

RESEARCH REPORT

The Banner Scanner State of Compliance

US Private Mid-Market B2B SaaS Top 100

Q3 2026

BANNER SCANNER

Contents

1.	Executive Summary	3
2.	Cohort & Method	5
3.	Banner Presence by Region	7
4.	CMP Vendor Usage	8
5.	Pre-Consent Tracker Loading: Scale	9
6.	Pre-Consent Tracker Loading: Top Services Detected	10
7.	Reject Button: Presence, Parity, and Effectiveness	11
8.	Cookie Banner Characteristics	12
9.	Cookie Banner Examples	14
10.	CIPA Exposure	15
11.	GPC Signal Integrity & Compliance	16
12.	After-Reject Tracker Persistence	17
13.	Pack Analysis	18
14.	Regional Benchmarks Summary	21
15.	Good Practice Recommendations	22
16.	How This Report Was Produced	24

Executive Summary

Banner Scanner assessed 100 privately held US mid-market B2B SaaS and software-platform companies.



Market observation

Consent tooling has become widespread across the SaaS industry, but technical enforcement has not kept pace. Most organisations now display a consent banner in Europe and California, yet non-essential trackers frequently continue to load before user choice, after refusal, and despite privacy signals.



Key finding

The dominant compliance problem is no longer banner deployment. It is consent enforcement. The visible banner is usually present. The technical controls behind it are often ineffective.



Why it matters

For GDPR and CIPA concerns, the relevant operational question is whether analytics and marketing tags are suppressed until a valid choice is made and whether rejection produces a real state change. High pre-consent tracker rates and high reject-no-effect rates indicate that the visible banner is not consistently governing the tag stack. For CPRA requirements, the highest-priority signals are different: Global Privacy Control handling and ineffective opt-out mechanisms.

The cookie banner is often present, but its configuration is rarely fully working.



89%

Pre-consent tracking

of London-site scans loaded at least one non-essential tracker before interaction.



80%

GPC Non-Compliance

of California CMPs detected the GPC opt-out signal but were not actively configured to honour it.



79%

Incorrect language

of German-site scans showed the cookie banner in English rather than German.

Executive Summary (continued)

METRIC	FINDING	SEVERITY
Pre-consent loading	89% of London sites and 88% of Falkenstein sites load non-essential trackers before the user interacts with the banner.	High GDPR compliance risk
Reject button absent	22% of banner-visible London sites and 23% of Falkenstein sites have no reject button on the first layer.	High
Broken reject button	51% of all London-region sites have a reject button that has no effect on tracker loading after it is clicked.	High
Banner language	79% of Falkenstein-region banners are served in English rather than German — the simplest fix in this dataset.	High
GPC (California)	Only 20% of CMPs actively honoured the GPC opt-out signal in California, despite 99% detecting it.	High CPRA compliance risk

Top Remediation Opportunities

OPPORTUNITY	PREVALENCE	EASE
Fix German language localisation	79%	Easy
Fix reject buttons with no effect	51%	Medium
Add first-layer reject buttons	22-23%	Easy
Enable GPC handling	80% gap	Easy

What actually loads before consent?

SERVICE	DETECTION RATE
Google Analytics / Ads (via GTM)	56%
LinkedIn Insight	27%
Google Ads	25%
Facebook Pixel	22%
Bing Ads	22%

Cohort & Method

This report cohort is a balanced selection of 100 privately held, US-headquartered B2B SaaS and software-platform companies with strong mid-market relevance. Selection used public market signals such as funding and growth announcements, employee-count databases, software-category listings, G2 and software award presence, Cloud 100 and growth signals, and review-site visibility, across sales, marketing, productivity, HR, developer tools, data, security, finance, vertical SaaS, ecommerce, and customer operations. Public companies, mega-enterprise-first platforms, and companies in active acquisition or wind-down at audit time were excluded. Companies in this cohort include names such as Notion, Figma, Calendly, Gong, Zendesk, Intercom, Rippling, Gusto, Zapier, and Smartsheet.

The audit ran in July 2026 from London (UK), Falkenstein (Germany), and San Jose (California, USA). Each site was scanned by [Banner Scanner](#) from a clean cloud-based browser session following the same sequence: initial page load, banner detection, reject interaction, and a GPC-enabled load.

