

9 Point Website Privacy Audit

A Guide for Monitoring Customer Data Collection on Your Website



As more companies adopt Consent Management Platforms (CMP) and other technologies or processes to comply with regional data privacy laws, a periodic audit of your website data privacy efforts is essential to prevent natural entropy and verify that you are staying on top of compliance.

The 9 points explored in this tip sheet are designed to help you answer the question: Can you trust the technologies and policies you employ on your site to stay in place, function properly, and keep you in compliance?

Use the following points to ensure you're not only acquiring your customers' consent but validating that you are truly honoring their consent, as well as auditing all data collection points to ensure ongoing website privacy beyond consent management.

Many of these activities can be performed automatically by using a digital governance solution like ObservePoint. In the Feature Highlights and italicized text, we'll show you how ObservePoint can automate many of these crucial audit checkpoints for you.

1. Tag & Cookie Inventory

Before you can begin monitoring your website privacy, you'll need a comprehensive data discovery audit to understand exactly what data collection technologies are deployed, what cookies are being set, and what customer data they're collecting.

Most likely, you have data collection technology installed on every page and cookies being dropped upon entry—and depending on how large your digital property is, that could mean hundreds, even millions, of data collection points.

You can identify technology and cookie presence manually page-by-page, but given the scope of hundreds or thousands of pages with dozens of data collection technologies, it's a nearly impossible task to accomplish once, let alone to monitor regularly, but it is necessary to protect your customers' data and prevent data leaks

Audits

ObservePoint has powerful, scalable Audits that enable you to quickly scan a large batch of pages on a regular basis. Companies like Adobe, PepsiCo, and Hewlett Packard Enterprise use ObservePoint's Audits to regularly scan their site and discover which technologies are gathering what data. Using an Audit, you can easily verify which technologies are installed on each page of your site and who's on the receiving end of that data. Set up recurring Audits to compare changes in approved and unapproved technologies and cookies over time.

TAG NAME	TAG CATEGORY	PAGES TAGGED	PAGES NOT TAGGED
 Google Analytics 4	Analytics	1,784	610
 Google Global Site	Tag Management	1,784	610
 Google Optimize	Experience Management	170	2,224
 Google Tag Manager	Tag Management	1,789	605

2. Data Collection Triggers

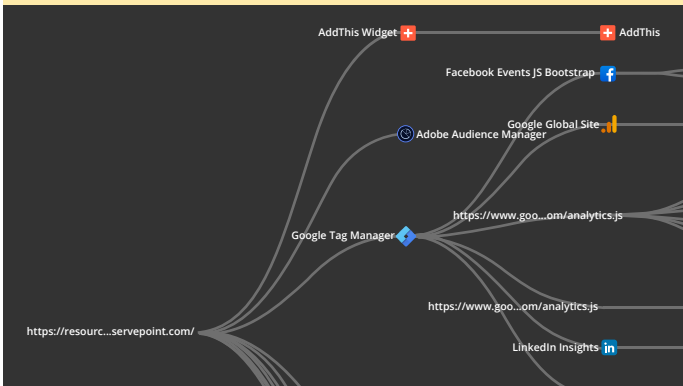
Consent Management Platforms like OneTrust, Quantcast, TrustArc, and others integrate with your Tag Management System to collect user consent and trigger data collection based on their preferences. What you'll need to look out for are any hard-coded or unapproved piggybacking tags that aren't deployed by your TMS because those will not be detected by your CMP, nor your TMS for that matter.

And trust us, piggybacking and hard-coded tags are more common than you might think. Ad agencies or third-party vendors can often have piggybacking tags related to media placements, and it's common for old technologies that were coded into a web page to be hanging around and passing data from your site years later.

Once you identify these tags or data collection technologies, you can decide what action to take, whether to investigate their sources further, delete them, or move them into your TMS so your team and your CMP can control them.

Tag Initiators

Tag Initiators from ObservePoint illustrate the relationship of the cookies and technologies present on every page of your site in a simple, visual flowchart. Quickly see which tags are being delivered by your TMS and discover any that are unexpected or unauthorized. Have a clear picture of what technologies are initiating which data collection activities. Tag Initiators is helpful in both data discovery and data mapping.



