THE STATE OF WEBSITE PRIVACY

2024

Insights on privacy compliance trends, risks, and best practices for websites.

privado

Table of Contents

INTRODUCTION

- PRIVACY REGULATION ↑
- CONSENT COMPLIANCE FINES ↑
- CONSUMER PRIVACY EXPECTATIONS ↑
- 75% OF THE MOST VISITED WEBSITES ARE NOT COMPLIANT

Privacy regulation is increasing

As of September 2024, 71% of all countries have enacted modern privacy regulations governing personal data, and a third of the remaining countries have drafted privacy regulations.

Europe's GDPR (General Data Protection Regulation) created the need for consent compliance on websites in 2018. In 2024, new regulation has made consent compliance a priority in the US and other countries around the world.

GDPR requires that users opt in before companies operating in the EU and UK can collect or share personal data on websites (and elsewhere).

With enforcement for CPRA (California Privacy Rights Act) beginning in 2024, companies operating in California must give users the opportunity to opt out of personal data sharing for advertising purposes, also known as the "Do Not Sell or Share" rule. CPRA amended the California Consumer Privacy Act (CCPA) that only gave users the right to opt out the sale of personal data. Although nearly 20 other US states have passed their own privacy laws, CPRA is still the bar for consent compliance in the US because CPRA's consent requirements are either similar or greater than other state laws.

Because most privacy teams lack the tools to monitor consent compliance on websites, they must rely on others to properly configure consent banners and data flows. Even with a consent management platform (CMP), someone would still have to manually check the configuration of each banner, pixel, and tag manager for every website in every region to monitor compliance.

With most websites getting updated on a weekly basis, automated and regular monitoring is required to ensure consent compliance. Without it, companies open themselves up to privacy fines and reputational damage.

Consent compliance fines are starting to pile up

In the last few years, European and US authorities have begun issuing significant fines to large and small companies for non-compliant data collection and sharing on websites.

Six of the 20 largest GDPR fines are due to consent compliance violations on websites, with Amazon receiving the second-largest GDPR fine to date, $888M, for targeting users with ads without proper consent in 2021.

In the US, at least 10 companies since 2022 have been fined for violating consent compliance on websites as regulated by CPRA/CCPA, the FTC (Federal Trade Commission), or HIPAA (Health Insurance Portability and Accountability Act).

Consumer privacy expectations are increasing

As privacy regulation and enforcement have ramped up, consumers have dramatically raised their data privacy standards for companies. US state privacy regulations have given consumers the right to access and delete their personal data, and such requests have increased 246% from 2021 to 2023.

As big tech companies like Google have received several GDPR fines, many consumers have moved to new privacy-safe browsers and search engines such as Brave and DuckDuckGo.

75% of the most visited websites in the US and Europe are not privacy compliant

Using Privado.ai's automated consent monitoring to scan the top 100 most-visited websites in the US and Europe, we found a high-rate of non-compliance in both regions.

In the US, 76 of the top 100 websites do not honor opt-out consent signals as required by CPRA.

In Europe, 74 of the top 100 websites do not honor GDPR opt-in consent requirements.

As regulation and enforcement continues to accelerate globally, it is critical for privacy teams to implement monitoring and governance solutions to prevent fines that can cause serious financial and reputational damage.

76

of the top 100 websites in the US are not CPRA compliant

74

of the top 100 websites in Europe are not GDPR compliant

II

HIGHLIGHTS

- UNITED STATES WEBSITE PRIVACY COMPLIANCE RATES
- EUROPE WEBSITE PRIVACY COMPLIANCE RATES
- THIRD-PARTY DATA SHARING BENCHMARKS

Website Privacy Compliance in the — United States

76% of the most visited websites in the US do not honor CPRA opt-out signals

75% of the most visited websites share personal data with advertising 3rd parties even when users opt out

69 Non-compliant websites average 69 CPRA consent compliance risks

Website Privacy Compliance in — Europe

74% of the most visited websites in Europe do not honor GDPR opt-in consent requirements

72% of the most visited websites share personal data with advertising 3rd parties without opt-in consent

23 Non-compliant websites average 23 GDPR consent compliance risks

3rd Party Data Sharing Benchmarks

17

In the US, the most visited websites share personal data with an average of 17 advertising 3rd parties

70%

Over 70% of the most visited websites in the US and Europe share personal data with Google Ads and Facebook Ads

6

In Europe, the most visited websites share personal data with an average of 6 advertising 3rd parties

78%

78% of the most visited websites in the US and Europe use a tag manager to share personal data across advertising third parties

III

METHODOLOGY SUMMARY

- DATA COLLECTION
- COMPLIANCE CHECKS

Methodology overview: Scanned the 100 most visited websites in the US and Europe in September of 2024 for consent compliance with CPRA and GDPR respectively using Privado.ai's automated consent monitoring technology

Technological approach: Simulate each possible user consent action in the applicable location; check cookie and network request activity for each action

Compliance checks summary by regulation

CPRA

Third-party cookie blocking: Check if advertising third-party cookies are dropped for users who opt out

Network request blocking: Check if advertising third-party trackers/pixels fire and make network requests to share personal data for users who opt out

GDPR (EU & UK)

Third-party cookie blocking: Check if third-party cookies are dropped for users who opt out or take no action

Network request blocking: Check if third-party trackers/pixels fire and make network requests to share personal data when users opt out or take no action

Interactive Advertising Bureau (IAB) Transparency and Consent Framework (TCF) compliance

Methodology for top 100 most visited websites in the US and Europe

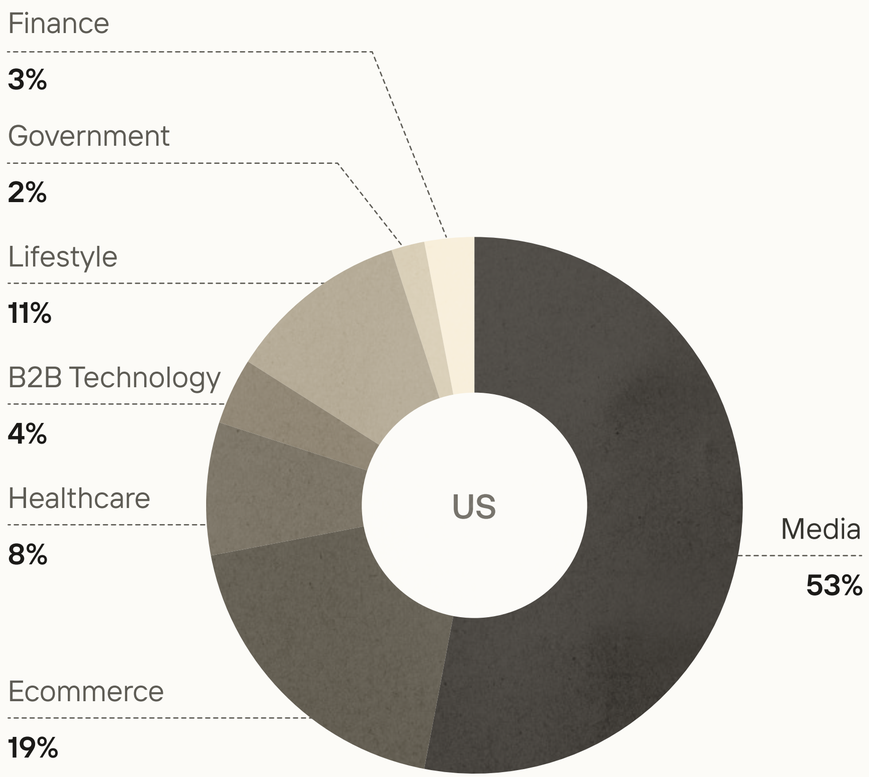
Selected according to highest organic search traffic in September 2024

