

AN ENTERPRISE GUIDE TO TRACKER LIST CURATION

What it is, why it matters, and how to review
the cookies, trackers and third-party
technologies on your properties and website

sourcepoint.com



TABLE OF CONTENTS

2	Introduction
4	Part One Privacy Compliance: You are who you work with
9	Part Two Tracker impact on web performance: The customer experience and your bottom line
13	Part Three Trackers and brand trust: Doing well by doing good
16	Part Four Tracker assessment scorecard
17	Part Five Frequently asked questions, best practices & tips
19	Conclusion

TRACKER AND COOKIE CURATION IS MORE IMPORTANT THAN YOU THINK

You want to create a seamless user experience for people visiting your website while ensuring you're maximizing customer experience and marketing opportunities—all while putting consumer data privacy first. And like any other enterprise, you're working with a robust stack of technology partners and utilizing tracking technologies like pixels and cookies to make it all happen.

Balancing all of these objectives is not an easy task.

But did you know that these technology partners (especially your partners' partners you're not aware of—more on that later!) can pose a serious threat to your business? In a world where privacy is top of mind for consumers, you can't afford to leave yourself vulnerable to things like data leakage, non-compliance, and reputational risk.

This is why we created this guide to help you navigate the process of deep cookie, tracker and vendor assessments. When you conduct regular automated assessments, you will:

- Have a better understanding of the partners you are working with
- Know what types of cookies, trackers, and technologies are working behind the scenes on your site
- Stay on top of regulatory data privacy requirements and identify compliance gaps
- Improve the overall performance of your website

Contrary to what you might assume, more trackers is usually not better. By looking at the on-site behaviors of trackers to curate and reduce the amount of technology partners on your list, you'll see a tangible benefit to your bottom line. Keep reading to learn how conducting tracker and vendor assessments positively impacts compliance, website performance, and brand reputation.



WHAT IS DATA LEAKAGE?

Data leakage is a lot more common than you may realize, and it can cause revenue loss as well as compliance risk. It occurs any time data is shared from one source to an external destination or recipient. Unauthorized third-party cookies or vendors can tap into your audience data when authorized vendors trigger them and pull data that helps them build audience segments based on your users without even compensating you for the information.

This can erode trust with your audience, cause you to miss out on revenue opportunities, and potentially put you at risk of being non-compliant with global data privacy regulations.

Learn how Sourcepoint's Diagnose insights platform can help prevent data leakage.

PRIVACY COMPLIANCE: YOU ARE WHO YOU WORK WITH

In the ever-shifting landscape of privacy compliance, it's not enough to make sure that you are adhering to the various legislative regulations and industry frameworks. Everyone you partner with, every vendor that your partners share your data with, is required to meet the same standards to ensure compliance.

Sure, you can decide which third-party technologies you want on your site, but what about their partners? These unknown vendors could access your site without you even realizing it. Not only is the unknown putting you at risk for non-compliance, but it's also potentially leaving monetization opportunities on the table.

So, how can you be sure your site and your partners are adhering to data privacy laws? There are myriad privacy regulations impacting global compliance today, from the California Consumer Privacy Act to the LGPD (the Brazilian privacy national law), and more on the way, but for this guide, we'll focus on the European Union **General Protection Regulation (GDPR)**, since it's the most mature regulation. Many aspects of the GDPR have been incorporated into subsequent regulations — not to mention it is applicable around the world.



DOES THE GDPR MATTER IF MY BUSINESS IS OUTSIDE OF THE EU?



The short answer is yes. Your headquarters location is irrelevant if your digital properties are attracting traffic from EU residents. In this scenario, you're not only exposing your business to risk by being non-compliant, but you're also potentially missing out on customer engagement and ad revenue.

The GDPR was a significant turning point for how personal data is handled online but left enterprises, publishers, agencies, and vendors concerned about becoming and remaining compliant. Shortly after the GDPR was announced, the Interactive Advertising Bureau launched the **IAB Europe Transparency and Consent Framework (TCF)** to standardize the industry approach to GDPR. This collaborative effort included the IAB Europe, IAB Tech lab members, and the digital advertising industry at large.

What's the TCF?

