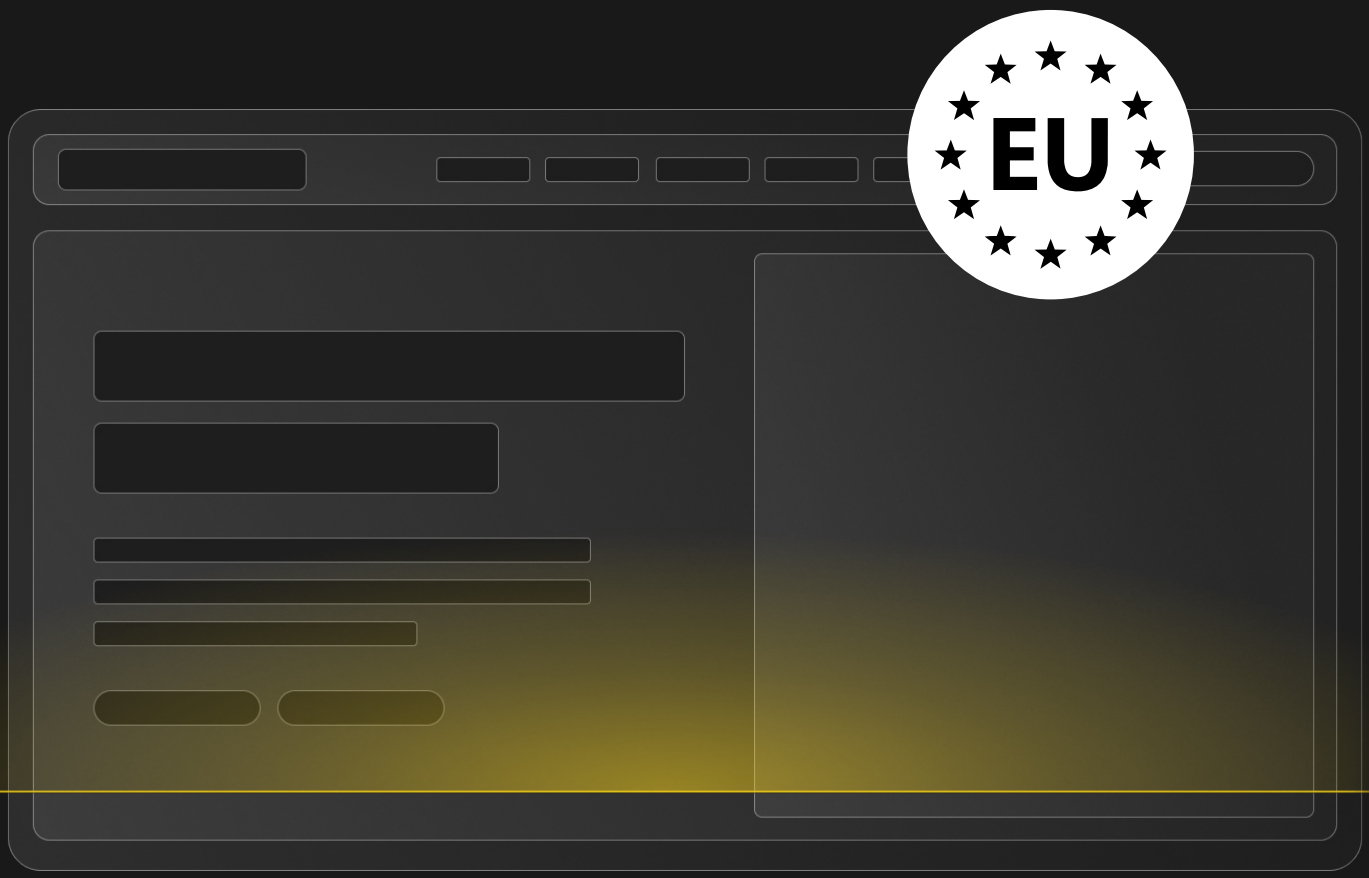
Where Europe's Top Websites Fall Short on Web Governance

Privacy Compliance Lessons from Europe's 1000 Highest-Revenue Websites



ObservePoint

Executive Summary

Running a website in Europe has never carried more regulatory weight. Eight years after GDPR came into effect, you might expect Europe's largest organisations to have the fundamentals in hand. What we found suggests otherwise, even though fines loom as nine-figure realities for enterprises in every sector. The European Accessibility Act now applies to digital services. And, data transfer rules continue to catch companies off guard, as TikTok's €530 million fine in May 2025 made clear.

