Unconsented Tracking in Sweden

A Study of Website Compliance Among Sweden's Leading Brands

Verified Data

This study was supported by
Search Integration

Author: Brian Clifton

February 2026

Verified-Data.com

Executive Summary

This study examines whether 40 leading Swedish brands technically enforce user choices made in consent banners—specifically, whether tracking stops when a visitor selects "Reject All."

The findings reveal a consistent pattern: **while consent banners are widely implemented, technical enforcement often lags**. In 23 of the 40 websites audited, tracking technologies—including Google Analytics and third-party pixels—loaded despite consent rejection.

However, these outcomes are not evidence of intentional non-compliance. Instead, they reflect a **systemic implementation gap**—one that arises from the complexity of integrating consent signals across tag management systems, marketing tools, and organisational workflows.

The good news: **this gap is both understandable and fixable**. With better monitoring, clearer ownership, and regular validation, organisations can align their technical behaviour with their compliance intent.

This report does not name or rank individual organisations. Its purpose is not to assign blame, but to identify common failure points and offer practical guidance for improving data governance in complex digital environments.

01 Introduction: The Challenge of Consent Enforcement

Under the GDPR and ePrivacy Directive, valid consent must be obtained before any personal data is collected via cookies, scripts, or tracking pixels. This includes analytics, advertising, and even some support tools.

A user's choice—whether to accept or reject tracking—must be respected not just in design, but in execution.

Yet in practice, many organisations face a disconnect:

The consent banner captures the decision, but the website does not enforce it.

Generally, this appears not due to negligence or disregard for the law. Rather, it stems from the operational complexity of modern web ecosystems:

- Multiple teams manage different scripts (marketing, IT, UX).
- Consent signals must propagate from the CMP (Consent Management Platform) to the tag manager.
- Scripts are added, updated, or reconfigured without reassessment of consent logic.

This study explores where and how that breakdown occurs—and how it can be systematically addressed.

The Price of Ignoring Consent

In September 2025, the French data protection authority imposed the largest penalty to date for failure to respect user consent choices, issuing a **€150M fine against SHEIN**.

This pattern is not limited to France. In Sweden, **Avanza Bank was fined €1.5M** and the pharmacy **Apoteket €3.7M**. Outside Europe, regulators are becoming similarly assertive. In the United States, the largest fine to date is **Disney's $2.75M** for consent failures.

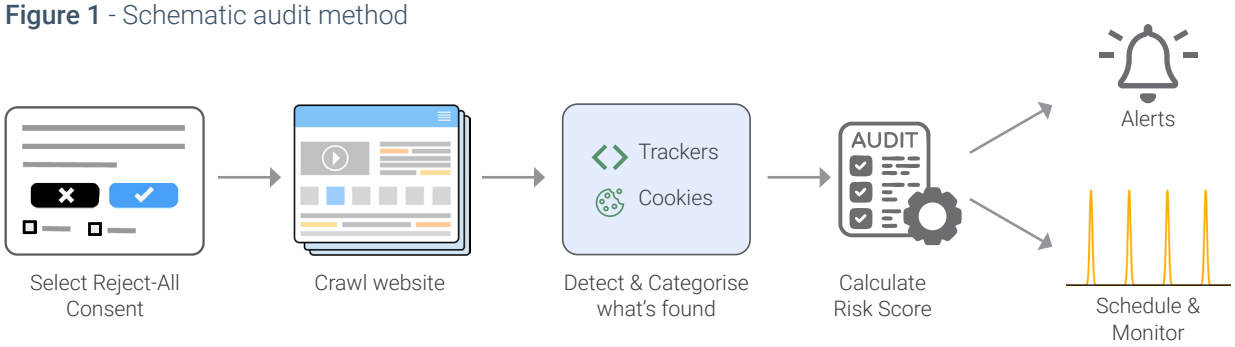
02 Scope and Methodology

The audit evaluated 40 websites representing major Swedish enterprises across sectors, including manufacturing, retail, finance, and media. Sites were selected based on public visibility and digital presence.