Source: Ahrefs.com

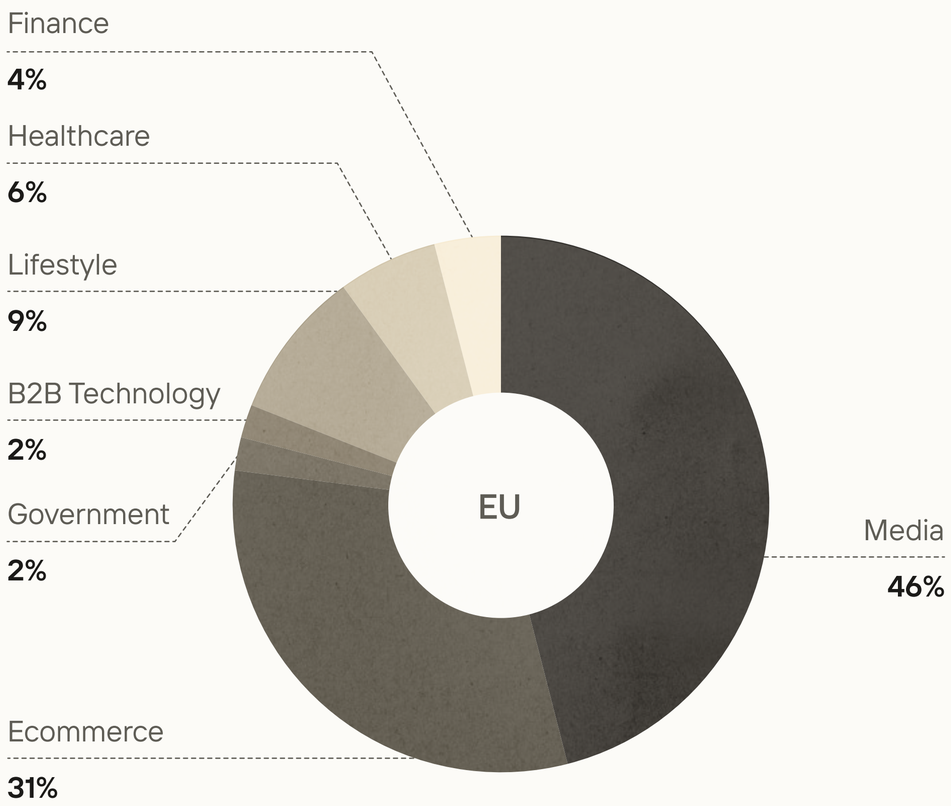
Created separate top 100 lists for the US and Europe; used UK data as a proxy for Europe

See appendix for full methodology details and website list

Top 100 Websites in US Industry Breakdown



Top 100 Website in Europe Industry Breakdown



IV

CURRENT PRIVACY REGULATION IN THE US AND EU

- CPRA/CCPA IN THE UNITED STATES
- GDPR IN EUROPE
- IAB’S TCF CONSENT REQUIREMENTS

CPRA/CCPA in the United States

California's CPRA has set the "do not sell or share" standard for consent compliance in the US. When the CPRA amendment to CCPA went into effect in 2024, it required companies to give users the option to opt out of the selling or sharing of their personal data for advertising purposes.

Global Privacy Control Browser Requirement

In addition to giving users the option to opt out on a website or app, CPRA also requires companies to honor users' Global Privacy Control (GPC) setting in their web browser. GPC allows users to universally opt out of personal data selling and sharing for all websites.

Other US State Privacy Laws

Although nearly 20 other states have passed their own privacy laws and more are in the process, CPRA is still the bar for consent compliance in the US. CPRA's consent requirements are either similar or greater than other state laws, and CPRA allows for stricter enforcement than other state laws.

US Federal Privacy Law Status

In April 2024, the US Congress proposed a new federal privacy law, the American Privacy Rights Act, that would override all state privacy laws, but the law is still a long way from being passed. The law would dramatically raise privacy standards and enforcement across the US; it would require opt-out consent for personal data sharing and opt-in consent for sensitive data.

GDPR in Europe

GDPR, which governs the European Union (EU) and United Kingdom (UK), remains the strictest consent compliance law. GDPR requires companies to obtain user consent before collecting, processing, or sharing any personal data. As a result, users must opt in before first or third party cookies can be placed in the user's web browser, collect device IDs in mobile apps, or send personal data to third parties.

IAB Transparency and Consent Framework (TCF)

To provide the digital advertising industry with a standardized approach to comply with GDPR, the IAB (Interactive Advertising Bureau) introduced TCF in 2018. To comply with TCF, websites and apps must create a user preference center that gives users the option to opt into data usage and sharing by purpose and by third party.

Most companies implement this with CMPs that categorize data use and third parties and limit data flows based on user preferences. For websites that run auctions to serve ads, TCF requires that ad auctions not receive user identifiers that enable personalized ads unless users opt in. TCF is a voluntary standard websites opt in to. TCF non-compliance may or may not lead to a GDPR violation.

V

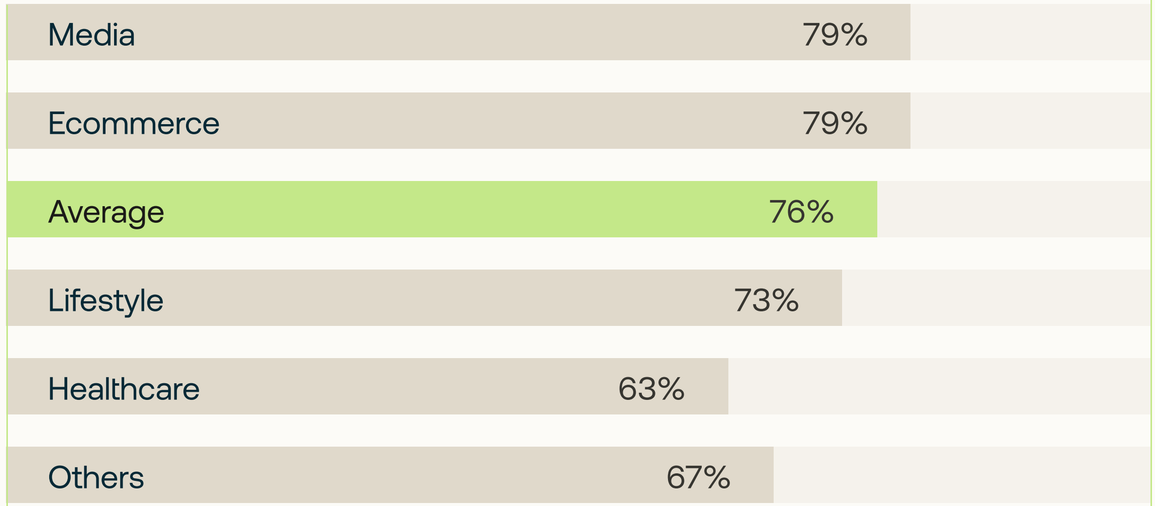
US CONSENT COMPLIANCE FINDINGS

- PRIVACY NON-COMPLIANCE BY INDUSTRY AND REASON
- WHY WEBSITES STRUGGLE WITH CONSENT COMPLIANCE
- NOTABLE US CONSENT COMPLIANCE FINES

76%

of the most visited websites in the US do not honor CPRA opt-out signals

CPRA NON-COMPLIANCE RATE BY INDUSTRY



Non-compliance with the CPRA/CCPA “Do Not Sell or Share” rule is prevalent across all industries in the US

As US privacy regulation and enforcement have increased, most websites are at risk of consent compliance violations

Media, ecommerce, and lifestyle (B2C technology) websites make up 83% of the top 100 websites and have the three highest rates of non-compliance risk. Because all three industries rely heavily on advertising to drive and monetize website traffic, these websites tend to share user data with the most advertising, marketing, and analytics partners to improve measurement and performance.

To comply with the CPRA amendment to CCPA, all websites must block personal data sharing with advertising third parties if the user opts out of data sharing. Despite recent privacy fines, most websites are continuing to drop third-party cookies and send personal data to advertising third parties even when users opt out.