The IAB's TCF framework has become the dominant GDPR standard for the digital media ecosystem. It helps coordinate all the different players by outlining exactly what information publishers need to communicate to users, including identifying what data is being collected, how vendors intend to use it, and who the vendors are. Consent Management Platforms (CMP) that want to utilize the TCF must undergo a validation process, but utilizing the TCF is not a guarantee of GDPR compliance. Likewise, vendors who want to participate in the TCF must register with the IAB's Global Vendor List (GVL). The GVL is composed of a list of vendors that work with publishers and advertisers and who have agreed to utilize the TCF's consent string, but it's not a guarantee of GDPR compliance. Some free or "freemium" TCF CMPs only allow publishers to utilize the entire GVL — all 700+ vendors — without the ability to modify it.

Google Consent Mode and how a Consent Mode Partner can help

Another turning point in consent and how personal data is handled is happening now in 2024. Google introduced the Google EU User Consent Policy in 2015, that required marketers advertising with Google to obtain and respect an end-user's consent due to two European privacy regulations, the General Data Protection Regulation (GDPR) and the ePrivacy Directive (ePD). Now in 2024, Google is expanding it to cover its audience and measurement platforms, so that it can maintain ad visibility in the European Economic Area (EEA). As a result, app and web advertisers who do business in the EEA need to enable Consent Mode.

Google recommends working with a certified Google CMP Partner to properly enable and manage Consent Mode. A Google CMP Partner can assist your enterprise with:

- Implementing or upgrading your website / app consent banner
- Managing your consent banner content
- Passing the consent signals back to Google to provide verifiable consent for conversion measurement and audience targeting

Google CMP Partners, like Sourcepoint, offer solutions and software for handling consent mode, responsibly sharing your consent data with Google while maintaining your important advertising goals, and managing your consumers' consent and data privacy effectively.



SOURCEPOINT IS A GOOGLE CMP PARTNER

Google CMP Partners can help you build your cookie consent banners, manage your consumers' consent and data privacy from the first moment that interact with your apps, websites and consent banners, and responsibly direct consent mode mode to Google without interrupting or compromising your advertising.

Sourcepoint is a Google CMP Partner. **Contact us or request a demo** for help with Google Consent Mode, data privacy and consent management.

Compliance is dynamic

The GDPR and Google Consent Mode is only the beginning. There's also the **California Consumer Privacy Act** (plus more than 15 U.S. state privacy laws as of this writing), federal U.S. laws, the Brazilian law, Canadian laws – with many other countries drafting their own. It can be overwhelming to keep track of these requirements on top of everything else you're doing to ensure your website is compliant and efficiently generating customer engagement and revenue.

Frameworks are helpful, but you're still on the hook for checking up on changes to the frameworks and the lists of registered vendors. A tool like Sourcepoint Diagnose simplifies the process by surfacing all of the data you need in one place to better understand your site's data privacy health compared to industry benchmarks.

And you're probably wondering, what's at stake if you're non-compliant? Well, besides the potential for missed revenue opportunities, there is also the possibility of fines. Non-compliance with GDPR can cost you up to €20 million (\$24.1 million) or 4% of annual global turnover (whichever is higher). It is dependent on the severity of the infringement. Non-compliance in the U.S. has also proven to be costly for enterprises. Whether European or in the U.S., businesses are on the hook for fines and penalties related to non-compliance.

For example, in 2023, BetterHelp, the online counseling app banned from sharing personally private and sensitive health data to third-parties and Facebook for advertising, and ordered to refund customer \$7.8 million by the U.S. Federal Trade Commission (FTC). The year before, in 2022, Fortnite video game maker Epic Games was fined a massive \$275 million penalty for violating children's privacy laws and ordered to change its default privacy settings due to violations with the U.S. COPPA, the Children's Online Privacy Protection Act. And this is only in the U.S., large fines and settlements have been levied on companies doing business in Europe and the EEA.

No Consent = A Missed Opportunity

Beyond non-compliance, if there's a vendor processing data on your website and you're not collecting consent for them, you could be potentially missing out on an additional source of revenue—more about that in PART TWO: Tracker Impact on web performance.