Each was tested using an automated workflow that simulates a real user interaction (see also Figure 1):

1. **Consent Selection:** Click "Reject All" on the consent banner.
2. **Crawl & Interaction:** Navigate 25 pages, simulating scroll, navigation, clicks, and video interactions.
3. **Network Monitoring:** Log and categorise all cookies and network requests.
4. **Analysis:** Identify unauthorised tracking and assign a Risk Score.

Figure 1 - Schematic audit method



The **Risk Score** quantifies the extent of unconsented tracking:

- **Critical Failures (10 points each)**: Clear violations where tracking should not occur after "Reject All". For example, an advertising cookie being set or an advertising pixel loading.
- **Warnings (5 points each):** Ambiguous cases where further investigation may be needed. For example, chat interaction widgets and support ticketing systems that may not be for data collection but still load components.

For example, a high-risk site was calculated as having a Risk Score of 175 based on advertising cookies and tracking pixels that should not have been set:

175 = (2 cookies x 10) + (15 pixels x 10) + (1 warning pixel x 5)

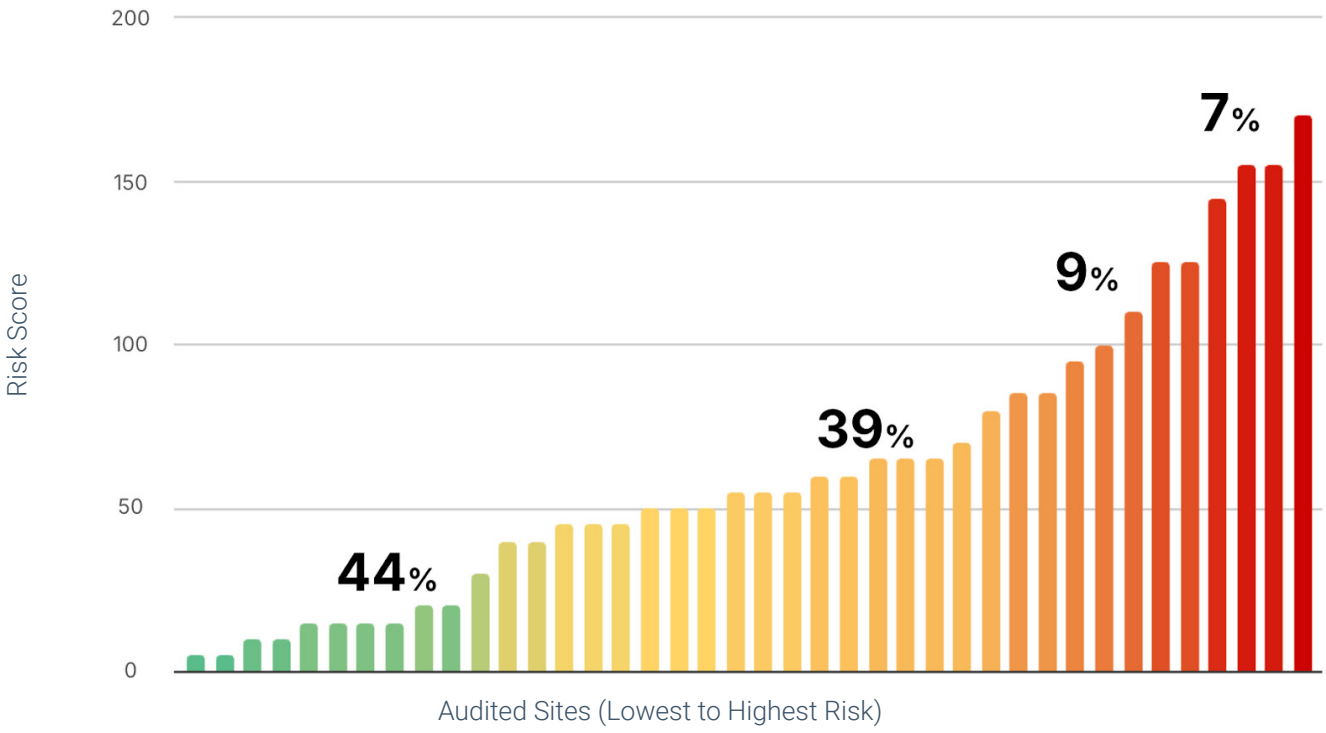
A lower score indicates stronger technical enforcement of user choice. The crawl settings used are shown in Appendix II.