REGION	JURISDICTION	WHY IT MATTERS
London	UK GDPR	Post-Brexit UK data protection law mirrors EU GDPR for consent. DPA enforcement is active; the ICO has issued fines and guidance on cookie consent since 2019.
Falkenstein	EU GDPR	EU GDPR jurisdiction. German DPA (DSK) guidance requires opt-in consent for non-essential cookies. Language localisation is a compliance requirement.
California	CCPA / CPRA / CIPA	Opt-out regime under CCPA/CPRA requires honouring GPC signals and providing opt-out mechanisms. CIPA §631 creates civil litigation exposure for tracking tools active before consent.

PHASE	WHAT IS MEASURED
First page load	Baseline. All scripts and network requests active before the user takes any action on the consent banner.
After reject	The scanner clicks the reject button (if present). Non-essential trackers still loading after this constitute a direct consent failure.
After GPC signal	The scanner sends an HTTP-level Global Privacy Control opt-out header. Sites that continue data-sharing are non-compliant in California and increasingly under GDPR.

All figures are derived from the deterministic aggregate-stats file and rounded to whole percentages. All findings are aggregated across the cohort. No individual company data point is presented.

Figures are cohort-level evidence for prioritisation, not individual legal determinations. Sector sample sizes are modest and directional. Findings represent observable technical behaviour at the time of scanning and are not legal conclusions about any individual company.

Cohort & Method (continued)

TERM	DEFINITION
CMP	Consent Management Platform: the tool that displays the banner and records consent state.
GPC	Global Privacy Control: a browser opt-out signal that sites can read and act on.
CIPA	California Invasion of Privacy Act; this report uses CIPA-oriented signals as prioritisation indicators only.
GTM	Google Tag Manager: a common deployment layer for analytics and marketing tags.
Non-essential tracker	Any analytics, advertising, or data-sharing script not strictly required to operate the site.
Reject no effect	A per-scan risk label applied when a refusal produced no measurable reduction in non-essential tracker activity.
Effective GPC outcome	The GPC signal was read and resulted in a measurable reduction in data-sharing activity. See also CMP honoured GPC — a site can produce an effective outcome without the CMP actively registering the signal.
CMP honoured GPC	The CMP configuration actively registered and responded to the GPC signal — for example, by updating consent state or suppressing tag firing. A higher bar than an effective outcome: a site can achieve measurable tracker reduction through hard-coded suppression or other mechanisms without the CMP itself explicitly acting on the signal.

Banner Presence by Region

Banner visibility differs sharply by jurisdiction. London and Falkenstein showed banners on 83% of site scans, while San Jose showed banners on 62% of site scans, consistent with an opt-out regime rather than a universal opt-in banner pattern.

In the UK and EU, cookie and tracking banners are a practical requirement for sites using non-essential cookies or similar technologies because consent must be obtained before those technologies run. In California, the compliance model is different: CCPA/CPRA and CIPA do not create a universal GDPR-style banner requirement, but a clear banner or comparable notice-and-choice layer can reduce risk by surfacing opt-out choices, privacy disclosures, and tracking or session-replay notices before sensitive tools operate.

METRIC	 LONDON	 FALKENSTEIN	 CALIFORNIA
Banner visible	83%	83%	62%
No banner shown	17%	17%	38%
Banner visibility for site scans per region			

Cookie banners provide site visitors with information and accept/reject options. But it is the CMP configuration behind the scenes that provides enforcement. Banner presence is an adoption signal, not an enforcement signal.

COMMENTARY

"Just because you can see a banner, it doesn't mean anything is being blocked."

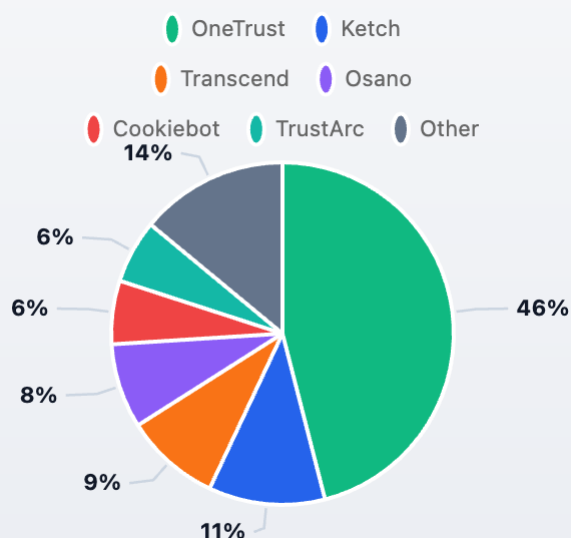
— Carl Gottlieb, Banner Scanner

CMP Vendor Usage

CMP usage is a key market signal because vendor choice shapes how consent state reaches tags, GPC handling, and privacy disclosures. Sites use a single CMP vendor across all regions. Using the London GDPR scan region data point, OneTrust dominated detected CMP usage, while Ketch, Transcend, and Osano formed the next tier.