3. Consent Acquisition

It's helpful to think of your CMP or home-grown consent acquisition tools and cookie banners as the first conversion point, where you are acquiring your customer's consent to give them more information. This is a pivotal requirement in many data privacy regulations; however, consent management technologies are not infallible.

As with any digital implementation, they are subject to human error and entropy. Website updates can inadvertently affect the CMP installation, and every possible entry point into your website must have cookie banner coverage to ensure compliance. Your team needs to perform regular tests, especially after any website changes, to ensure these acquisition points are up and running continually, preventing you from accidentally tracking users without consent.

Audits

ObservePoint looks out for the particular pain points that CMPs present in an automated way. You can monitor your CMP implementation by making sure it's installed on every page of your site by running an Audit. You'll be able to see if your implementation was incomplete or if there are parts of your site that are managed by other partners who may not have a CMP installed.

PAGES MISSING TAGS (BY ACCOUNT)	PAGES WITH TAGS (BY ACCOUNT) ↓
5%	95%
6%	94%
6%	94%
6%	94%
14%	86%

4. Consent Validation

An important part of quality assurance for your consent acquisition points or CMP is to make sure that consent preferences are actually being honored after they are specified. As mentioned in the previous step, consent management implementations have to be deployed and monitored for performance like any other software solution.

Once you have acquired your customers' consent, you'll need to test traveling through your site or app with that customer's consent preferences to make sure cookies are not being placed at the wrong time by accident. With how much is at risk for not honoring these preferences, you need to test and confirm the consent management technologies your company is investing in are actually reducing your risk of liability.

Consent Categories & Journeys

ObservePoint's Consent Categories were developed just for this purpose. It allows you to define standards for which tags, cookies, request domains, and geolocations should be approved or unapproved under various states of user consent. Then you can set up Journeys (simulated user sessions) with those consent profiles to verify if data is being collected without the proper consent or sent to unapproved destinations.

Consent Categories ⓘ
CATEGORY NAME TYPE

Approve All Cookies	Approved
Deny All Cookies	Unapproved
Required and Analytics Only	Unapproved
Required and Performance Only	Approved

5. Data Transfers & Geolocation Monitoring

With more and more data protection laws coming online, the physical location of data collected from your customers has become an important compliance issue, so you need to be monitoring the destination and storage location of your customers' data. The GDPR only allows data collected from EU citizens to be sent to other countries with the same level of consumer protection.

Do you know where your data is going? Are you sure? What about your third-party technology partners deployed on your site? Where are they sending it? You need to know each data collection point, who is collecting that data, and where they are sending it. Ignorance is no excuse.

Technology Geolocation

ObservePoint can help you identify and record the geolocation of all network requests with a quick visual of where your data is being sent. You can also get reports of any geolocations you didn't specify as acceptable and get notifications when they pop up.



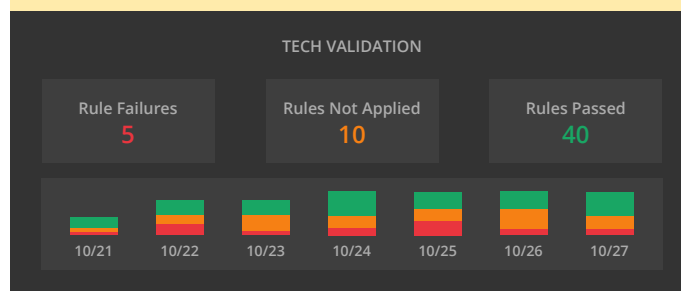
6. PII Detection

GDPR and other regulations require that organizations collecting personally identifiable information (PII) must notify consumers of what they're using it for, keep the data encrypted, and comply with requests for deletion from consumers.

You should know exactly where on your site or app you're collecting PII, via forms or other user experiences, to monitor what customer information you're gathering and how you are securing that data. You'll also want to ensure you're not inadvertently passing PII to Google, Adobe Analytics, or another technology. Most vendors have policies that prohibit the sending of PII. Check with your website team and vendors to verify that no such transmission is happening and remain compliant.