03 Results & Analysis

3.1 A Spectrum of Technical Enforcement

The audited websites displayed a wide range of results. Some sites showed minimal tracking after rejection. Others, including large B2C and corporate sites, exhibited high levels of non-consented tracking - as shown in Figure 2.

Figure 2 - The distribution of Risk Scores across 40 sites



Best Practice (Score < 50):

44% of sites showed minimal unconsented tracking. These organisations demonstrate effective integration between consent and execution.

Moderate Risk (50–100):

39% of sites exhibited recurring but isolated failures—often due to misconfigured tags or overlooked integrations.

High Risk (Score > 100):

16% of sites showed persistent tracking, including analytics and advertising scripts firing after "Reject All."

The highest scores were not limited to any single sector. Both B2B and B2C organisations appeared across the spectrum, suggesting that compliance is driven by governance, not business model.

3.2 Where Consent Signals Break Down

The audit identified several recurring patterns—none of which may reflect malice, but all of which expose technical fragility.

Google Analytics Is the Most Common Failure

In 23 of 40 sites, Google Analytics loaded despite "Reject All." This is not a failure of Google, but of integration: the tag manager did not respect the consent signal.

Common causes:

- Google Analytics configured to fire on "All Pages" without a consent condition.
- Legacy GA3 code not fully removed.
- CMP and tag manager use different consent states (e.g., "analytics" vs. "performance").

Third-Party Scripts Load Without Validation

Chat widgets, support tools, and embedded content often load scripts that collect IP addresses or behavioural data—even when not required for core functionality.

These are frequently treated as "necessary," but may still process personal data and require consent.

CMP Alone Does Not Guarantee Compliance

A Consent Management Platform captures user choice—but does not enforce it. Enforcement depends on correct configuration in the tag management system (e.g. Google Tag Manager, Tealium).

If the tag manager does not "listen" to CMP signals, tracking proceeds unchecked.

Ownership Gaps Across Teams

Marketing teams deploy tools. IT manages infrastructure. Legal defines policy.

But no single team owns the end-to-end consent flow.

This leads to misalignment: a CMP is implemented, but tag configurations are not updated. A new campaign launches, but consent logic is not re-tested.

04 What This Means For Data Governance

The gap between consent and enforcement is not unique to Sweden. It is a **global challenge** in complex digital environments. But it is also a **manageable one**. Organisations can reduce risk through practical, incremental improvements.

1. Treat Consent as a Technical Control

Consent is not just a legal requirement—it is a technical condition.

Ensure that:

- All tracking scripts are integrated with consent checks.
- The tag manager uses the same consent categories as the CMP.
- Trackers requiring consent are disabled by default and only enabled when consent is granted.

2. Map and Monitor All Trackers

Maintain an up-to-date inventory of all scripts that process personal data.

Regularly audit:

- What scripts are active.
- Which collect personal data and therefore subject to consent regulations.
- Whether they respect “Reject All” and other consent options you offer.
- A small audit (25–100 pages) conducted regularly can catch regressions early.

3. Assign Clear Ownership

Designate a **data governance lead**—someone responsible for ensuring alignment between CMP, tag manager, and data policy. This role bridges marketing, IT, and legal teams, ensuring continuity.

4. Test, Don’t Assume

Even well-configured systems degrade over time. Conduct regular technical audits to verify that:

- “Reject All” truly stops tracking.
- New scripts comply with consent logic.
- Vendor integrations do not bypass controls.

05 Conclusion: From Compliance to Continuous Verification

This study highlights a critical insight: **consent capture is not the same as consent enforcement**.