Detected CMP Vendor Share

Share of detected CMP vendors in the London GDPR scan region.



CMP MARKET SIGNAL

46%

of detected CMPs were OneTrust

OneTrust remains dominant in this sector.

Ketch

11%

Transcend

9%

Osano

8%

Cookiebot

6%

Market prevalence is not proof of governance quality. Later sections in this report show that CMP deployment does not automatically suppress trackers, honour reject, or propagate GPC intent.

COMMENTARY

"Vendor choice matters, but implementation matters more. A CMP only earns its keep when it is configured and maintained effectively."

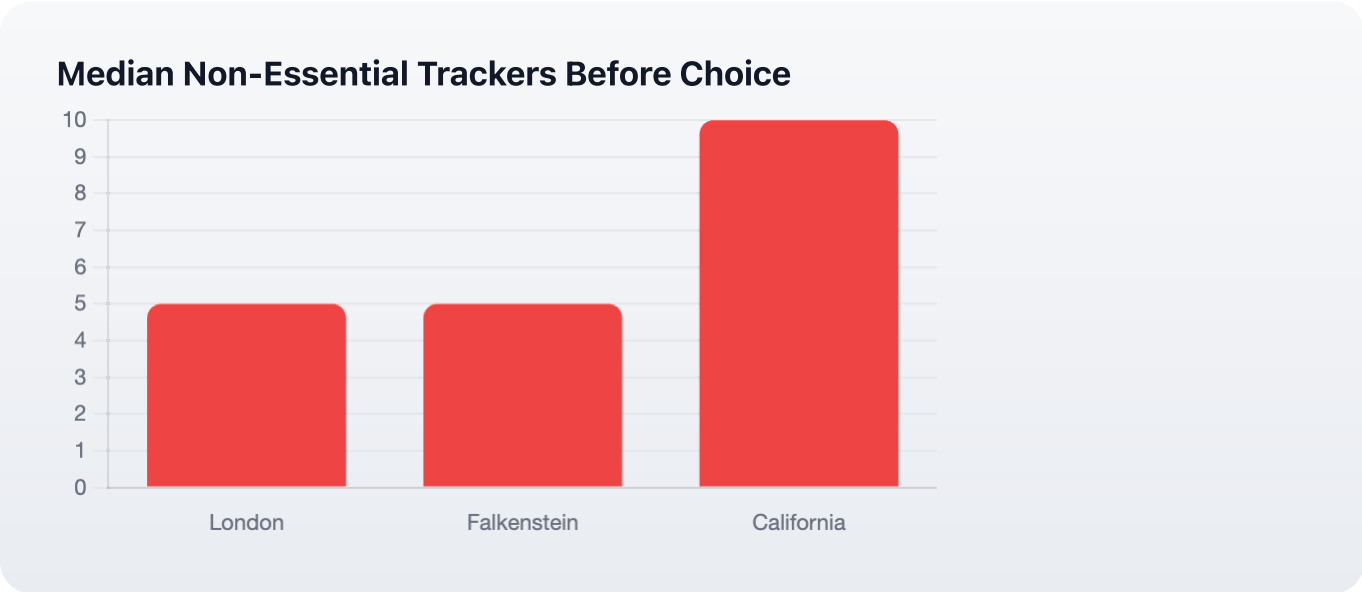
— Carl Gottlieb, Banner Scanner

Pre-Consent Tracker Loading: Scale

Across all three regions, almost nine in ten site scans loaded at least one non-essential tracker before the user interacted with the banner.

METRIC	 LONDON	 FALKENSTEIN	 CALIFORNIA
Any non-essential tracker	89%	88%	88%
Median non-essential trackers	5 trackers	5 trackers	10 trackers
90th percentile non-essential trackers	18 trackers	16 trackers	25 trackers
Any data-sharing tracker	71%	71%	78%
Median data-sharing trackers	2 trackers	2 trackers	4 trackers

Percentage rows show share of regional site scans; tracker-count rows show median or 90th percentile tracker volume.



The first page load is the critical compliance event: scripts fire before the user has received notice or had a chance to provide consent.