Although there were only five non-compliant healthcare websites (out of eight) in the top 100, healthcare-related companies run the highest risk of getting fined if they are not compliant. Any company processing sensitive health data that falls under stricter, federal regulation and enforcement that has led to several fines for violating FTC (Federal Trade Commission) statutes and the HIPAA (Health Insurance Portability and Accountability Act).

Top compliance risks

1 Network Request Non-Compliance

When users opt out of data sharing, advertising third-party trackers/ pixels still fire and make network requests to share user data

75% of the most visited websites share personal data with advertising 3rd parties even when users opt out

2 3rd Party Cookie Non-Compliance

When users opt out of data sharing, advertising third-party cookies are still dropped in the user's browser for tracking purposes

70% of the most visited websites drop advertising 3rd party cookies even when users opt out

Why do websites in the US struggle to comply with opt-out requests?

Most privacy teams lack the tools to monitor consent and data flows on their websites (and in general). Even for companies that use a consent management platform (CMP) to centrally configure consent banners and data flows, the privacy team must rely on other teams to properly set up the banners and data flows for every third party on every website.

On web, users can opt out of data sharing via the consent banner or the Global Privacy Control (GPC) signal. GPC is a web browser setting that allows users to universally opt out of data sharing on websites. CPRA requires companies to adhere to both user signals.

To adhere to user opt out signals, companies must block advertising third-party cookies and network requests from advertising third-party pixels. By default, third-party pixels cookie each user so that they can identify that user primarily to target them with personalized ads on other websites or marketing channels. Additionally, third-party pixels make network requests to collect additional personal data primarily to measure and optimize advertising.

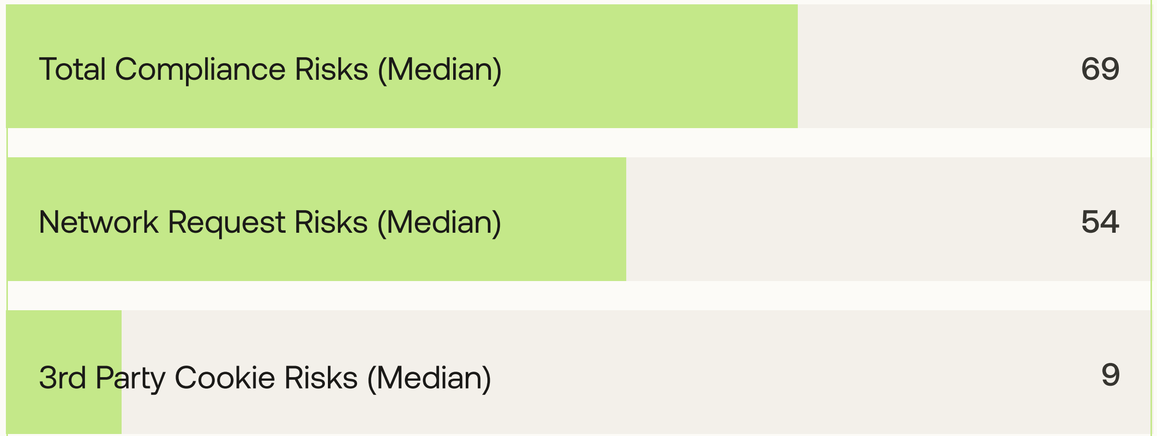
As marketing and engineering teams update websites on a weekly or monthly basis, privacy teams need continuous visibility and governance over personal data flows to third parties.

To comply with CPRA/CCPA, websites must block third-party cookies and network requests that share data with advertising 3rd parties if users opt out

69

Non-compliant websites average 69 CPRA compliance risks

MEDIAN VOLUME OF CONSENT COMPLIANCE RISKS



Among the 76% of the most visited websites with compliance risks, the volume of risks ranged from 1 to 1,455 with a median of 69

Why do websites in the US have so many instances of non-compliant data sharing?

Since cookies were first introduced to Microsoft's Internet Explorer browser in 1995, cookies and other personal data have been vital to the advertising and marketing technology ecosystem. Without cookies and other PII (Personally Identifiable Information), many aspects of the web experience would not be possible including personalized ads and shopping carts (yes, shopping carts would empty after each page load without a way to identify the user).

Over the years as countless new technology solutions have been developed, marketing teams have continued integrating more and more third parties with their websites to try to improve marketing measurement and performance. Additionally, each third-party integrated may drop multiple cookies and make multiple network requests to accomplish different objectives.

With so many third parties making multiple attempts to collect user data, privacy teams cannot rely on a system of manual configuration and monitoring. They need comprehensive automated solutions to continuously monitor and govern consent and data flows.

Notable Consent Compliance Fines – US

Sephora

Sephora was the first company to be fined for violating California's CCPA in 2022. Sephora was fined $1.2M for two reasons: failing to disclose to website visitors that they were selling their personal information; and failing to process opt-out requests made via the Global Privacy Control (GPC) web browser setting.

Although Sephora did not explicitly sell personal data for money, their exchange of personal data with third parties in exchange for discounted or free advertising and analytics services constituted a “sale” under CCPA. CCPA defines a sale as the exchange of personal data for something of value. Sephora made no mention of selling personal data in their public privacy policies or consent banners and therefore, were found to be in violation.

In addition, CCPA requires the companies honor users’ Global Privacy Control (GPC) setting in their browser, which allows users to universally opt out of personal data selling and sharing for all websites. California found that Sephora was ignoring the GPC browser signal and still selling data for users who opted out via GPC.

Monument

Monument is an alcohol addiction treatment service, and they were fined $2.5M by the FTC (Federal Trade Commission) in 2024 for sharing personal health data against its privacy promises. According to the FTC complaint, Monument’s website and other communications claimed they were HIPAA compliant and their users’ personal data would not be shared with any third parties.

This violation fell under FTC jurisdiction because it involved personal health data, but Monument also could have been fined for violating CPRA for sharing sensitive data that was not explicitly communicated to users in their privacy policy.

The FTC claims Monument sent sensitive health data to marketing partners to retarget customers and target new users. The data was allegedly shared via pixels and APIs after Monument set up standard and custom events on their website. The FTC says Monument gave the custom events titles that revealed sensitive details about its users such as “Paid: Weekly Therapy” or “Paid: Med Management,” when a user signed up for a service. To rest its case, the FTC states that Monument shared this event data tied to users’ personal identifiers such as email address and IP address.

$1.2M
Sephora

$2.5M
Monument

VI

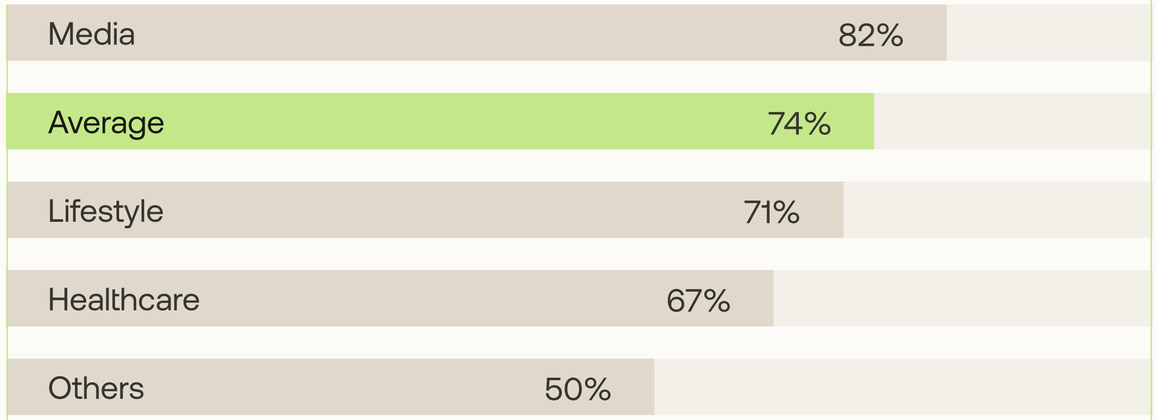
EUROPE CONSENT COMPLIANCE FINDINGS

- PRIVACY NON-COMPLIANCE BY INDUSTRY AND REASON
- IAB TCF NON-COMPLIANCE RATES
- NOTABLE EUROPE CONSENT COMPLIANCE FINES

74%

of the most visited websites in Europe do not honor GDPR opt-in consent

GDPR NON-COMPLIANCE RATE BY INDUSTRY



Websites across industries risk GDPR violations because third-party pixels are collecting data when users opt out or take no action

Media and ecommerce websites have the most consent compliance risk in Europe

Media and ecommerce websites make up 78% of the top 100 websites and account for 86% of the non-compliance. Because these two industries rely heavily on advertising to drive and monetize website traffic, these websites tend to share user data with the most advertising, marketing, and analytics partners to improve measurement and performance.