PART ONE SUMMARY

Privacy Compliance

3

- Regulatory compliance is not only your responsibility, but you must ensure all the trackers, partners and vendors processing your consumer data are compliant as well.
 - Failure to monitor your sites and understand on-page tracker and vendor behavior not only puts you at risk — it can impact your customer engagement and ability to monetize your site.
 - Data privacy regulatory compliance is a moving target. Without the support of a diagnostic tool, it's challenging to ensure that all the trackers and cookies on your properties, apps and website are up-to-date on compliance.
-

PART TWO:

TRACKER IMPACT ON WEB PERFORMANCE: THE CUSTOMER EXPERIENCE AND YOUR BOTTOM LINE

The performance of your website is paramount to the success of your overall business. It's a bit of a slippery slope—a poorly performing website will rank lower in Google Search and, in turn, limits the audience size associated with your site, which can then reduce engagement.

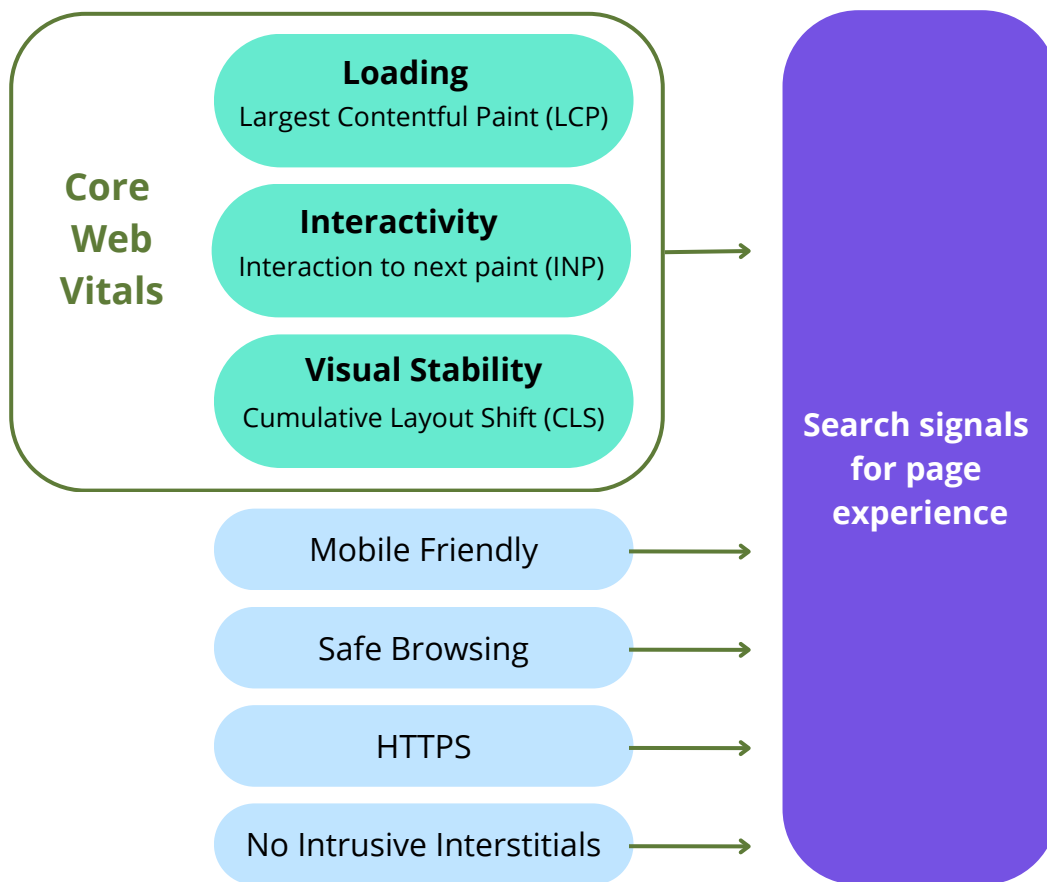
So, what can an enterprise do to prevent this slip? One factor that should be top of mind is Google's Core Web Vitals.



WHAT ARE GOOGLE'S CORE WEB VITALS?