Pre-Consent Tracker Loading: Top Services Detected

Failures concentrate around a small number of familiar advertising and analytics services. That concentration points to deployment patterns in tag managers and marketing templates rather than isolated obscure technologies.

SERVICE	SHARE OF SCAN ROWS	CATEGORY
Google Analytics / Ads (via GTM)	56%	marketing
LinkedIn Insight	27%	marketing
Google Ads	25%	marketing
Google Analytics	24%	analytics
Facebook Pixel	22%	marketing
Bing Ads	22%	marketing
Reddit	19%	marketing
ZoomInfo	17%	marketing
Microsoft	13%	analytics
Microsoft Clarity	13%	analytics
<i>N.B. Google Analytics and Google Ads are often loaded by the Google Tag Manager script itself, rather than as a separate script. Banner Scanner recognises the tracking service independent of the script which loads it.</i>		

Reject Button: Presence, Parity, and Effectiveness

The reject action is one of the most important components of any CMP. Current EDPB and DPA guidance generally expect banners to have a reject button in the first layer of the banner and that it be equal in prominence to the accept button. The reject button must disable the applicable scripts once pressed.

METRIC	 LONDON	 FALKENSTEIN	 CALIFORNIA
Reject button present	78%	77%	51%
Reject matches accept prominence	59%	59%	48%
Reject no effect risk	51%	46%	12%
Reject-button and prominence rows use banner-visible or determinable banners; reject-no-effect risk uses all regional site scans.			

LONDON REJECT FAILURE

51%

of London-site scans showed reject no effect

London has the highest reject-no-effect rate in this cohort. Non-essential trackers stayed active after the reject action.

A banner with an accept button but no reject option forces users to either accept, spend time drilling into configuration settings or navigate away. This may undermine the validity of consent under current EU and UK regulatory guidance. The user has not been given a genuine free choice. California's notably higher absent-reject figure reflects the opt-out design: many sites legitimately show only an accept/acknowledge option with a settings link.

Banner Scanner compares rendered pixel area, background colour contrast, and button style between accept and reject buttons. EDPB Guidelines 03/2022 on dark patterns specifically cite size and colour asymmetry as deceptive design that invalidates freely given consent.

Reject behaviour is the clearest gap between visible compliance and technical enforcement. The banner may offer a refusal path, but the tracker stack frequently continues to run after that path is used.

A broken reject button is likely to be viewed as a serious compliance issue: it actively deceives the user into believing consent has been refused while continuing to load non-essential trackers. In the UK region, 51% of all sites fall into this category.

The CNIL levied €150 million in fines in 2022 specifically targeting the gap between how easy it is to accept versus reject. A broken reject button goes further — it makes refusal technically impossible while appearing to offer it.

Cookie Banner Characteristics

Beyond the reject button, a complete consent banner should provide four elements: an accept option, a reject option, a link to granular category controls, and a link to the full cookie or privacy policy. This section reports pass rates for each element, measured only on sites with a visible banner.

Banner completeness remains uneven. Accept buttons are more common than reject buttons, and policy links lag behind settings links in both GDPR scan regions.

METRIC	 LONDON	 FALKENSTEIN	 CALIFORNIA
Accept button present	90%	90%	77%
Reject button present	78%	77%	51%
Settings link present	79%	75%	69%
Policy link present	57%	58%	64%
<i>Accept and reject rows use banner-visible scans; settings and policy rows use determinable banners.</i>			

The completeness findings are design and configuration signals. They do not replace the tracker evidence, but they help explain why users may be nudged toward acceptance even where a CMP is present.

One in four European region banners lacks a settings or granular preferences link — the mechanism through which users exercise the right to selective consent under UK and EU GDPR Article 7. Offering only binary accept/reject without category-level controls is permitted but limits the granularity of consent a user can meaningfully give. 43% of London banners and 42% of Falkenstein banners omit a direct link to the cookie or privacy policy. The GDPR requires transparency about processing purposes at the point of collection. A policy link is one of the most straightforward elements to add to an existing banner.

CMP Language Localisation

The EU GDPR's transparency and informed-consent standards require cookie banners and their linked notices to be in "clear and plain language" the user understands, which in practice means localising them to the official language of each EU market an organisation targets. Consent requires informed choice. A user who cannot read the language their consent banner is written in cannot give meaningful, specific, and informed consent under GDPR Article 4(11).

Cookie Banner Characteristics (continued)

The Falkenstein figure represents CMPs configured with English as the default locale without geo-targeting rules. This is almost certainly a configuration oversight rather than a deliberate choice — all major CMPs support locale-based language switching. The fix is a CMP configuration change, not a development task, which makes this the highest-return remediation in the dataset relative to effort.