Rules

You can set up Rules in an Audit to test for approved and unapproved data collection technologies. Using ObservePoint's Rules with RegEx pattern matching, you can check for transmission of PII (such as emails and identification numbers), unauthorized technologies, or proprietary data, and receive alerts if any unauthorized data collection occurs.



7. Privacy Policy Presence

Data protection laws like GDPR, CCPA, and LGPD require that specific and transparent privacy policies are accessible to your site visitors from every page. Don't stumble on one of the simplest steps of compliance. As with your consent acquisition, you should be regularly testing that your privacy policy is accessible from every entry point.

It's also a good idea to check your privacy policy verbiage as many regulations state that the language should be concise and intelligible. The objective is to be clear about what information is being collected and for what purposes it will be used. Huge fines have been levied against companies for having vague privacy policies that did not clarify their intended use of collected data.

Rules

You can create a custom Rule to confirm that your privacy policy page is always available and accessible. You can run this Rule in regularly scheduled Audits and configure reports to alert you if anything is amiss.

Rule Name

Privacy Policy Present

Add Labels

less x + label

Labels

less

Validate rule 1 times per action/page

☒ Send Notification(s)

8. JavaScript Errors

Websites rely on JavaScript to function; however, JavaScript files can be edited by anyone who has access to the site's code. Unauthorized or accidental JS file changes can put you at risk of data leakage, hefty fines, and loss of credibility.

Do you know what third-party JS files are on your site and who can edit them? It's a best practice to have your team monitor your website JavaScript for changes and errors, malicious or inadvertent, to reduce the risk of interference with your privacy efforts.

JavaScript File Changes Report

ObservePoint scans your site to give you a complete inventory of first and third-party JavaScript files. You can also monitor changes over time and get alerts when JS files are added or removed.

Pages Scanned	Changed Files	New Files	
1	4	6	
FILE NAME	FILE DOMAIN	1st/3rd PARTY	CHANGE TYPE
vtt.global.min.js	vjs.zencdn.net	3rd Party	No Change
e6554cc1-7dba-45fe-82...	www.chubb.com	1st Party	New File
www.widgettapi.js	www.youtube.com	3rd Party	New File
index.min.js	players.brightcove.net	3rd Party	New File
1906d04b-3e66-4e76-b...	www.chubb.com	1st Party	New File

9. Possible Data Leakage

Nearly all of the above points can lead to issues of data being passed inappropriately. Any organization with a digital presence has faced, is facing, or will soon face more than one of these challenges. No one is immune. For many companies, the new regulations of the last few years have led them to perform audits and consider website privacy for the first time. And, they're discovering several of these weak points at once but are not sure what to do about them.

Consult with your website teams to see how they're currently addressing each of these points to identify where possible data leakage can occur. If during an audit of your privacy efforts, you uncover unauthorized tracking technologies on your site sending data to third parties, that's a red flag you need to investigate further and immediately.

Comparison Reports & Notifications

We've already discussed Audits enabling you to know what's on your site, but you can also schedule regular Audits to run and send you notifications when any new, unauthorized data collection occurs. These are called Comparison Reports, and you can configure approved/unapproved lists for data collection technologies, see changes over time, and get alerts when new technologies are found.

Tag Name	Differences	Pages Count
 Adobe Analytics	No tag presence changes were found.	100
 Google Tag Manager	2 TAG FEWER THAN PREVIOUS RUN	5
	NO CHANGE	94
	2 NEW TAGS FOUND	1
 Google Analytics	No tag presence changes were found.	100
 Google Universal Analytics	No tag presence changes were found.	100

Expedite & Automate Your Website Privacy Audit with ObservePoint

Clearly, a thorough website privacy audit is a significant undertaking and one with a short shelf life at that. With multiple teams constantly updating your code, entropy degrading software implementations, and new tracking technology cropping up, you can only trust the quality of your data as far back as validated by your last audit.

Of course, the problem is that for most enterprise websites, a page-by-page audit is nearly impossible to execute manually, which is why automation is so important. Ongoing, automated audits help maintain trust in your CMP and other data collection technologies on your digital properties, reducing the burden on the teams responsible for data privacy.

ObservePoint's automated solution for Privacy Compliance can help. Schedule a demo with an ObservePoint representative to learn more.

SCHEDULE DEMO