Against that backdrop, ObservePoint audited 1000 of Europe's highest-revenue websites. What we found should concern any digital, legal, or compliance leader: consent mechanisms are inconsistently deployed, trackers fire before opt-in, a majority of sites send visitor data to U.S. servers, and nearly a third of pages carry at least one critical accessibility failure.

When problems appear at this scale, across organisations of this size and sophistication, a systemic change needs to occur.

KEY FINDINGS AT A GLANCE:

- **25.5%** of sites had no detectable consent manager
- **49.6%** of pages set third-party cookies with no user action taken
- **31.6%** of pages carry at least one critical accessibility failure (WCAG 2.1 AA)

Why This Matters Now

For much of GDPR's early history, enforcement moved slowly. Large fines made headlines, but smaller organisations and even some large ones waited to see how aggressively regulators would act. That period of uncertainty is over.

As of mid-2026, cumulative GDPR fines have surpassed €6.29 billion. The Irish Data Protection Commission, France's CNIL, Italy's Garante, and the Dutch Autoriteit Persoonsgegevens have all demonstrated willingness to move against well-resourced, sophisticated companies. The cases driving the largest penalties share a common thread: data transferred outside the EU without adequate safeguards, users left uninformed, or tags and cookies tracking before consent is given.

Meanwhile, the European Accessibility Act entered into force in 2019 and became enforceable in June 2025, extending legal obligations regarding digital accessibility beyond the public sector for the first time. Businesses that have not treated accessibility as a compliance matter, only an ethical one, are now exposed.

What the data shows is that regulatory requirements and day-to-day website practice have yet to converge, even at the top end of the market.

Methodology

ObservePoint Benchmark

We used ObservePoint to scan approximately 1,000 websites drawn from the Fortune 500 Europe list and the next 500 highest-revenue organisations. Each site was crawled 10 pages deep, starting from the homepage. Scans were conducted simulating visitor sessions from Germany, the EU's largest economy and one of its most active enforcement jurisdictions, to test consent posture and geolocation data flows as a European user would actually experience them.

Tests covered: tracking tag presence and vendor identification; consent manager detection; cookie behavior with no user action taken; Google and Bing Consent Mode signal analysis; geolocation data egress; and accessibility against WCAG 2.1 Level A and AA criteria.

Results reflect the state of each site during the audit window. Individual sites may have changed since. References to "third-party cookies" include any cookie set from a third-party domain and are not limited to advertising technology specifically.

Findings in Detail

1

Tags Start Firing Before Visitors Have A Say

When we visited pages without taking any action, as in, without giving consent, advertising and social tags were already running on a significant share of sites.

30.0%

of pages had advertising trackers present with no user action

11.0%

of pages had YouTube player tracking present with no user action

17.1%

of pages had social media trackers present with no user action

6.8%

of pages were still running the deprecated Google Universal Analytics tag

The advertising tracker figure is particularly notable. Thirty percent of pages are loading ad technology in a state where the visitor has expressed no preference, while under the ePrivacy Directive, the default state should be opted out. This is a structural misconfiguration often caused by implementation errors between a consent management platform (CMP) and tag management system (TMS) that many organisations fail to verify.

The continued presence of Google Universal Analytics on 6.8% of pages also deserves attention. Google formally sunset Universal Analytics in 2023. Sites still running it are not only losing data quality to a deprecated system, but they're also slowing down their pages with detritus.