LANGUAGE MISMATCH

79%

Falkenstein banners in English

The EU GDPR requires intelligible information at the point of consent. A banner a user cannot read produces invalid consent.

COMMENTARY

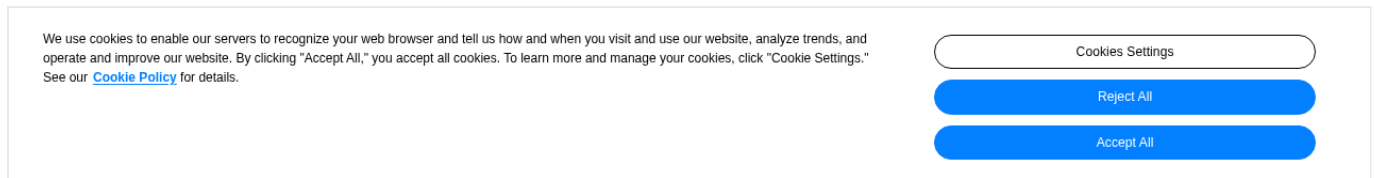
"Enabling language localisation within the CMP configuration takes seconds, but is a common miss."

— Carl Gottlieb, Banner Scanner

Cookie Banner Examples

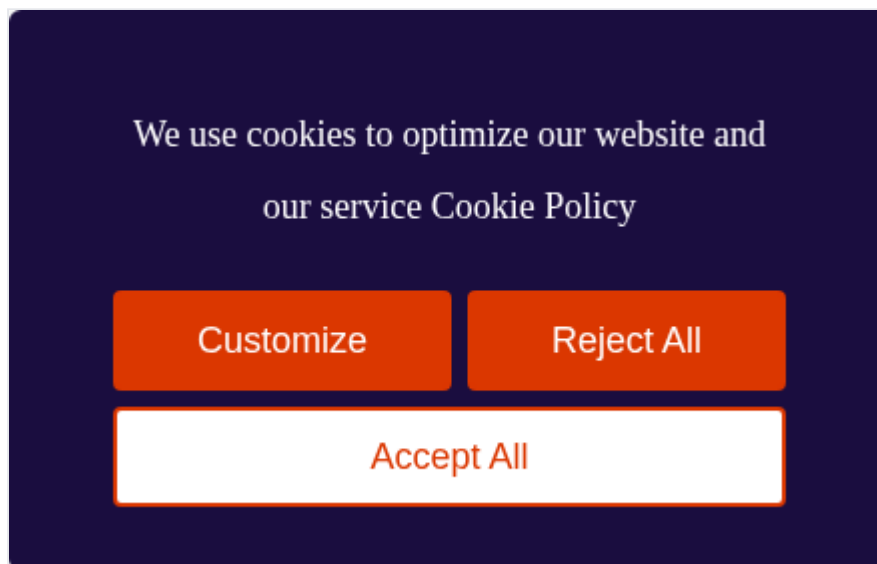
Banner Scanner collects screenshots during its website scanning in each region. The following examples were captured in this cohort alongside the report data.

Equal-choice banner examples



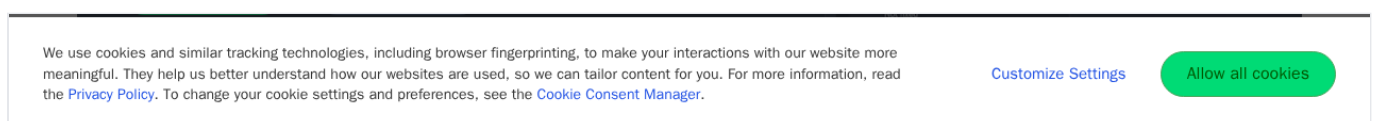
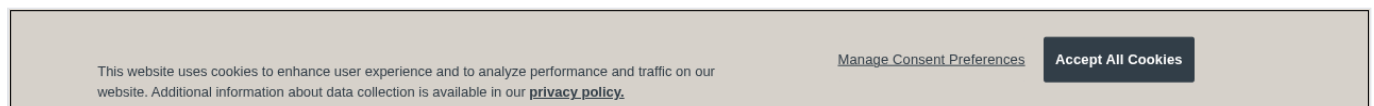
Accept and reject buttons are presented identically in the first banner layer.

