ObservePoint

Dark Pattern Privacy Fines

And How to Avoid Them

In January, Google and Facebook were fined $238 million between them for dark patterns under the GDPR. According to France's data protection regulator, they failed to provide users with an easy way to disable cookies.

Dark Patterns

This refers to UX and design practices that manipulate or steer users into behavior that may be profitable for the company and harmful to the user or something the user didn't intend.

What are some dark patterns that affect consent?

1. Not asking for consent

This would fall under dark patterns if it's intentional, but some businesses do not ask for their customers' consent to form a legal basis for processing data. Reasons could range from deliberate obfuscation to simply not paying enough attention. Consent must be given to provide data for clear and specifically defined uses, according to regulations like GDPR.

A recent example is a business that had acquired multiple brands and one of the brands was a high traffic website that had failed to ask for consent. A GDPR fine was levied on the holding company.

How to ensure you're getting consent

ObservePoint can automatically scan all of your digital properties for ongoing monitoring and due diligence. It can check for your Consent Management Platform (CMP) and tag presence on every page in an easy-to-read Tag Inventory Report.

2. Making it difficult to refuse consent

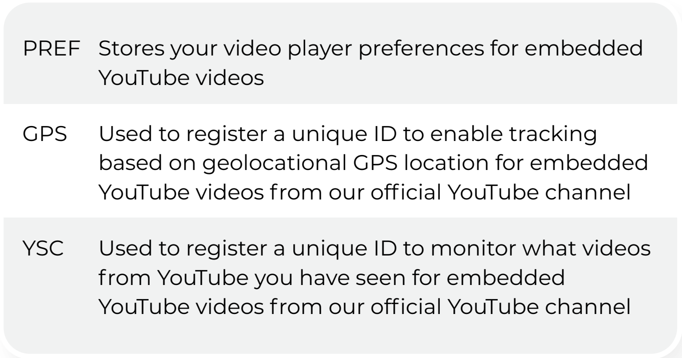
This is what Google and Facebook were fined for. It refers to practices such as:

- ☑ Requiring more steps to decline consent
- ☑ Making the button to refuse consent smaller than the one to give consent
- ☑ Lowering the contrast on the text
- ☑ Or hiding it in some other way

3. Asking for consent and classifying certain tech as "Strictly Necessary"

If you are a marketing manager, you may feel that a remarketing tag is "necessary," but if your website can run smoothly without it, then it isn't strictly necessary, especially from the customer's point of view. Hence, they are not giving informed consent because you misinformed them about the necessity of the tag.

Look at this example of Strictly Necessary Cookies on a car company's site:



PREF	Stores your video player preferences for embedded YouTube videos
GPS	Used to register a unique ID to enable tracking based on geolocational GPS location for embedded YouTube videos from our official YouTube channel
YSC	Used to register a unique ID to monitor what videos from YouTube you have seen for embedded YouTube videos from our official YouTube channel

YouTube viewer preferences might help the company play the correct video content for visitors from particular geolocations, but would a visitor agree that this was strictly necessary?

How to search and classify cookies

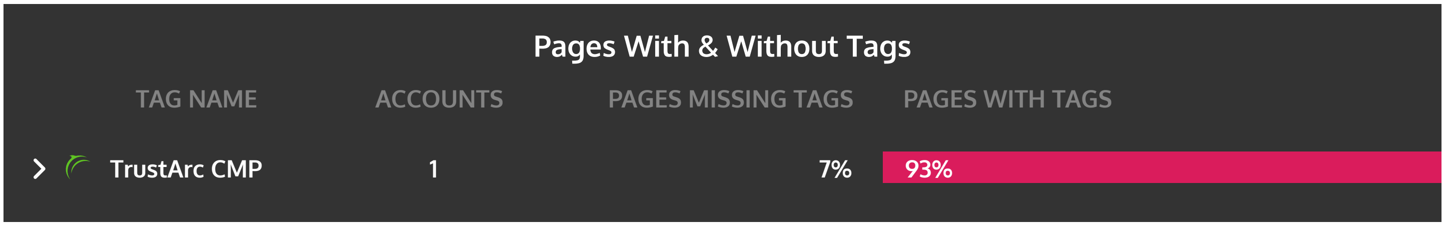
ObservePoint's Privacy Compliance solution has a Categories Report that can help you identify your cookies, allowing you to classify them correctly.

4. Asking for consent but not honoring it

Most organizations investing in a CMP fully intend to honor customers' consent preferences. However, **the implementation process is fraught with obstacles** that could derail these good intentions.