What good looks like:

- No non-essential tags should fire before a visitor has engaged with a consent banner.
- Tag management platforms should block all non-essential categories by default; consent should unlock them, not the other way around.
- Deprecated tags like Universal Analytics should be on an active deprecation register with a deadline, not left running indefinitely.

2

Third-Party Cookies Are Widespread Before Consent

Nearly half of all scanned pages set third-party cookies with no user action taken. This matters because third-party cookies are the primary mechanism by which users can be tracked across different websites. Setting non-essential third-party cookies before consent is generally unlawful under the ePrivacy Directive.

49.6%

of pages set third-party cookies before any user action

567

unique third-party cookies observed across the dataset

56

distinct third-party cookie vendors identified

0.73%

of pages set non-secure (HTTP) third-party cookies

The top three vendors setting third-party cookies across European enterprise sites were Google, LinkedIn, and Adobe. These are core components of most organisations' marketing and analytics stacks. That is partly what makes the problem difficult to address: the tags causing compliance exposure are often the same tools that teams rely on for campaign measurement and lead attribution.

The presence of 56 distinct cookie vendors across the dataset also illustrates a governance problem that often goes unexamined. Tag sprawl, accumulated over years of campaigns, integrations, and vendor relationships, means that even a well-intentioned consent banner may not be blocking all the cookies it should. Consent platforms can only govern what the team knows is running. Auditing to discover the actual inventory is not optional.

What good looks like:

- Run a full cookie audit to build a complete inventory before assuming your consent manager covers everything.
- Review which tags are injecting additional third-party requests (piggyback tags) that may bypass your tag manager entirely.
- Classify every cookie vendor against GDPR legal bases; legitimate interest is not a blanket justification for tracking cookies.
- Revisit the cookie inventory frequently; every new campaign or vendor integration is an opportunity for new cookies to appear.

3

A Quarter of Sites Have No Detectable Consent Manager

Of the 1000 sites scanned, 254, or just over a quarter, had no consent management platform detectable on the homepage. For a dataset comprising Europe's largest organisations operating under GDPR, this is a striking result. A functioning consent mechanism is not a nice-to-have; it is the infrastructure through which GDPR's opt-in requirement is implemented.

It is worth noting that CMP detection has limits. Some implementations may not be identifiable from the homepage alone. But even accounting for that uncertainty, the number of sites without visible, functional consent UI is far higher than one would expect from organisations that have had eight years to address it.

Equally important is the question of whether CMPs that are present are actually working correctly. A consent banner that appears but fails to block non-essential cookies on opt-out undermines a privacy program. Presence is necessary but not sufficient.

What good looks like:

- Every page of a site should surface a consent mechanism, not just the homepage.
- Consent should be tested as an opted-out visitor: check which cookies and tags still fire after a visitor declines.
- CMP configuration should be reviewed whenever new vendors are added or tag manager setups change.

4

Consent Mode Adoption Is Incomplete and Often Incorrect

Google's Consent Mode is the mechanism by which a site signals to Google's ad infrastructure whether a user has consented to tracking. When implemented correctly, it allows advertisers to maintain some modelled reporting while respecting the privacy choices of opted-out users. When absent or misconfigured, Google's tags continue to operate as if consent had been granted.

Google Ads:

- 435 sites sent data to Google
- 205 of those (47.1%) sent any Consent Mode (gcd) signal at all
- Of those that sent a signal: 71.2% correctly signaled "denied"
- 28.8% signaled "granted" or "unknown," effectively bypassing consent

Bing Ads:

- 12 sites sent data to Bing
- 1 of those (8.3%) sent any Consent Mode signal
- That single site correctly sent a "denied" signal

Of the 435 sites sending data to Google, fewer than half sent any Consent Mode signal at all. Of those that did, nearly a third sent an incorrect signal, either "granted" when a German user had not consented, or an ambiguous "unknown" value that Google's systems may interpret as permission to proceed. The net effect is that a substantial portion of sites using Google advertising are transmitting signals that do not accurately reflect their users' choices.