To comply with GDPR, all websites must block personal data collection and sharing with third parties unless the user provides opt-in consent. Despite recent increasingly large GDPR fines, most websites are continuing to drop third-party cookies or send personal data to third parties via network requests when users opt out or take no action on the consent banner.

Top compliance risks

1 Network Request Non-Compliance

When users opt out or take no action on the consent banner, third-party trackers/pixels still fire and make network requests to share user data

72% of the most visited websites share personal data with advertising 3rd parties without opt-in consent

2 3rd Party Cookie Non-Compliance

When users opt out or take no action on the consent banner, third-party cookies are still dropped in the user's browser for tracking purposes

39% of the most visited websites drop advertising 3rd party cookies when users opt out or take no action

Why do websites in Europe struggle to comply with opt-in consent requirements?

Most privacy teams lack the tools to monitor consent and data flows on their websites (and in general). Even for companies that use a consent management platform (CMP) to centrally configure consent banners and data flows, the privacy team must rely on other teams to properly set up the banners and data flows for every third party on every website.

To comply with GDPR's opt-in consent requirements, companies must block third-party cookies and network requests from third-party pixels if the user opts out or takes no action on the consent banner. By default, third-party pixels cookie each user so that they can identify that user primarily to target them with personalized ads on other websites or marketing channels. Additionally, third-party pixels make network requests to collect additional personal data primarily to measure and optimize advertising.

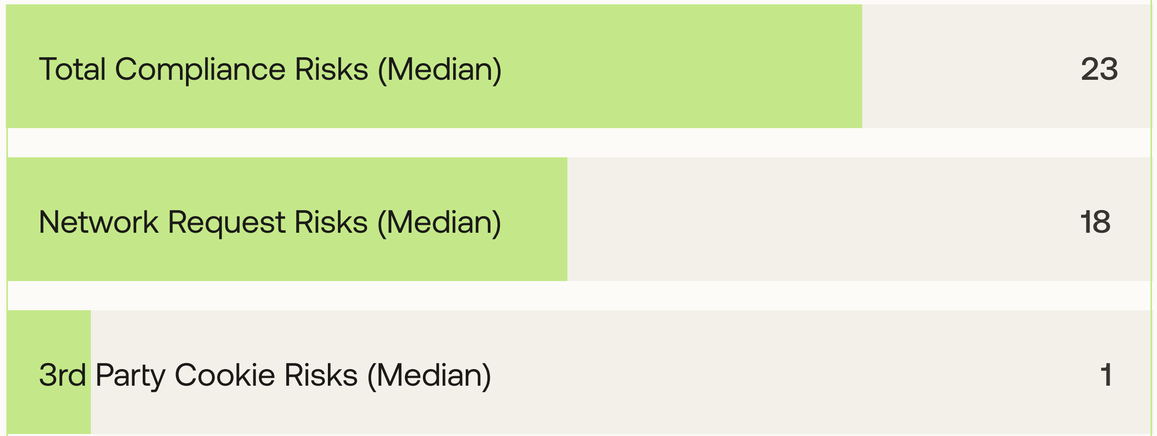
As marketing and engineering teams regularly update websites to launch new campaigns, privacy teams need full visibility and governance over personal data flows to third parties.

To comply with GDPR, websites must block third-party cookies and network requests that share data with 3rd parties if the user opts out or takes no action

23

Non-compliant websites average
23 GDPR compliance risks

MEDIAN VOLUME OF CONSENT COMPLIANCE RISKS



Among the 74% of the most visited websites with compliance risks, the volume of risks ranged from 1 to 268 with a median of 23

Why do websites in Europe have so many instances of non-compliant data sharing?

Because the most-visited websites rely heavily on digital advertising to drive and monetize website traffic, they work with a large pool of advertising partners that require personal data to measure and optimize ad spend. Additionally, many other partners are used to conduct user analytics and personalize web experiences. Each third-party integrated may drop multiple cookies and make multiple network requests to accomplish different objectives.

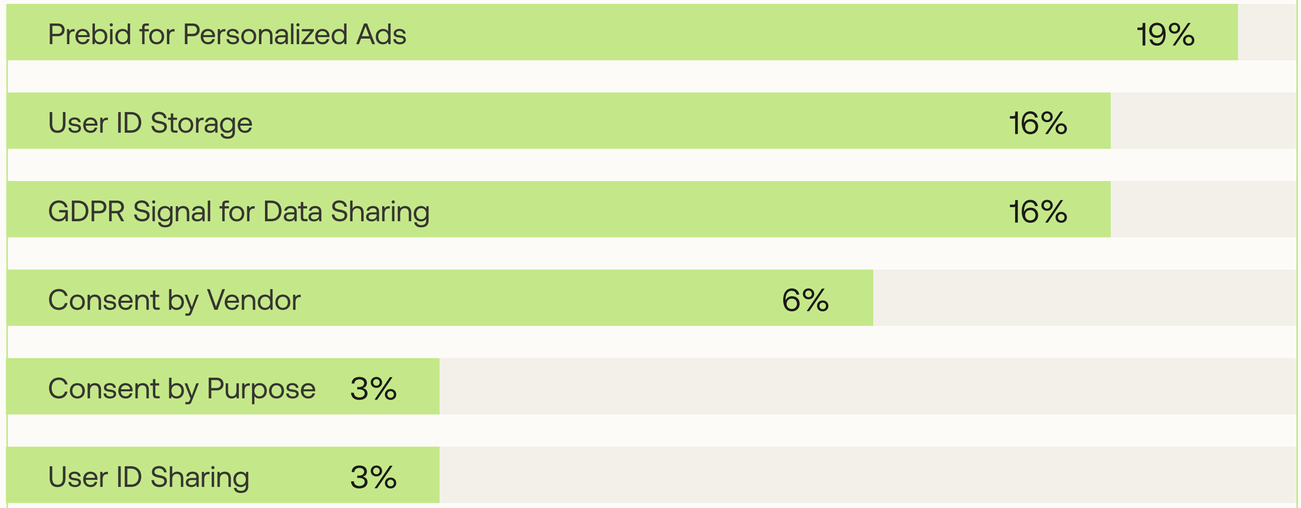
As marketing teams test new partners to improve performance, the number of third-party pixels on a website often continues to grow and grow. This often occurs because partners' pixels are left on websites collecting data even after marketing teams stop working with those partners.

Privacy teams typically lack the visibility and controls to track what third parties are integrated with their websites and whether they are honoring consent requirements. With teams using so many third parties to optimize websites, privacy teams need comprehensive automated solutions to continuously monitor and govern consent and data flows.

39%

of most visited websites in Europe using IAB's TCF do not honor all consent requirements

IAB TCF NON-COMPLIANCE RATE BY REASON



Among the 35% of top websites using IAB's Transparency and Consent Framework (TCF) to collect consent for advertising, 39% don't fully comply

What is the IAB Transparency and Consent Framework (TCF)?