In late 2020 Google announced a new set of webpage experience signals related to speed, responsiveness, and visual stability that directly impact Google Search rankings. According to Google:

- LCP: Your page's main content should load in 2.5 seconds or fewer
- INP: Your page should become interactive in less than 200 milliseconds
- CLS: Layout shift of the visual page content should be less than 0.1



A great place to start working on improving your Core Web Vitals is to focus on your tracker and cookie list. Every technology you include in your stack adds stress to your site and brings its own compliance risk with no guarantee that the tracker technology is even delivering value.

This means you need to be selective about who you add to your site to ensure you aren't negatively impacting your site's performance. Some initial questions to ask when evaluating the impact of the trackers on your website performance include:

- Who exactly are you working with?
- What triggers, cookies, or tags are they firing behind the scenes on your website?
- Are these trackers providing value for your business, or are they detracting value by contributing to a poor website experience?

It can be tempting to assume that you'd be reducing your ability to drive engagement and revenue if you got rid of some of your trackers. You may even think non-allowed indirect or downstream vendors are providing additional revenue opportunities, which would be great, but if you're not collecting consent for them and don't have a commercial agreement, you're not going to see any benefit. The good news is, when done correctly, this is not the case. The key is to use a data-driven approach to refining your tracker list.

By removing trackers that didn't meet their privacy compliance standards or were inactive, one global media brand we recently worked with reduced their tracker and cookie list by 18% and improved their Core Web Vitals across all properties. And they achieved all of this without negatively impacting their revenue. In the end, they were able to prove the removed vendors weren't providing value, and their audience enjoyed an improved site experience.

PART TWO SUMMARY

Tracker impact on web performance

- The performance of your web pages may be negatively impacting your customer engagement and ability to monetize your site effectively.
- Cookie and tracker behavior can impact Google's Core Web Vitals, a set of performance signals that now directly influence your search engine rankings.
- Every tracker technology you work with impacts your web performance and opens you up to potential compliance risks, so you need to focus on who you partner with and how they are either adding or detracting value.

PART THREE:

TRACKERS AND BRAND TRUST: DOING WELL BY DOING GOOD

In a world where data breaches are becoming more common, consumers are increasingly aware of the information they are sharing online, which means you need to ensure data privacy standards are being met across all consumer touchpoints.

Your brand reputation is more important than ever, and a large part of that is impacted by who you work with. Every vendor running cookies, tags, and scripts on your site's back end can impact consumer trust. One unethical vendor or offhand use of a third-party pixel by you and your teams can affect your brand and its reputation.

For example, in 2022 and 2023, several large enterprises saw the effect of their offhand use of a tracking pixel. The FTC used the 1988 Video Privacy Protection Act (VPPA) to file alleged violations against enterprises sharing identifiable information and video viewing history through the Meta (Facebook) tracking pixel without user consent. Among the companies that faced potential lawsuits were online news outlets like the Boston Globe which settled for \$4MM, retail brands like Home Depot, and even the fast food chain Chick-fil-A. It's fairly common for enterprise websites to employ third-party technologies to track user behavior, and it's also common for websites to feature video content. But in these cases, the combination made for a wide range of potential targets for VPPA class actions from the FTC. The casual use of a tracking pixel and video content led to unwanted outcomes and potential damage to brand reputation.

It's vital for organizations to understand what tracking technologies are being used on its websites and apps, whether trackers exist on pages with video content, and whether information is collected that could be used to identify individual users in connection with the videos viewership. If conditions like this are met, your organization could be open to risk.

Consumers are awakening to the importance of data privacy

According to Cisco, a staggering 84% of consumers say they want more control over how their data is being used. At the same time, a recent Pew Research Center survey finds that 79% of Americans are concerned about how companies are using their data. It's clear that data privacy is top of mind for consumers, and they have become more proactive about finding out what personal data is out there and where it is being tracked and used.

There are so many tools readily available to help educate consumers about the third-party tools accessing their data while running in the background of their favorite sites and apps. Browser extensions like Privacy Badger and The Markup's Black Light tool all work to show consumers all the ad trackers, third-party cookies, and pixels actively running behind the scenes. With Privacy Badger, consumers can also proactively block these third parties from accessing their data.

Enterprises are at a critical point with consumer trust. You can't afford to turn a blind eye to the third parties accessing your web visitors' data. Without a regular review of the trackers, cookies, and pixels running on your site, you put your brand's reputation at risk and jeopardize the trust of your audience.