Bing's numbers barely register: one site out of twelve. Microsoft's Consent Mode implementation appears to remain an afterthought, despite Bing Ads being a material channel for many European advertisers.

What good looks like:

- Consent Mode should be implemented for every ad platform in use: Google, Bing, and any other that supports it.
- The signal sent should match the user's actual consent state: "denied" for opted-out users, "granted" only for those who have explicitly consented.
- Test Consent Mode behavior from European IP addresses specifically, using a simulated opted-out session.

5

95% of Pages Send German Visitor Data to the United States

When we simulated a visitor browsing from Germany, 95.5% of scanned pages transmitted data to servers in the United States. This is the most consistently problematic finding in the dataset, and the one most directly tied to the largest GDPR fines in history, including Meta's €1.2 billion penalty in 2023 and TikTok's €530 million fine in May 2025, both of which centred on EU-to-US data transfer failures.

A transfer to the U.S. is not automatically unlawful: the EU-U.S. Data Privacy Framework, operative since 2023, provides a valid transfer mechanism for certified organisations. But the sheer volume of U.S.-directed traffic, touching virtually every site in the dataset, suggests that many organisations are not actively auditing which transfers are occurring, let alone whether

A sample of non-European geolocations for pages scanned from a German IP:

United States	**95.51%**	Russia	**0.08%**
Canada	**0.93%**	Chile	**0.02%**
Japan	**0.17%**	UAE	**0.01%**
Brazil	**0.17%**		

Excluding the U.S., 1.45% of pages sent data to non-EU countries.

What good looks like:

- Map your data flows by conducting regular audits from European IP addresses.
- For each non-EEA destination, verify that a valid transfer mechanism is in place: an adequacy decision, Standard Contractual Clauses (SCCs), or binding corporate rules.
- U.S.-based vendors should be checked against the EU-U.S. Data Privacy Framework registry; certification does not automatically extend to all subsidiaries or use cases.
- Data flows to jurisdictions without an adequacy decision should be reviewed as a priority.

6

Accessibility Failures Are Pervasive and Now a Legal Obligation

The European Accessibility Act entered enforcement in June 2025, establishing for the first time a consistent, EU-wide legal standard for accessibility across private sector digital products and services. Accessibility has been an ethical expectation for years. It is now a legal requirement.

The audit tested pages against WCAG 2.1 Level A and AA criteria, the standard referenced by the EAA. Nearly a third of all pages carried at least one critical failure at this level.

31.6%

of pages had at least one critical WCAG 2.1 AA issue

The three most common critical failures across the dataset:

- ARIA attributes must conform to valid values WCAG 2.0 · Level A · Criterion 4.1.2 (Name, Role, Value) Affected 12.64% of pages
- Images must have alternative text WCAG 2.0 · Level A · Criterion 1.1.1 (Non-text Content) Affected 7.84% of pages
- Buttons must have discernible text WCAG 2.0 · Level A · Criterion 4.1.2 (Name, Role, Value) Affected 7.74% of pages

Missing image alt text and buttons without labels are among the most basic accessibility requirements and among the most straightforward to fix. Their prevalence at this scale reflects not technical complexity but the absence of accessibility in routine development and QA processes. Screen reader users, keyboard-only navigators, and users with visual impairments encounter these failures directly. For Europe's largest organisations, this represents a significant portion of potential customers being actively excluded.

It is also worth noting that automated scanning catches a reliable subset of accessibility failures. Manual testing by accessibility specialists is required to identify others. The 31.6% figure should be read as a floor, not a ceiling.

What good looks like:

- Automated accessibility scanning should be integrated into your deployment pipeline to catch issues before they reach production.
- Complement automated scanning with manual reviews by accessibility specialists; some failure categories cannot be detected programmatically.
- Track accessibility fixes with clear owners and deadlines. Like technical debt, accessibility debt only grows if you ignore it.
- Train development and QA teams on EAA obligations and WCAG 2.1 criteria. Awareness is the first step to prevention.