To provide ad buyers, ad sellers, and intermediaries with a standardized approach to comply with GDPR, the IAB (Interactive Advertising Bureau) introduced TCF in 2018. TCF is a voluntary standard websites opt in to and is often required to work with ad partners. Most notably, ad exchanges often require publishers to implement TCF to sell personalized ads. TCF non-compliance primarily leads to serving fewer personalized ads but may also lead to a GDPR violation.

TCF Non-Compliance Reasons

01

Prebid for Personalized Ads

Websites should not send user identifiers to initiate ad auctions unless users opt in, and auctions should be delayed long enough for users to opt in.

02

GDPR Signal for Data Sharing

Failure for the CMP's GDPR signal to match users' consent action can cause network requests or personalized ads to occur without consent.

03

User ID Storage

User identifiers like cookies or advertising IDs should not be stored by the website unless the user opts in

04

Consent by Vendor

Unless the user opts in to share data with specific vendor(s), no specific vendors should be instructed to receive personal data

05

Consent by Purpose

Unless the user opts in to share data for specific purpose(s) such as advertising, personal data shouldn't be shared for any specific purposes

06

User ID Sharing

The buyer/advertiser in an ad auction should not receive any user identifiers unless the user opts in

Notable Consent Compliance Fines – Europe

Amazon

Amazon was fined $888M for violating GDPR in 2021 because they allegedly used personal data to deliver personalized advertising without proper consent. Amazon claims personalized advertising is part of the contract users enter into when they sign up for Amazon, but the Luxembourg National Commission for Data Protection disagrees.

They claim Amazon is in violation of GDPR because users were not sufficiently informed about Amazon's use of their personal data before being given the opportunity to opt in. As of September 2024, Amazon is still contesting the fine in Luxembourg's court system.

If this fine against Amazon stands, it would be the second-largest GDPR fine ever following only the $1.3B fine issued to Meta in 2023 for improperly transferring personal data from the EU to the US.

Criteo

Criteo was fined $44M for violating GDPR in 2023 primarily due to their use of personal data to deliver personalized advertising. Criteo, a much smaller company than Amazon with only about 3,000 employees, agreed to pay $44M after appealing the original fine amount of $66M.

The CNIL, France's privacy enforcement agency, found Criteo, a digital advertising partner, had committed five GDPR infringements. Most of Criteo's infringements stem from Criteo's practice of collecting personal data from their customers' users without consent.

Criteo's customers placed Criteo's pixel on their website before launching ad campaigns with Criteo, and that pixel was configured to collect personal data regardless of whether users opted into or out of data sharing. Under GDPR, the partner is obligated to verify that their customers' users provide consent before collecting data, and the CNIL found that Criteo did not have mechanisms to validate that consent was properly obtained by their customers.

$888M
Amazon

$44M
Criteo

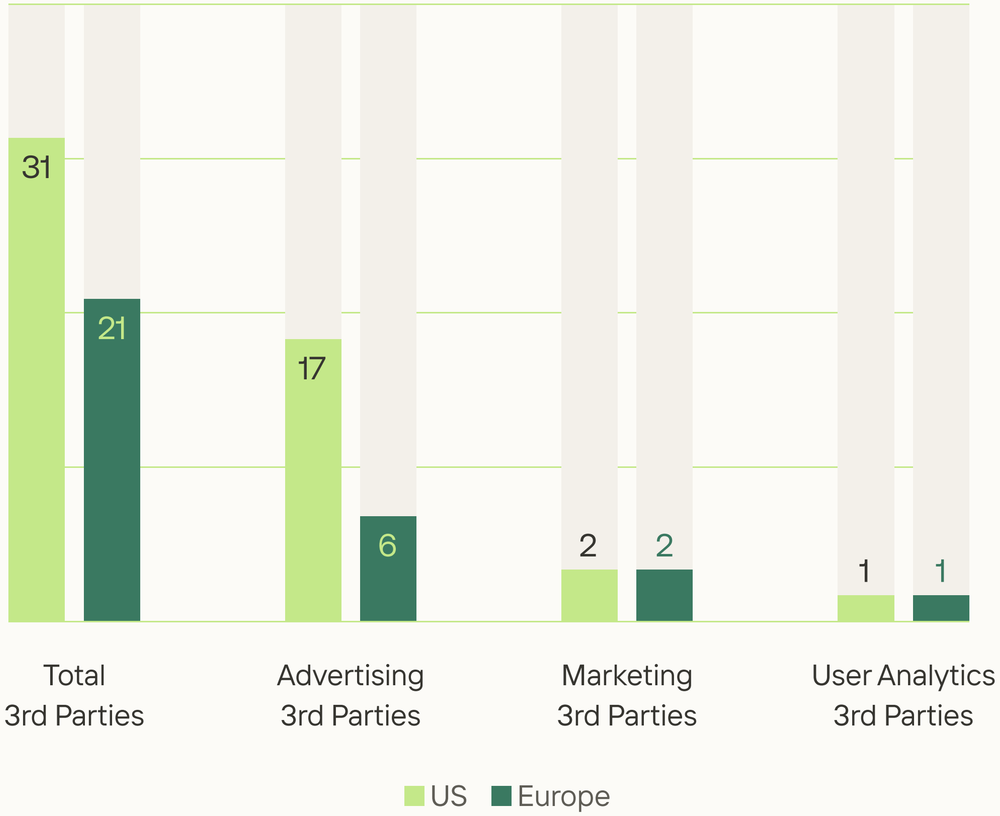
VII

BENCHMARKING PRIVACY PRACTICES

- INTEGRATED 3RD PARTY VOLUME
- TOP ADVERTISING 3RD PARTIES
- TAG MANAGER USAGE

The most visited websites share personal data with an average of 17 advertising 3rd parties in the US and 6 in Europe

MEDIAN 3RD PARTIES INTEGRATED WITH TOP WEBSITES



Top websites in the US and Europe average over 20 third parties integrated via pixels that drop cookies and collect personal data, mostly for advertising

Advertising 3rd parties such as Google and Facebook make up the vast majority of all third parties integrated with websites, and advertising third parties pose the greatest risk for CPRA and GDPR violations. Using personal data for personalized ads has led to some of the largest GDPR fines to date, including all four noted in this report.