Reject visually demoted



The reject button is present but visually weaker than the accept path to promote acceptance rather than refusal.

No first-layer reject



The first banner layer lacks an equivalent direct reject action.

CIPA Exposure

The California Invasion of Privacy Act (CIPA) §631 prohibits the intentional reading or interception of communications without consent of all parties. Plaintiffs' attorneys have successfully applied this to session replay tools, live chat widgets, and pixel tracking scripts that capture user activity. Unlike GDPR enforcement (regulator-initiated fines), CIPA exposure is civil litigation risk — class actions filed directly by plaintiffs. Statutory damages are \$5,000 per violation with no cap, making class actions across large user bases a material financial risk.

All statistics in this section are drawn from the California scan only.

SIGNAL	 CALIFORNIA
Banner visibility	62%
Reject button present	51%
Accept button present	77%
Reject button matches accept	48%
Settings link present	69%
Privacy link present	64%
Pre-consent data sharing	78%
GPC effective	46%
Session replay detected	36%
Live chat detected	20%
Third-party scripts pre-consent	85%
Percentage of websites scanned from California	

DISCLOSURE GAP

78%

of California-site scans shared personal information without consent

The strongest California risk signal is third-party data sharing such as with ad networks.

Banner Visible

62%

GPC Effective

46%

California exposure signals concentrate around disclosure and tracking technologies. The scanner found session replay, live chat, and third-party scripts before consent.

Many recent CIPA claims have focused on enabling data sharing ad networks and third-party analytics tools without prior consent.

GPC Signal Integrity & Compliance

Having a CMP deployed and having a CMP correctly configured are two different things. This section covers the gap between GPC signal detection and GPC signal action. Every CMP in the cohort read the GPC signal correctly. The failures are entirely in what happens next. GPC is particularly important in California but arguably not required within Europe.

The California Privacy Protection Agency's enforcement action against Sephora saw a \$1.2 million fine in part for failing to honour GPC opt-out signals. That enforcement action reinforced that honouring GPC signals is an enforceable CPRA obligation.

METRIC	 LONDON SITE SCANS	 FALKENSTEIN SITE SCANS	 CALIFORNIA SITE SCANS
CMP honoured GPC	30%	30%	20%
Effective outcome	8%	10%	46%
Ignored outcome	52%	51%	15%
Row totals do not sum to 100%; the remainder includes sites with no baseline data-sharing activity (where GPC had nothing to block) and sites where the GPC signal produced no measurable change in tracker activity.			

CALIFORNIA GPC

46%

of California-site scans produced effective outcomes

California was the only region where effective GPC handling approached a meaningful level.

While still low, the California picture is notably better for GPC effectiveness, which is likely a direct consequence of CCPA/CPRA requirements and enforcement — the CPPA has issued material fines specifically for GPC failures, creating a strong compliance incentive.

After-Reject Tracker Persistence

After-reject persistence measures the tracker load that remains active after the scanner clicks the reject button. A compliant site should show near-zero non-essential trackers post-reject. Residual non-essential trackers after rejection indicate that the consent management implementation is incomplete, misconfigured, or overridden by hard-coded tags firing outside CMP control.

After-reject persistence measures the residual tracker stack after an explicit refusal. This is broader than the reject-no-effect risk label and gives a direct view of what still leaves the browser after rejection.

METRIC	 LONDON	 FALKENSTEIN	 CALIFORNIA
All sites	61%	61%	28%
Median	2 trackers	2 trackers	0 trackers
90th percentile	11 trackers	11 trackers	10 trackers
<i>Non-essential trackers detected after a reject action. The persistence row is share of regional site scans; remaining rows show tracker-count distribution after rejection.</i>			

GDPR RESIDUAL STACK

61%

of European site scans still loaded trackers after reject

Sites' compliance status can drift over time as organisational change occurs.

At baseline the median non-essential tracker count was 5 (London) and 5 (Falkenstein). The after-reject median of 2 in both GDPR regions shows that a material proportion of the pre-consent tracker stack survives the reject action. California's lower after-reject figures reflect the opt-out framework — US-facing stacks tend to suppress trackers under CCPA opt-out more reliably than under GDPR reject.

Pack Analysis

A common compliance strategy is to monitor industry peers to assess what the rest of "the pack" is doing, in an attempt to sometimes lead, but usually to stay firmly at the centre of the pack in an attempt to hide from external scrutiny. For this analysis we observed median data points.

While competitive analysis is important, readers should note that the "centre of the pack" strategy is becoming increasingly flawed, especially as compliance scanning at scale has become automated.