The presence of a consent banner signals intent. But true compliance is demonstrated in code—when the website respects the user's choice.

The failures observed are not signs of wrongdoing. They are symptoms of complexity—of systems that evolve faster than governance can keep up.

The solution is not shame, but **measurement**. By regularly verifying technical behaviour, organisations can:

- Reduce legal and reputational risk.
- Strengthen internal alignment.
- Build real trust with their audiences.

This is not about perfection. It's about progress—and the commitment to align what users choose with what actually happens.

Next Steps: Improve Your Data Governance

To understand how your organisation compares, request an independent technical audit of your web properties. Using the same methodology as this study, the assessment verifies whether consent choices are consistently enforced across your digital ecosystem.

You receive a confidential report supporting internal governance, risk management, and regulatory readiness.

For further information or to discuss an assessment, contact: hello@verified-data.com.

About the Author

Brian Clifton is a data privacy and measurement strategist, best-selling author, and former Head of Web Analytics for EMEA at Google. He is the founder of **Verified Data** and advises organisations on building trustworthy, compliant data practices in the GDPR, CCPA, HIPAA era.

This study was supported by **Search Integration** - a Digital Intelligence Consultancy based in Sweden.

Appendix I - List of websites audited

Company	Country	Start URL	Consent
Alfa Laval AB	SE	https://www.alfalaval.se/	Reject all
AstraZeneca AB	SE	https://www.astrazeneca.se/	Reject all
Atlas Copco AB	SE	https://www.atlascopco.com/sv-se	Reject all
Boliden AB	SE	https://www.boliden.com/sv/	Reject all
Boozt	SE	https://www.boozt.com/se/sv	Reject all
Bubbleroom	SE	https://www.bubbleroom.se	Reject all
Cervera	SE	https://www.cervera.se	Reject all
Chilli	SE	https://www.chilli.se	Reject all
Din Sko	SE	https://www.dinsko.se	Reject all
Ellos	SE	https://www.ellos.se	Reject all
Essity AB	SE	https://www.essity.se	Reject all
Gant	SE	https://www.gant.se	Reject all
Gina Tricot	SE	https://www.ginatricot.com/se	Reject all
H&M	SE	https://www2.hm.com/sv_se	Reject all
Hemtex	SE	https://www.hemtex.se	Reject all
ICA Gruppen AB	SE	https://ica.se	Reject all
IKEA	SE	https://www.ikea.com/se/sv/	Reject all
Indiska	SE	https://indiska.com/se	Reject all
Jysk	SE	https://jysk.se	Reject all
Kappahl	SE	https://www.kappahl.com/sv-se	Reject all
MIO	SE	https://www.mio.se	Reject all
MQ	SE	https://www.mq.se	Reject all
Nelly	SE	https://nelly.com/se	Reject all
Nordic Nest	SE	https://www.nordicnest.se	Reject all
Peab AB	SE	https://peab.se/	Reject all
PostNord AB	SE	https://postnord.se	Reject all
Royal Design	SE	https://royaldesign.se	Reject all
Scania AB	SE	https://www.scania.com/se/sv/home.html	Reject all
Scorett	SE	https://www.scorett.se	Reject all
Securitas AB	SE	https://securitas.se	Reject all
Shein	SE	https://www.shein.se	Reject all
SKF AB	SE	https://www.skf.com/se	Reject all
Skopunkten	SE	https://www.skopunkten.se	Reject all
SSAB AB	SE	https://www.ssab.com/sv-se	Reject all
Svenskt Tenn	SE	https://www.svenskttenn.com/se/sv	Reject all
Systembolaget AB	SE	https://systembolaget.se	Reject all
Telia Company AB	SE	https://www.telia.se/	Reject all
TV4 AB	SE	https://tv4.se	Reject all
Vattenfall AB	SE	https://www.vattenfall.se/	Reject all
Volvo Cars AB	SE	https://www.volvocars.com/se/	Reject all

Appendix II - **Crawl Settings for the Study**