Here are a few examples:

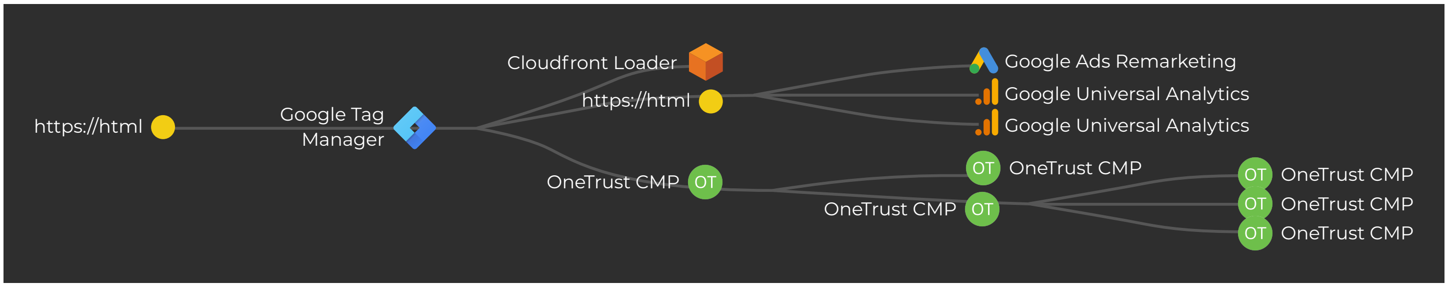
CMPs are not always implemented on every page and regular updates to your website can interrupt their functionality.



Pages With & Without Tags

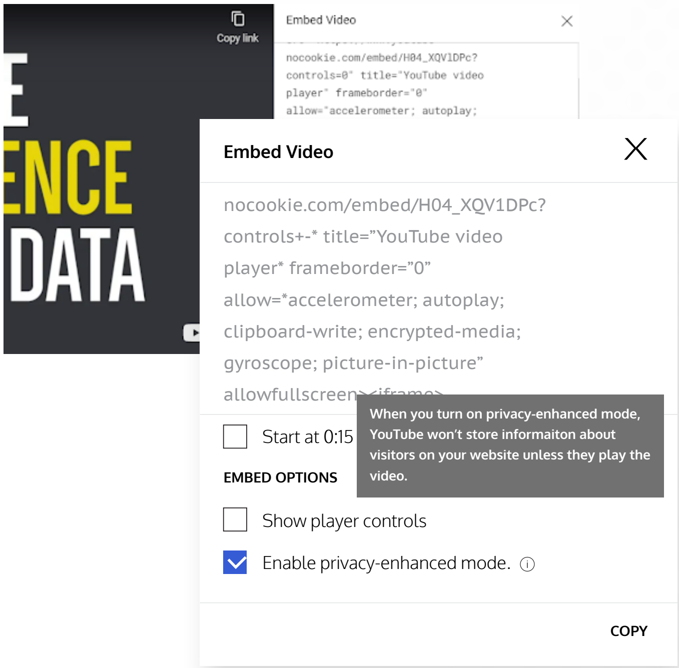
TAG NAME	ACCOUNTS	PAGES MISSING TAGS	PAGES WITH TAGS
> TrustArc CMP	1	7%	93%

CMPs aren't always deployed through the Tag Management System (TMS) properly, so it can't control the tags as intended. Even if it is connected properly, the CMP can't see anything loading outside of the TMS.



Tag Initiators with CMP outside of TMS

Third-party content outside of the scope of your CMP is sometimes used on your website. For example: many businesses leverage embedded YouTube videos as part of the branding and content strategy but do not consider the tracking consents within the video.



Embed Video

```
nocookie.com/embed/H04_XQV1DPc?
controls=0" title="YouTube video
player" frameborder="0"
allow="accelerometer; autoplay;
```

Embed Video

```
nocookie.com/embed/H04_XQV1DPc?
controls+-* title=”YouTube video
player* frameborder=”0”
allow=*accelerometer; autoplay;
clipboard-write; encrypted-media;
gyroscope; picture-in-picture”
allowfullscreen></iframe>
```

□ Start at 0:15

When you turn on privacy-enhanced mode, YouTube won’t store informaiton about visitors on your website unless they play the video.

EMBED OPTIONS

□ Show player controls

☑ Enable privacy-enhanced mode.

COPY

How to test consent preference

If you’re asking for consent but still dropping the wrong types of cookies, then your CMP is doing the exact opposite of keeping you compliant and free from liability. ObservePoint’s Privacy Compliance solution allows you to set up Rules, then travel through your website with a specific consent preference to verify that the CMP is acting accordingly.

Build Trust & Avoid Fines

If you’re trying to build trust and confidence with your customers and avoid large fines, using dark patterns or doing just the minimum required for compliance is a poor strategy. Adopting the best practices of privacy and transparency starts with knowing what’s truly happening on your site.

Watch this video to see Privacy Compliance features in action, and we’d be happy to show you how it can help with your specific privacy goals!