Supplementary Data: Page Performance Baseline

The audit also captured core web performance indicators across the dataset. These are relevant to governance conversations because slow pages and excessive tag bloat are often symptoms of the same underlying problem: a lack of oversight over what is loading on each page.

- Average Largest Contentful Paint (LCP): **2.23 seconds (target: under 2.5s)**
- Average Time to First Byte (TTFB): **0.69 seconds (target: under 0.8s)**

The good news is that the aggregate averages sit within broadly acceptable ranges. But averages obscure variance: sites with heavy third-party tag loads or unoptimised media will perform significantly worse than the mean. Tag governance and page performance are not separate conversations.

Enforcement Context: What Regulators Have Actually Done

The following actions represent some of the most significant GDPR enforcement decisions in recent years. They map directly to the failure modes identified in this audit: pre-consent tracking, inadequate data transfer safeguards, and insufficient transparency.

May 2025 — TikTok — €530M Transfer of EEA user data to China without adequate safeguards; failure to inform users of transfers. Irish Data Protection Commission · dataprotection.ie

October 2024 — LinkedIn — €310M Unlawful processing of user data for behavioural analysis and targeted advertising; no valid legal basis for first- and third-party data use. Irish Data Protection Commission · dataprotection.ie

August 2024 — Uber — €290M Transfer of sensitive personal data of EU drivers to U.S. servers for over two years without appropriate legal safeguards. Dutch Data Protection Authority · autoriteitpersoonsgegevens.nl

September 2023 — TikTok — €345M Inadequate protection of children's data; public-by-default accounts for minors; insufficient age verification. Irish Data Protection Commission · dataprotection.ie

May 2023 — Meta (Facebook) — €1.2B Transfer of personal data of EU/EEA Facebook users to the United States in violation of the Schrems II ruling. Irish Data Protection Commission · dataprotection.ie

January 2023 — Meta (Instagram) — €390M Reliance on contractual necessity as legal basis for processing personal data for behavioural advertising. Irish Data Protection Commission · dataprotection.ie

The pattern across these decisions is consistent: data moving outside the EU without proper safeguards, users tracked without valid consent or legal basis, and organisations that treated compliance as an exercise rather than a technical and operational reality.

A Practical Roadmap:
Three Pillars of Web Governance

The findings in this report are not difficult to understand. What is difficult is building the operational infrastructure to catch and fix them continuously, across complex websites maintained by multiple teams.

PILLAR 1

Audit Continuously and From the Right Geography

- Manual spot checks are insufficient for sites of enterprise scale. Automated scanning across privacy, analytics, accessibility, and conversion paths should run on a regular cadence.
- Test from European IP addresses. What a site does for a U.S. visitor and what it does for a European visitor should be different.
- Simulate both opted-in and opted-out consent states in every audit cycle. The opted-out state is where most violations live.
- Include Google and Bing Consent Mode verification as a standard audit check.

PILLAR 2

Know What Is Actually Running on Your Site

- Maintain a live inventory of every tag, cookie, and third-party vendor active on your website. The difference between what your tag manager shows and what is actually firing is often significant.
- Audit for piggyback tags, third-party scripts that inject additional tags outside your tag manager's visibility and therefore outside your consent manager's control.
- Map every data flow by destination country. For any non-EEA destination, verify the transfer mechanism: adequacy decision, SCCs, or binding corporate rules.
- Build deprecation timelines for legacy tech.

PILLAR 3

Establish Ownership, Process, and Accountability

- Website governance requires cross-functional ownership: legal, marketing, engineering, and privacy teams cannot operate in isolation. A governance charter that defines responsibilities and escalation paths is the foundation.
- Remediation should be tracked with clear owners and resolution deadlines.
- Report compliance posture to leadership regularly. Executives who are unaware of their site's actual behavior compared to regulatory requirements cannot make informed decisions about investment in remediation.
- Accessibility should be treated as a first-class compliance concern alongside privacy.