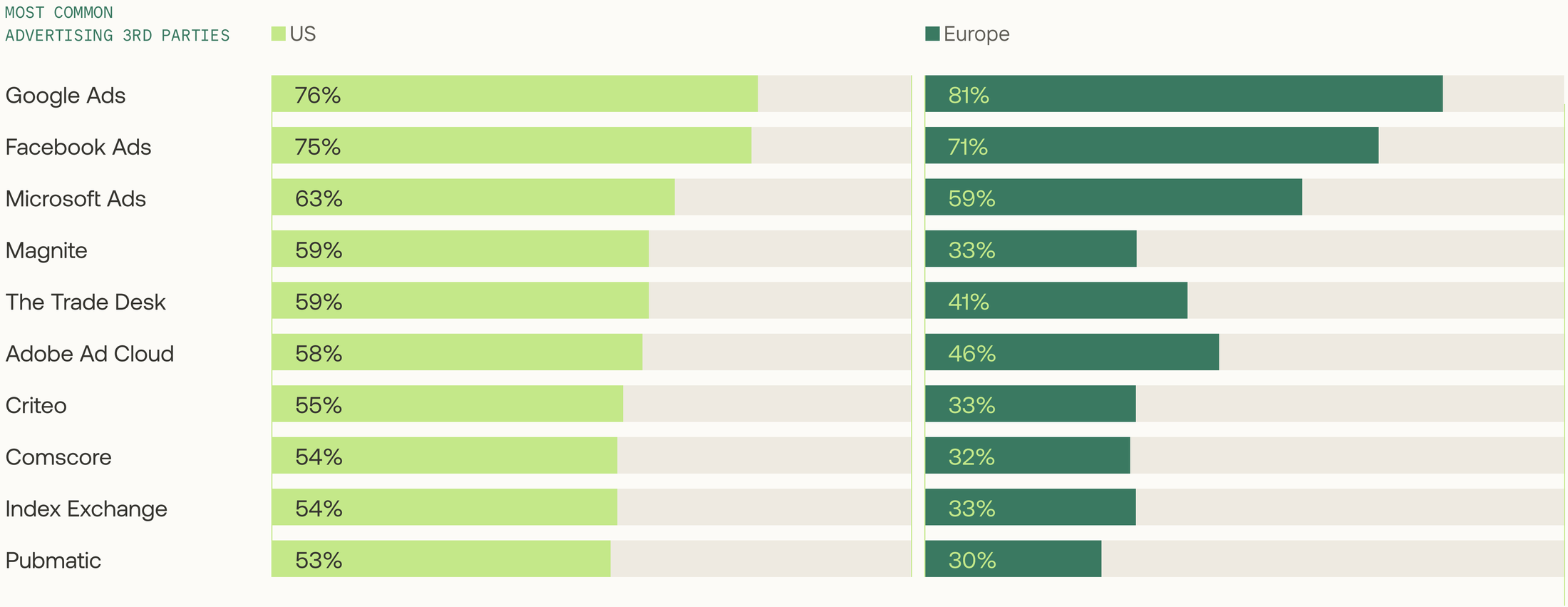
Marketing 3rd parties include partners that send marketing notifications like Klaviyo and partners that personalize web experiences such as Optimizely.

User Analytics 3rd parties include product analytics tools such as Amplitude and customer data platforms like Segment.

Other 3rd parties are made of many categories including development tools, cloud services, payments, and security.

Over 70% of the most visited websites in the US and Europe share personal data with Google Ads and Facebook Ads

8 of the top 10 advertising 3rd parties are the same in the US and Europe, but websites in Europe generally share data with less 3rd parties.



Despite the privacy risks, it is possible for websites to share personal data with advertising 3rd parties in a compliant manner

CMPs and consent testing solutions are needed to ensure compliance

Although most websites are sharing data to advertising third parties and advertising third parties represent the largest compliance risk, all advertising third parties can be integrated with websites in a compliant manner.

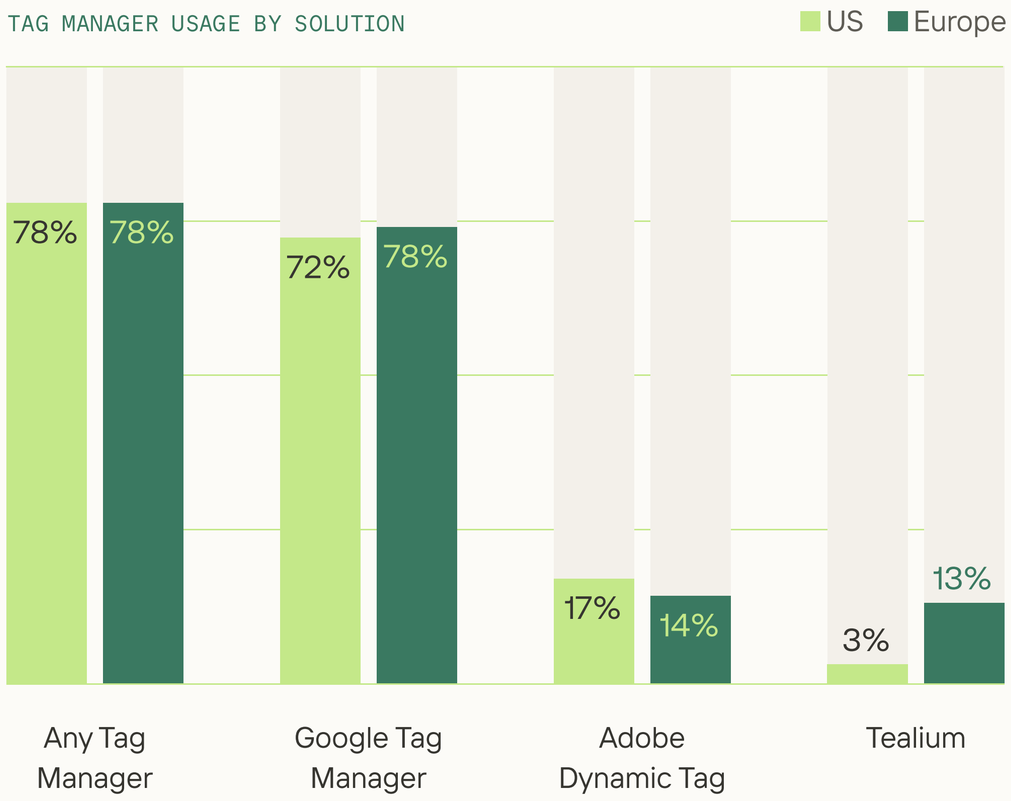
Consent Management Platforms (CMPs) should be used to centrally manage consent banners and data flows to each third party. Additionally, website scanning solutions should be used to help privacy teams monitor that each integrated 3rd party has been approved and that CMPs are configured properly for each third party.

Large advertising 3rd parties have tools and support for privacy risk mitigation

In particular, the most common advertising third parties have features and customer support to help marketing teams run advertising in a privacy compliant manner largely because these advertising third parties are also under the most scrutiny. Privacy teams should have checks in place to communicate risks to marketing and engineering teams, who can then request support from advertising third parties if needed.

78% of most visited websites in the US and Europe use a tag manager to share personal data across advertising 3rd parties

TAG MANAGER USAGE BY SOLUTION



78% of top websites use tag managers to enable marketing teams to quickly integrate other advertising 3rd parties with websites without developer support

Tag managers are effective tools for marketing teams to centralize implementation and management of website pixels in one solution, but they can also lead to increased privacy risk.

Without a tag manager, marketing teams would need to submit a request to developers to implement a new pixel each time they want to test a new advertising third party. For many organizations, this request would trigger a check to see if this third party has been approved. If not, a vendor risk assessment would typically get conducted and the privacy team would get involved.

With a tag manager, marketing teams can integrate an advertising third party's pixel without any developer support. This flexibility allows marketing teams to move fast and not drain developer resources, but it can allow the marketing team or even their marketing agency to integrate new third parties without the privacy team ever knowing about it.

VIII

IMPLICATIONS FOR PRIVACY PROFESSIONALS

- WEBSITES ARE THE SOURCE OF INCREASING PRIVACY RISK
- CONSENT MANAGEMENT PLATFORMS LACK COMPLIANCE VISIBILITY
- CONTINUOUS WEBSITE MONITORING IS NEEDED

01

Websites are the source of increasing privacy risk

Now that privacy regulation and enforcement has become increasingly strict, most websites are at risk of non-compliance. The same can be said for mobile apps as well.

The existing marketing and analytics ecosystem relies on personal data for measurement and personalization, and organizations have yet to fully adapt to the new normal of limited data processing based on consent. With third-party pixels and tag managers currently collecting all kinds of personal data on nearly every webpage, many companies are now at risk of significant privacy fines and reputational damage.

02

Consent management platforms alone do not ensure consent compliance

Consent management platforms (CMPs) are effective at managing the complexity of implementing consent banners and data flows across websites, but CMPs can't sufficiently monitor and validate consent compliance. CMPs rely on continual manual configuration to maintain compliance. If consent policies or data flows are not configured correctly for every device/channel, location, type of data, or third party pixel, there are no alerts or safeguards to prevent non-compliant data sharing or collection.

Additionally, non-compliance can occur if the CMP is not updated when changes are made to the website by engineering or marketing teams. Unfortunately for privacy teams, companies have an increasing number of websites in different countries, and they are being updated constantly with releases often occurring weekly.