At a time when first-party data is more valuable than ever, you need to be vigilant about protecting those relationships.

PART THREE SUMMARY

Cookies, trackers and brand trust

- Your revenue depends on building direct and transparent relationships with consumers.
 - By potentially allowing unscrupulous trackers access to data from your site, you're exposing your business to significant regulatory and reputational risk.
 - Consumers are more empowered to take ownership of how downstream technologies and third parties are accessing their personal data on the sites they visit.
-

TRACKER ASSESSMENT SCORECARD

Without a regularly scheduled review of your cookie and tracker list, you don't have a clear understanding of the level of data vulnerability on your site. Third parties are the biggest source of risk for your business, and it's important to know who you are working with directly and indirectly so you can keep your business protected from bad actors.

Take a look at the questions below to understand some of the criteria you need to consider when evaluating vendors processing consumer data on your pages.

☐	Do they have servers in the same country as you or does the data go to a country that does not offer the same level of protection?
☐	Does the provider adhere to the principle of data minimization or do they use permanent cookies with an excessively long lifespan?
☐	Does the provider use intrusive JavaScript methods to create a fingerprint of the device without the user being able to deactivate this processing via an opt-out?
☐	How prevalent is this vendor across your vertical?
☐	What is the error rate for requests from this vendor?
☐	What is their average response time?
☐	What kind of fees do they charge?
☐	Do they offer support?

FREQUENTLY ASKED QUESTIONS, BEST PRACTICES AND TIPS

Below are some frequently asked questions, best practices, and tips to help you perform more effective assessments.

- **How often should I review my tracker and cookie list?**

Outside of changes to privacy frameworks and legislation, reviewing your list on a quarterly basis is a good baseline as it gives you several months' worth of data.

- **Do I need to evaluate my list when privacy frameworks are updated?**

It is good to get in the habit of reviewing your list whenever there are legislative changes to privacy regulations. The goal is to ensure that you are all up-to-date on any changes to privacy frameworks and that they properly require consent when needed.

- **Use data to make informed decisions.**

It's easy to get lost in the tiny details of every vendor on your list. There are tools available to help you visualize the information you need to know to effectively evaluate whether a tracker provides value (or detracts value) for your business.

- **How many vendors should I work with?**

When it comes to your trackers and vendors it is not a one-size-fits-all scenario, but it largely depends on the type of enterprise you are, your industry, your business model and most importantly, your legal and data privacy posture. What is imperative is to ensure that you only work with the necessary vendors that add value to your business and match with your web and data privacy goals, most notably those trackers and vendors you and the business have audited and have a strong relationship with.

- **When should I start working with an insights platform to evaluate vendors?**

While it is possible to evaluate your vendors on a regular basis manually, it can be very time-consuming and inefficient. Using a scanning tool like Sourcepoint's **Diagnose insights platform**, you can easily access a more comprehensive view of all triggered cookies, trackers, and technologies on your site. Not only do you have a view of who has the first point of access, but you also gain insight into the partners of your vendors that may be accessing data from your site without working with you directly. The more data and information you have, the better-informed decisions you can make for your business.

CONCLUSION

Congrats. You now have the knowledge you need to implement an effective, data- driven review of your vendors.

Remember:

- Regulatory compliance is not only your responsibility, but you have to ensure all third-party and downstream trackers and cookies you're working with are compliant as well.
- Every tracker you work with impacts your web performance and opens you up to potential compliance risks, so you need to focus on who you partner with and how they are either adding or detracting value.
- Consumers are more empowered to take ownership of how third parties access their consent and privacy data on the sites they visit. Ensure the vendors you are working with don't break the trust between you and your site visitors.

Ready to take your tracker list curation to the next level? **[Request a demo](#)** of Sourcepoint's Diagnose solution today.

ABOUT SOURCEPOINT

Sourcepoint is the practical data privacy software company trusted by the world's most influential brands. Supporting over 30 billion consumer touchpoints per month, Sourcepoint offers enterprise-grade privacy automation for complex, dynamic compliance challenges.

Sourcepoint has offices in New York, Berlin, and London.

Learn more at sourcepoint.com.