of data trackers they consent to, you'll need to define whether the cookie is essential or for marketing, analytics, or advertising purposes.

## 4. Add Cookie to Production Environment

Once any issues have been identified and resolved, you can move your cookie to the production site. It's always a good idea to monitor your site for problems following any changes you make.

## 5. Update Your Record of Processing Activities/Data

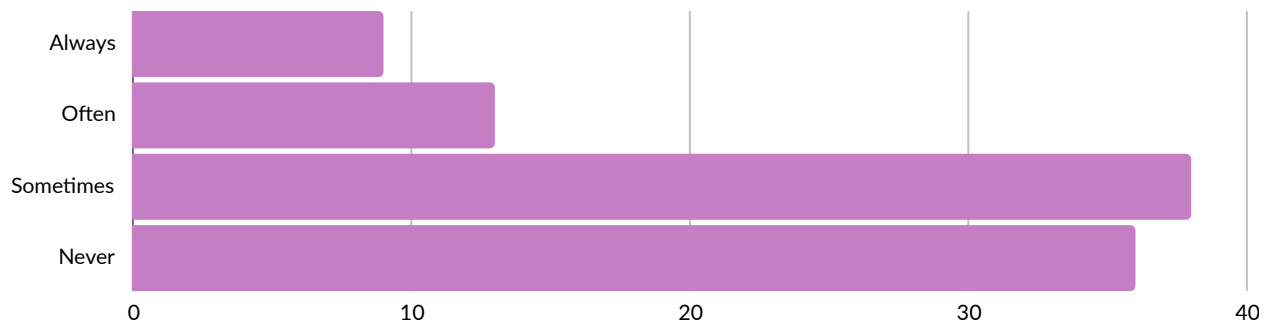
If you're subject to the GDPR, then you're required to maintain a Record of Processing Activities (RoPA). However, even if you aren't subject to the GDPR, then creating a RoPA or an equivalent data inventory will make it many times easier to demonstrate and maintain compliance.

RoPAs and data inventories document details about processing activities, such as what information your new cookie collects, how long that data is retained, and where it transfers that data. Much of this information should have been included in the initial cookie request, but you may need to do some work to identify relevant cookie details.

Creating a RoPA and/or data inventory from scratch can be tricky if done manually. Automated tools for data mapping and inventory can significantly accelerate this process.

## 6. Update Disclosures and Policies

Since website users are now being actively tracked by the new cookie, you need to make sure your public-facing documents reflect this tracking behavior. It could be that the specific data privacy law you're subject to and the category of cookie you've used don't require any updates; in that case, great! However, it's still a best practice to check your privacy and cookie policies for accuracy.



Percentages of respondents who say they always, often, sometimes, or never read privacy policies before agreeing to them. (Source: Pew Research, 2019).

This step can feel like a frustrating bottleneck, especially if the responsibility associated with your policies and website cookies is split across your legal, compliance, and technical teams. After all, the legal department probably doesn't want just anybody to make changes to the website's privacy policy, but they're usually too busy to make the change immediately. To address this, Osano developed TrustHub, which gives privacy professionals control over multiple privacy documents in one centralized location.

## 7. Conduct Ongoing Maintenance

Cookies and other data trackers can't be something you set and forget. Conduct regular reviews of your vendor relationships on at least an annual basis to ensure their cookies still function as initially intended. This step in the cookie governance lifecycle also includes real-time monitoring for any security concerns, like data breaches; have there been any affected systems that store or process user data collected by one of your cookies?

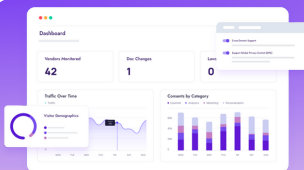
Your organization might become subject to new laws with new requirements as well. If you've produced the documentation that the previous steps required, then you'll be well on your way to confirming that you are compliant or making the necessary adjustments to get there.

## Automate for Efficient Compliance

While this process is achievable with a manual solution, it can easily become an untenable amount of work. Since cookie governance isn't explicitly required by data privacy regulations, then it becomes tempting to let this whole process slip. Ultimately, that will result in the proliferation of cookies on your website whose functions you don't understand or that you don't even need in the first place. That leads to a slower website, less transparency for your consumers, and noncompliance.

Data privacy platforms can help automate many aspects of the cookie governance process. With Osano, you can:

- Search through a database of 11,000+ vendors and their associated Privacy Scores, so you can identify high-risk or trustworthy vendors at a glance.
- Scan for and discover cookies on your website.
- Categorize cookies based on automatic recommendations for regulatory compliance.
- Update privacy documents from one centralized location.
- Streamline and automate privacy impact assessments.
- Map and discover stores of consumer data throughout your organization.
- Generate RoPAs.
- And more.



## Book a Demo of Osano!

### About Osano

Osano is a complete data privacy platform trusted by thousands of organizations around the world. Its platform simplifies compliance for complex data privacy laws such as GDPR, CCPA, LGPD, and more. Features include consent management, subject rights management, data discovery, and vendor risk monitoring. Osano is the most popular cookie compliance solution in the world, used on over 900,000 websites to capture consent for more than 2.5 billion monthly visitors.