

TRUE or FALSE ?

Website Data Privacy

Common assumptions you can't afford to make.



If you have a privacy policy, a "Do Not Sell My Info" link, and a cookie consent banner on your footer, you'll be compliant with GDPR, CCPA, and other regulations.

FALSE

While you SHOULD have these consent policies and tools accessible on your footer, what you need to confirm is that they are accessible to users coming to your site from EVERY possible entry point. Footers might not be on every single page of your site or the wrong template might've been used to build a page. Not having notices on every page is one of the easiest ways to get fined.


California fined Sephora \$1.2M for failing to disclose to customers that it was selling their personal information.*

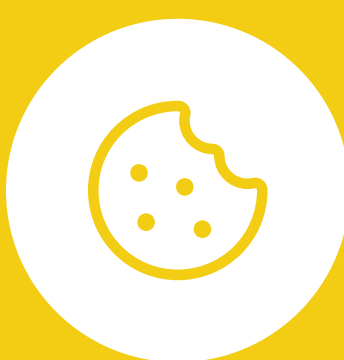
France fined Amazon €35M for dropping cookies automatically without prior consent.*

If you have a Consent Management Platform, you're all set regarding privacy regulations.

FALSE

Consent Management Platforms (CMP) are just the beginning of staying compliant. While they are the best tools to manage your visitors' preferences, you also need to verify those preferences are actually being honored with third-party validation. Implementation errors and Tag Management System blindspots can mean cookies are dropped inadvertently without user consent.





A CMP will show me all tags and cookies on my site, including when and where new/unapproved data collection technologies appear.

FALSE

A CMP can provide deduped lists of your current cookies; however, they don't provide detailed, contextual information like where the cookies are on your site, what information they're collecting, and where they're sending that data. They also don't alert you to new technologies that might be added to your site and have not been approved, putting you at risk for data collection violations.


30-40% of sites audited by ObservePoint have severely flawed CMP implementations.*

By 2024, nearly 75% of the world's population will be governed by some kind of data privacy law.*

If I have servers in Europe, then I don't have to worry about geolocations for GDPR.

FALSE

You'll still need to monitor network requests from third parties to make sure your data isn't being sent to countries that are not on your approved list. New partners or piggybacking tags could be sending data to locations you won't be aware of if you don't check regularly. GDPR requires that customers' data is sent and processed in other countries only if they have the same level of consumer protection.





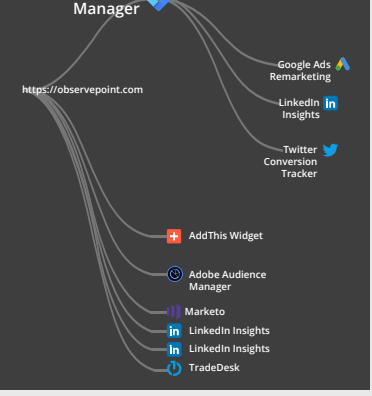
Changes to the JavaScript files on your website are not a big deal.

TRUE **FALSE**

If you've made them.

If other teams or unknown third parties have access and are making changes to your code without your knowledge. Unchecked JS changes or those made by third parties put your data at risk and can result in data leakage or theft.



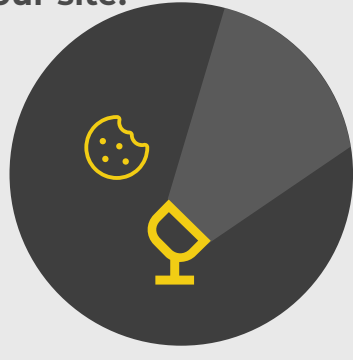


A CMP can see and check all data collection on your site.

FALSE

A CMP relies on your Tag Management System as its source of truth for cookies and tags. If you have hard-coded or piggybacking tags, the TMS won't notice them, which means the CMP will not properly see or classify them.

Tags are often found loading outside of the TMS, as shown using ObservePoint's Tag Initiators report in the image to the left.





Rogue or piggybacking tags are bad.

FALSE **TRUE**

Not all piggybacking tags are bad. Some are necessary for functionality.

You still need to find and approve or remove any you don't already know about. Advertising technologies often launch other technologies for efficiency, but old campaigns or new partners might be collecting and sending data to places you haven't vetted and approved.

Equifax and TransUnion were affected by malware piggybacking off of third-party data analysis code.*

British Airways was fined \$26M for failing to protect the personal and financial data of more than 400,000 customers.*

Knowing where Personal Identifiable Information (PII) is collected and stored is vital to privacy compliance.

TRUE

If your site is collecting PII, you'll need to know where you're storing it, make sure to encrypt the data, and keep an eye on where the data is being sent, so you minimize the risk of data breaches and remain compliant with privacy regulations.



Is it TRUE ObservePoint can help with...?

- Policy & Banner Monitoring**
True! ObservePoint can automatically scan your website pages regularly and at scale to verify that policies and banners are accessible from every entry point.
- Consent Management Platform Validation**
True! ObservePoint can test navigating through your site in various states of consent to validate that user-specified preferences are being respected.
- Inventorying ALL Tags & Cookies**
True! ObservePoint can audit all data collectors on your site at scale and show you exactly what page they're on and what data they're collecting.
- Geolocations of Data**
True! ObservePoint can identify and quickly illustrate on a map where your network requests for data are originating.
- JavaScript File Changes**
True! ObservePoint can show you changes over time and whether they're first or third-party, so you're not the last to know.
- Rogue or Piggybacking Tags**
True! ObservePoint discovers and diagrams the relationships between technologies, so you can quickly check any new/unapproved tags.
- PII Collection**
True! ObservePoint can be configured to monitor areas of your site that collect personal information, so you can take the necessary security measures.

Get A Website Privacy Audit

Fill out a quick form if you'd like to see how an audit of your own site will prove immediately useful.

[REQUEST PRIVACY AUDIT](#)

*sources
<https://iapp.org/news/a/california-attorney-general-announces-first-ccpa-enforcement-action/>
<https://www.cniff.fr/en/cookies-financial-penalty-35-million-euros-imposed-company-amazon-europe-core>
<https://resources.observepoint.com/reports/consent-management-platforms-adoption-and-market-share-analysis>
<https://www.zdnet.com/article/gartner-predicts-privacy-law-changes-consolidation-of-cybersecurity-services-and-ransomware-laws-for-next-4-years/>
<https://www.cnet.com/news/privacy/equifax-website-ads-served-adsware-malware-expert-finds/>
<https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2020/10/ico-fines-british-airways-20m-for-data-breach-affecting-more-than-400-000-customers/>