03

Continuous website monitoring is needed to mitigate privacy risk

As marketing and engineering teams regularly update websites to launch new campaigns, privacy teams need full visibility and governance over personal data flows to third parties. Any data collection or sharing that conflicts with published privacy policies and applicable regulations needs to be automatically flagged and addressed immediately.

Privacy teams need tools that provide a real-time view of third parties integrated with their websites, each data element being sent to which third parties, and consent banner functionality. Additionally, automated guardrails are needed to prevent website changes with clear privacy risks and trigger privacy reviews for changes that fall into a gray area. Without such tools, it is impossible for privacy teams to keep up with all data flows and website changes, and risks will continue to mount.

IX

PRIVACY GOVERNANCE BEST PRACTICES

- MANAGE CONSENT BANNERS AND DATA FLOWS
- CATALOG THIRD PARTIES
- MONITOR DATA FLOWS
- IMPLEMENT CONTROLS

Privacy Governance Best Practices

To implement digital tracking governance successfully, companies must do the following for all websites and user-facing applications:

1. Manage consent banners and data flows
2. Catalog third parties
3. Monitor data flows
4. Implement controls

New regulations and increased enforcement require a new approach to maintain compliance called digital tracking governance. Digital tracking governance is responsibly managing personal data collected and shared by honoring user preferences and applicable regulations. This approach applies to websites as well as all user-facing applications such as mobile apps.

Manage consent banners and data flows

Design workflows to capture consent and share data according to user preferences and each state's or country's regulations.

Consent management platforms (CMPs) are the best solution to centrally set up and manage consent banners and data flows across websites and apps. Especially for companies operating different websites in different countries, it is critical to centrally manage how privacy policies are displayed and data flows are limited for each website.

The major limitation of CMPs is that they rely on teams to manually configure how data flows to each third party integrated with the website, and the tools need continuous oversight as website updates are made.

Catalog third parties

Create a real-time inventory of all advertising third parties and other third parties integrated with your digital properties - web and mobile. These third parties can be integrated via pixels, tags, tag managers, SDKs, APIs, beacons, etc.

The best way to get full coverage of third parties on a real-time basis is to scan the code of the website or app. The code contains the logic for how personal data is collected, used, shared, and stored. Privacy code scanning solutions are designed to create comprehensive and real-time data maps that catalog third parties and data flows.

Third parties collect data from websites by placing their specific pixel in the website's code, integrating with other third party tools deployed in the website's code, or through backend connections such as APIs. Privacy code scanning solutions identify third parties in all three situations because they can scan a company's entire codebase and integrate directly with data sharing intermediaries such as tag managers and customer data platforms (CDPs).

Instead of implementing a new pixel for each marketing partner, marketing teams often implement one tag manager on their website to send data to all marketing partners. Once the engineering team deploys the tag manager in the website's code, the marketing team can set up data sharing to almost any partner without further assistance.

Marketing teams also leverage CDPs to share data with marketing partners, primarily for building more targeted remarketing audiences, a potentially large privacy risk. CDPs are a centralized database solution used by many teams to connect and activate customer data from all touch points and systems, not just websites.

Tag managers and CDPs allow marketing teams to move fast when setting up measurement and remarketing audiences, and privacy code scanning gives privacy teams the real-time monitoring and governance needed to keep these tools in check.

Monitor data flows

Continuously monitor all personal data elements sent to third parties and internal destinations and verify the flows against user preferences and your privacy policy.

In addition to cataloging which third parties are set up to receive personal data from your website, it is critical to monitor whether third parties receive any personal data when users have not given proper consent and whether third parties receive sensitive data regardless of user preferences.

Privacy code scanning solutions are uniquely capable of monitoring both situations: when data flows don't follow consent and when certain sensitive data is shared, e.g., health, location, or financial data. To monitor data flows based on consent, user behavior is simulated on the website for each consent option: no action, accept, or reject. For each option, automated checks determine whether cookies are dropped and network data requests are made for each third party.

In addition to following the user's preferences, data flows should clearly follow the stated privacy policy. This means data cannot be used or shared for purposes not stated in the policy. By monitoring which third parties are receiving personal data, checks can be put into place to ensure data is not shared with non-compliant third parties if user preferences or policies do not allow personalized ads.

Lastly, privacy teams need to identify each data element shared with each third party to ensure that no sensitive data is shared and document proof of compliance. The only way to identify the flow of each data element is to analyze the website's code. Privacy code scanning automatically identifies all data elements the code processes and tracks its flow through internal systems to third parties, including tag managers and CDPs that share data to other third parties.

Privacy teams need to identify each data element shared with each third party to ensure that no sensitive data is shared and document proof of compliance.

Implement controls

Put automated guardrails into the process for updating websites and apps to prevent privacy violations. Regular checks should be run on live websites and during the development phase to flag and address risks before they become a bigger issue.

Privacy code scanning solutions can be seamlessly integrated into the software development lifecycle so that scans run each time new code is pushed for review. This way risks can be immediately communicated to developers and potentially resolved before even getting the privacy team involved.

Privacy code scanning solutions can also run regular website and app scans to simulate user behavior and identify data flows that conflict with user preferences.

These scans should be run on live websites and during staging (the step before changes go live). Once risks are automatically identified, privacy teams can determine when to intervene and when risks should be automatically blocked.

Privacy scans should be run on live websites and during staging to prevent risks before they go live.

KEY TAKEAWAYS

- MOST WEBSITES ARE AT RISK OF PRIVACY VIOLATIONS
- PRIVACY FINES ARE INCREASING
- PRIVACY REGULATION IN THE US IS CATCHING UP WITH GDPR
- CONTINUOUS CONSENT MONITORING IS NEEDED TO ENSURE COMPLIANCE

01

Most websites in the US and Europe are at risk of privacy violations

From scanning the top 100 most visited websites in the US and Europe, we found 76% of US websites were not CPRA compliant and 74% of websites in Europe were not GDPR compliant. For both the US and Europe, 99% of non-compliance was due to data sharing with advertising third parties without proper consent via network requests.

02

Privacy fine rates and amounts are rapidly increasing in the US and Europe

Europe has led the way in levying larger and larger fines on companies that violate GDPR. Total annual GDPR fines have grown steadily from $77.5M in 2019 to $2.2B in 2023. Six of the 20 largest GDPR fines are due to consent compliance violations on websites, with Amazon receiving the second-largest GDPR fine to date, $888M, for targeting users with ads without proper consent in 2021.

In the US, there were almost no privacy fines before 2022, and now there is one every few months. California issued its first fine for CCPA in 2022 and has already issued two CCPA fines in the first half of 2024. With the CPRA amendment to CCPA going into effect in February 2024, privacy fines from California are expected to pick up even further.

$2.2B

total GDPR fines in 2023, up from $77.5M in 2019

$888M

2021 Amazon fine, the second-largest GDPR fine to date

03

Privacy regulation in the US and around the world is catching up with Europe's GDPR

As of September 2024, 71% of all countries have enacted modern privacy regulations governing personal data. Since the beginning of 2023, three countries (Switzerland, South Korea, and Saudi Arabia) and seven U.S. states have put new privacy regulations into effect. Now almost every other US state is following suit. Over the next two years, 12 more US states will start enforcing their new privacy laws.

04

Privacy code scanning and consent management platforms are needed to ensure compliance

Privacy code scanning should be used in conjunction with a consent management platform to implement best-in-class digital tracking governance for websites and mobile apps.

Consent management platforms are critical for collecting, acting on, and recording consent, but they lack the full visibility and governance to ensure personal data doesn't improperly leak to advertising third parties. Privacy code scanning enables the complete and continuous visibility and governance needed to ensure compliance with today's complex web of privacy regulations.