Europe

METRIC	 LONDON	 FALKENSTEIN	RISK
Banner Visible	✓	✓	●
Reject Button	✓	✓	●
Reject Matches Accept	✓	✓	●
Settings Link	✓	✓	●
Policy Link	✓	✓	●
Local Language	✓	✗	●
GPC Effective	✗	✗	●

GDPR BANNERS

79%

of Falkenstein banners in English

GDPR requires intelligible information at the point of consent. A banner a user cannot understand produces invalid consent.

Non-essential scripts loaded before consent

5 trackers

PII sharing scripts loaded before consent

2 trackers

The typical European website scanned shows a cookie banner containing a settings link, a policy link, and a reject button which matches the accept button.

Scan results for London and Falkenstein are virtually identical. This is to be expected due to the similarity between UK and EU rules. Most companies use the same CMP configuration policy for the UK and EU regions. European regulators have generally focused on consent mechanisms rather than GPC implementation hence the average site tested does not implement GPC as an effective CMP blocking mechanism.

The major failing in Europe is having their German cookie banner presented in English. For these sites it is highly likely that all other non-English speaking countries have this same language localisation issue.

Pack Analysis (continued)

Europe Cookie Banners

Excluding button labels and preference controls, the typical European cookie banner contains only one or two short sentences. Most banners state that cookies are used to improve the user experience and analyse website usage, followed by a link to a cookie or privacy policy. References to advertising, personalisation, partners, device information, and detailed processing purposes appear less consistently and are often deferred to preference centres or linked policies rather than included in the initial banner text.

Based on the cookie banners seen in Europe, this is the average banner text shown:

We use cookies to improve your experience and analyse how our website is used. For more information about our use of cookies, please see our Cookie Policy.

California

Currently the California region, and most of the USA, present organisations with challenging compliance requirements due to the opt-out models needed for the CPRA, and opt-in consent models needed for a proactive CIPA/CDAFA/ECPA defence.

METRIC	 CALIFORNIA	RISK
Banner Visible		
Reject Button		
Reject Matches Accept		
Settings Link		
Policy Link		
GPC Effective		
No data sharing pre-consent		

CALIFORNIA RISK

85%

of California sites loaded third-party scripts pre-consent

Compliance is aligned to a CPRA opt-out model rather than opt-in.

Non-essential scripts loaded before consent

10 trackers

Banner visible

62%

PII sharing scripts loaded before consent

4 trackers

Reject button available

51%

Pack Analysis (continued)

The Banner Scanner data shows sites are handling the blended and evolving requirements of the California region in a defensive manner. Most sites present a cookie banner on first page load but are fairly evenly split on whether to show a reject button. The average site still has PII data sharing trackers enabled pre-consent, which aligns with the CPRA but is a risk for CIPA style claims.

GPC effectiveness is the common failure within the California region. Given this is often a single checkbox item to enable it is likely this metric will improve rapidly over time as teams review their CMP configuration. In the meantime, this is a notable risk given recent regulatory enforcement.

California Banners

Excluding button labels and preference controls, the typical US cookie banner contains one or two short sentences explaining that cookies are used to improve the website experience, analyse traffic or usage, and support advertising or marketing. Compared with the European sample, US banners more often mention advertising, marketing partners, or sharing information with analytics and social media partners. Detailed descriptions of cookie categories, device data, and processing purposes are still usually deferred to preference centres or linked policies.

Based on the cookie banners seen in California, this is the average banner text shown:

We use cookies to improve your experience, analyse website traffic, and support our marketing efforts. We may also share information about your use of our site with our analytics, advertising, and social media partners. For more information, please see our Cookie Policy.

Regional Benchmarks Summary

The following table consolidates headline compliance pass rates across all three regions. These are the numbers that form the basis of a compliance programme status report — they can be tracked over time as a cohort-level benchmark.

METRIC	LONDON (UK GDPR)	FALKENSTEIN (GDPR)	CALIFORNIA (CCPA)
Banner visible	83%	83%	62%
Reject button present*	78%	77%	51%
Reject = Accept prominence*	59%	59%	48%
Reject button functional*	48%	52%	87%
Settings link present*	79%	75%	69%
Policy link present*	57%	58%	64%
Banner in correct language*	100%	21%	100%
Sites with non-essential trackers pre-consent	89%	88%	87%
GPC effectively honoured	8%	9%	46%
* of banner-visible sites. All other metrics: all usable sites.			

The headline figures cover 100 companies across three regions — large enough to show where the industry consistently fails. Sector breakdowns point in the right direction but shouldn't be over-read; the real story is in the patterns that repeat regardless of sector: trackers firing before consent, GPC signals being ignored, and reject buttons that don't work.

Benchmarking is most useful when the same cohort, regions, and measurement definitions are repeated over time.

Good Practice Recommendations

The following actions are recommended for any organisation similar in nature to this tested cohort. They are prioritised by enforcement risk, not remediation effort. Actions within each tier can be addressed in parallel.

Tier 1 — Address immediately



Fix broken reject buttons

Identify any sites where the reject button is present but has no effect on tracker loading. Audit the CMP firing configuration — the most common cause is a GTM or hard-coded tag firing outside CMP control. Test in a clean browser session with network monitoring after each change.



Remove visual asymmetry between accept and reject

For every site banner with both buttons, verify that reject is not styled as a ghost button, plain text link, or smaller element. The EDPB Guidelines 03/2022 on dark patterns cite size and colour asymmetry explicitly as non-compliant.



Add first-layer reject buttons where missing

Sites offering only an accept button or a settings-only path on the first layer present elevated GDPR compliance risk under current equal-ease-of-refusal guidance. This is a CMP configuration change in most cases.



Fix banner language localisation in targeted countries

Configure the CMP to serve local-language banners for visitors in target territories. Most major CMPs support geo-targeting via locale configuration — this is not a development task.



Address GPC ignoring in California

For any site where a California scan shows the GPC signal being ignored, complete the CPRA-required opt-out mechanism configuration. The CPPA has already issued material fines for this specific failure.

Tier 2 — Address next



Enable settings link on banners without granular controls

Sites with binary accept/reject but no category-level controls should add a preferences link. This reduces challenge risk on consent granularity grounds under GDPR Article 7.



Add cookie policy links to banners

Nearly half of GDPR-region banners lack a direct link to the full cookie policy. GDPR Articles 13 and 14 require transparency about processing at the point of collection.



Review pre-consent tracker suppression

For sites with high pre-consent non-essential tracker counts, audit GTM or CMP configuration to ensure tags respect consent state. Move non-essential tags to fire only on consent granted.



Complete GPC partial implementations

For sites where GPC reduces but does not eliminate data-sharing trackers, review each remaining data-sharing tag against the CMP's GPC consent configuration.

Tier 3 — California CIPA priorities

Good Practice Recommendations (continued)

**Add CIPA wiretapping disclosure language**

For any California-facing site using session replay, live chat, or pixel tracking, add explicit disclosure before those scripts execute that electronic communications may be intercepted or monitored. Counsel should advise on precise wording. A blocking cookie banner is ideal here.

**Review session replay and live chat before consent**

Where session replay or live chat is present before consent, assess whether deferral until after user acknowledgement is required. The combination of these tools with no disclosure language is the highest-litigation-risk configuration in this dataset.

**Add GPC opt-out disclosure to privacy policy**

Of the sites where a GPC policy page could be evaluated, two-thirds lacked any statement on GPC handling. CPRA requires covered businesses to disclose their GPC approach in their privacy policy.

These are starting points for a compliance review programme, not a complete legal assessment. Individual site architecture, data processing activities, applicable law, and revenue thresholds all affect which obligations apply. Engage qualified privacy counsel before making compliance decisions.

The scan results point to a simple lesson: a consent programme is only as strong as the technical controls behind the banner. These recommendations turn the main patterns from the cohort into practical checks that teams can use when reviewing their own consent stack.

Once the technical controls are working, the visible layer becomes easier to assess: equal prominence for accept and reject, clear settings and policy links, and regional language that matches the visitor.

COMMENTARY

"The quickest privacy win is often not a redesign. It is checking that the controls already on the page actually control the stack behind it."

— Carl Gottlieb, Banner Scanner

How This Report Was Produced

Banner Scanner continuously scans live websites from real regional vantage points, capturing network evidence before consent and after reject and GPC signals in clean browser sessions. Every figure in this report derives from a deterministic aggregated statistics file, so the numbers are reproducible rather than impressionistic.

Banner Scanner measures consent banner presence, CMP behaviour, tracker activity, GPC handling, privacy disclosures, and litigation-risk indicators across web estates at scale.

The next measurement cycle will repeat the same cohort, regions, and stat definitions, so progress is measured against this baseline.

Scan your own website and those of your competitors at bannerscanner.com