71%

of all countries have enacted modern privacy regulations governing personal data

Privado.ai syncs privacy compliance with software development by providing full visibility and continuous governance for how personal data is processed. Privado.ai's privacy code scanning platform automates data mapping and assessments without questionnaires by continuously monitoring data flows across websites, apps, backend systems, and third parties. Scan websites and mobile apps to ensure data flows to trackers, pixels, and SDKs honor consent. By identifying privacy risks during and after software development, Privado.ai bridges the gap between privacy and engineering teams and reduces risk at scale.

Privado.ai is the leading privacy code scanning platform and is used by SMB and enterprise companies around the world, including Instacart, Riot Games, Infosys, HERE Technologies, Nasdaq, Headspace, and Oxford University Press.

Visit www.Privado.ai or follow us on LinkedIn

privado

Subscribe to our mailing list ↗

Join us for live webinars and roundtables ↗

Book 1:1 consultation with Nishant Bhajaria ↗

Request a product demo ↗

APPENDIX

- LIST OF WEBSITES SCANNED
- DETAILED METHODOLOGY

A. List of Websites Scanned – US

en.wikipedia.org	walmart.com	craigslist.org	bestbuy.com	apartments.com
youtube.com	indeed.com	usatoday.com	steampowered.com	cnet.com
reddit.com	linkedin.com	usps.com	xfinity.com	cbssports.com
amazon.com	healthline.com	cnn.com	investopedia.com	biblegateway.com
instagram.com	mlb.com	mail.yahoo.com	ca.gov	nerdwallet.com
facebook.com	clevelandclinic.org	lowes.com	costco.com	nordstrom.com
imdb.com	ebay.com	finance.yahoo.com	irs.gov	fedex.com
twitter.com	nih.gov	adobe.com	capitalone.com	airbnb.com
nytimes.com	play.google.com	usnews.com	go.com	medlineplus.gov
quora.com	homedepot.com	roblox.com	speedtest.net	marketwatch.com
tiktok.com	netflix.com	foxnews.com	realtor.com	edmunds.com
espn.com	allrecipes.com	people.com	mapquest.com	carfax.com
fandom.com	etsy.com	nba.com	eightsleep.com	verizon.com
pinterest.com	target.com	weather.com	quizlet.com	wikihow.com
yelp.com	yahoo.com	canva.com	expedia.com	bankofamerica.com
apple.com	forbes.com	spotify.com	genius.com	hulu.com
tripadvisor.com	merriam-webster.com	nike.com	cvs.com	chase.com
mayoclinic.org	medicalnewstoday.com	openai.com	caranddriver.com	bankrate.com
microsoft.com	zillow.com	rottentomatoes.com	dictionary.com	www.nhs.uk
webmd.com	britannica.com	nfl.com	apnews.com	cbsnews.com

Top 100 Most Visited Websites in US during September 2024 according to Ahrefs.com

A. List of Websites Scanned – EU

en.wikipedia.org	theguardian.com	linkedin.com	sainsburys.co.uk	premierleague.com
bbc.co.uk	indeed.com	uefa.com	booking.com	dunelm.com
youtube.com	argos.co.uk	healthline.com	easyjet.com	itv.com
amazon.co.uk	national-lottery.co.uk	play.google.com	screwfix.com	asos.com
www.gov.uk	dailymail.co.uk	ikea.com	uk.yahoo.com	merriam-webster.com
instagram.com	sky.com	diy.com	express.co.uk	jet2holidays.com
facebook.com	marksandspencer.com	tesco.com	forbes.com	sportsdirect.com
twitter.com	autotrader.co.uk	pinterest.com	moneysavingexpert.com	accuweather.com
imdb.com	skysports.com	thetrainline.com	medicalnewstoday.com	newlook.com
microsoft.com	thesun.co.uk	webmd.com	trustpilot.com	virginmedia.com
www.nhs.uk	fandom.com	currys.co.uk	quora.com	telegraph.co.uk
reddit.com	tiktok.com	skyscanner.net	nih.gov	vivastreet.co.uk
tripadvisor.co.uk	bbc.com	bt.com	britannica.com	google.co.uk
nytimes.com	mail.yahoo.com	sportinglife.com	nationalrail.co.uk	barclays.co.uk
metoffice.gov.uk	etsy.com	asda.com	openai.com	flashscore.co.uk
ebay.co.uk	boots.com	independent.co.uk	halfords.com	espncricinfo.com
apple.com	tui.co.uk	tfl.gov.uk	johnlewis.com	radiotimes.com
rightmove.co.uk	netflix.com	zoopla.co.uk	nike.com	whatsapp.com
bbcgoodfood.com	mayoclinic.org	clevelandclinic.org	santander.co.uk	paypal.com
next.co.uk	royalmail.com	mirror.co.uk	theaa.com	company-information.service.gov.uk

Top 100 Most Visited Websites in the UK during September 2024 according to Ahrefs.com

B. Detailed Methodology

Scanned the top 100 most visited websites in the US and Europe in September of 2024 for consent compliance with CPRA and GDPR respectively using Privado.ai's automated consent monitoring technology

Technological approach to simulate user consent behavior:

Simulate user browsing session in Chromium browser using custom DOM-based and puppeteer library provided functions

Simulate user actions such as "Click" or "Mouse Hover" for consent actions "Deny", "Accept All", and "No Consent Action"

To identify consent actions, we monitor banners provided by CMPs and use AI to identify actions for custom banners

CPRA compliance checks for websites in the US

Locations: Simulate visit to website with user located in California

Third-party cookie blocking: Check if advertising third-party cookies are dropped for users who opt out using their browser's Global Privacy Control (GPC) signal

Network request blocking: Check if advertising third-party trackers/pixels fire and make network requests to share user data for users who opt out using their browser's GPC signal

GDPR compliance checks for all websites in Europe

Locations: Simulate visits to website with user located in the United Kingdom

Banner visibility: Check if consent banners display properly on website

Third-party cookie blocking: Check if third-party cookies are dropped for users who opt out or take no action

Network request blocking: Check if third-party trackers/pixels fire and make network requests to share user data for users who opt out or take no action

IAB TCF compliance checks for websites in Europe opting into TCF

The Interactive Advertising Bureau's (IAB) Transparency and Consent Framework (TCF) is a voluntary GDPR compliance standard that websites opt in to. It is often required by ad partners when buying or selling ads in Europe.

Prebid for Personalized Ads: Websites should not send user identifiers to initiate ad auctions unless users opt in, and auctions should be delayed long enough for users to opt in.

GDPR Signal for Data Sharing: Failure for the CMP's GDPR signal to match consent actions can cause network requests or personalized ads to occur without consent

User ID Storage: User identifiers like cookies or advertising IDs should not be stored by the website unless the user opts in

Consent by Vendor: Unless the user opts in to share data with specific vendor(s), no specific vendors to should be instructed to receive personal data

Consent by Purpose: Unless the user opts in to share data for specific purpose(s) such as advertising, personal data shouldn't be shared for any specific purposes

User ID Sharing: The buyer/advertiser in an ad auction should not receive any user identifiers unless the user opts in

Third Party Identification

Merge third parties identified from cookies and network requests:

For US:

Load the website from California (Opt-out consent by law)

Wait for additional 30 seconds

Collect cookies dropped on the page

Use event listeners from puppeteer library to identify network requests

For Europe

Load the website in the United Kingdom (Opt-in consent by law)

Simulate “Accept All” action

Wait for additional 30 seconds

Collect cookies dropped on the page

Use event listeners from puppeteer library to identify network requests

Determine advertising third parties by comparing domain of cookie or network request against the IAB Global Vendor List

Methodology for top 100 most visited websites in the US and Europe

Selected according to highest organic search traffic in September 2024

Source: Ahrefs.com

Organic search traffic definition: Clicks from Google organic search results

Created separate top 100 lists for the US and Europe

For Europe, scanned top 100 websites in the United Kingdom as a proxy

Visit www.Privado.ai or follow us on LinkedIn

privado