Regulated for Medicine, Unregulated for Data

Consent Compliance Failures Across Online Pharmacy Websites in Europe and the United States

A joint study by Verified Data and Ghostery.

Author: Brian Clifton

May 2026

Verified-Data.com

Study Objectives

The objective of this study was straightforward:

To determine whether pharmacy websites respected user opt-out choices after consent had been explicitly denied, and whether meaningful differences in consent compliance exist between US and EU/UK online pharmacies.

The audits focused specifically on whether websites continued loading or transmitting requests associated with analytics, advertising, profiling, or tracking technologies after a legally recognised opt-out signal had been expressed.

The study was designed to evaluate actual technical behaviour rather than published privacy policies or stated intentions.

Executive Summary

Pharmacies operate within one of the world's most highly regulated sectors. Medicines, prescriptions, packaging, dosage, manufacturing, and patient safety are all governed by strict legal and operational standards. Yet the same level of rigor is often absent when it comes to digital privacy and consent compliance.

This whitepaper presents the findings of a consent compliance audit conducted jointly by **Verified Data** and **Ghostery** across online pharmacy websites in Europe and the United States during Q1 2026. The study evaluated whether pharmacy websites respected explicit user opt-out choices under applicable privacy laws, including the General Data Protection Regulation (GDPR), the ePrivacy Directive, and the California Consumer Privacy Act (CCPA).

Before publication, we adopted a collaborative disclosure approach. The organisations included in the study were contacted privately. The objective was to encourage remediation and constructive engagement rather than public criticism.

The findings reveal a significant disconnect between stated privacy controls and actual technical behaviour. In the majority of audited cases, websites continued transmitting tracking-related requests even after users explicitly rejected consent or expressed an opt-out preference through the Global Privacy Control (GPC) signal.

In addition, while some organisations acknowledged receipt of communications, none engaged substantively with the technical findings prior to publication.

These findings raise important questions regarding governance, vendor oversight, consent implementation quality, and the broader state of privacy compliance within healthcare-related digital environments.

01 Introduction

Healthcare is fundamentally built on trust.

Patients expect organisations handling medications, prescriptions, and health-related products to apply the highest standards of care — not only in clinical and pharmaceutical contexts, but also in the protection of personal information.

This expectation is particularly important online. Pharmacy websites may process browsing activity connected to highly sensitive topics including chronic illness, fertility, sexual health, mental health, addiction treatment, and medication research. Such data falls within categories widely recognised as sensitive personal information under modern privacy regulation.

At the same time, healthcare websites increasingly depend on complex ecosystems of analytics tools, advertising technologies, consent management platforms (CMPs), tag managers, and third-party integrations. In many cases, these technologies are deployed across large digital estates with limited visibility into their actual runtime behaviour.

The result is a growing compliance challenge:

- Do pharmacy websites technically honour a user's decision to opt out of tracking?
- To answer this question, Verified Data conducted an independent audit study across pharmacy websites in Europe and the United States.

02 Why Consent Compliance Matters in Healthcare

Privacy violations within healthcare environments are not merely technical configuration issues.

Health-related browsing data can reveal highly sensitive information about an individual, including:

- Medical conditions
- Pregnancy concerns
- Sexual health products
- Addiction-related products
- Medication usage
- Mental health interests
- Fertility treatments
- Chronic illness management

When combined with advertising technologies, identity matching systems, or data brokerage ecosystems, this information may contribute to profiling, behavioural targeting, or discriminatory practices.

Regulators have already demonstrated increasing concern in this area.

Notable examples include:

- The U.S. Federal Trade Commission's **action against GoodRx** regarding the sharing of health-related data with advertising platforms. GoodRx were fined $1.5 million.
- Investigations by The MarkUp into hospital websites transmitting potentially **sensitive information through Meta Pixel implementations**.
- Enforcement actions by the Swedish Data Protection Authority against pharmacy operators including **Apoteket and Apohem** related to sensitive customer data transmission through Meta's "Automatic Advanced Matching" functionality.

These developments demonstrate that consent compliance failures within healthcare are no longer hypothetical risks. They are increasingly becoming regulatory, legal, and reputational issues.

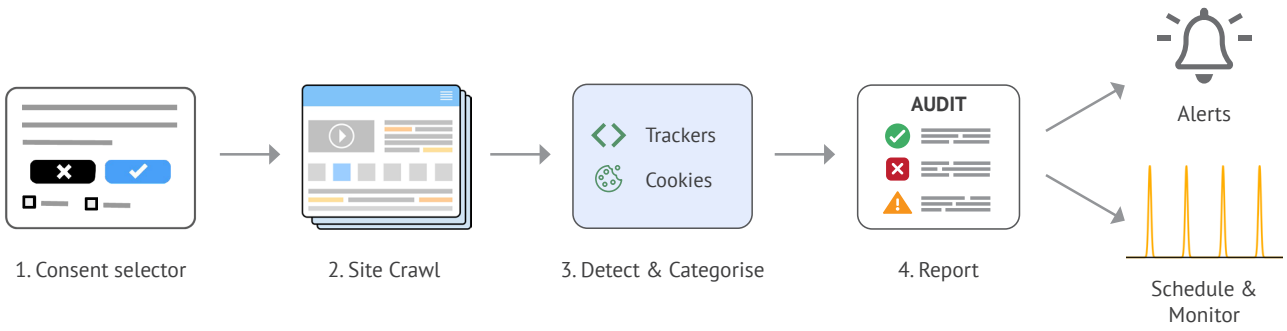
03 Audit Methodology

The audit study was conducted during Q1 2026 using the automated audit platform **Verified CONSENT**.

Each website listed in **Appendix I** 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



European Pharmacy Audits

European pharmacy websites were audited from servers located in Germany within the European Union.

The audit process simulated a user explicitly selecting a "Reject All" option on a consent banner. Following the consent interaction, the automated audit tool continued browsing the website by:

- Scrolling pages
- Clicking buttons and navigation links
- Triggering interactive elements
- Monitoring subsequent network requests

The audit system then analysed whether requests associated with analytics, advertising, profiling, or tracking technologies continued transmitting after consent rejection.

The **legal basis** for evaluation is:

- GDPR Articles 6(1)(a) and 7
- ePrivacy Directive Article 5(3)

Where tracking-related requests continued after consent rejection, the behaviour was classified as a consent compliance violation.

United States Pharmacy Audits

United States pharmacy websites were audited from servers located in California.

Rather than interacting with consent banners directly, these audits simulated users expressing an opt-out preference through the Global Privacy Control (GPC) signal.

GPC is a legally recognised browser-based privacy signal under the California Consumer Privacy Act (**CCPA**). It communicates that a user does not consent to the sale, sharing, or processing of personal data for advertising and profiling purposes.

Following detection of the GPC signal, websites are expected to disable applicable third-party tracking and data sharing activities.

As with the European audits, the automated system continued simulated browsing activity and monitored subsequent network requests for evidence of continued tracking behaviour.

04 Key Findings

The study identified a consistent pattern across many audited pharmacy websites:

Tracking-related technologies frequently continued operating after users had explicitly opted out.

Observed behaviours included continued transmission of requests associated with:

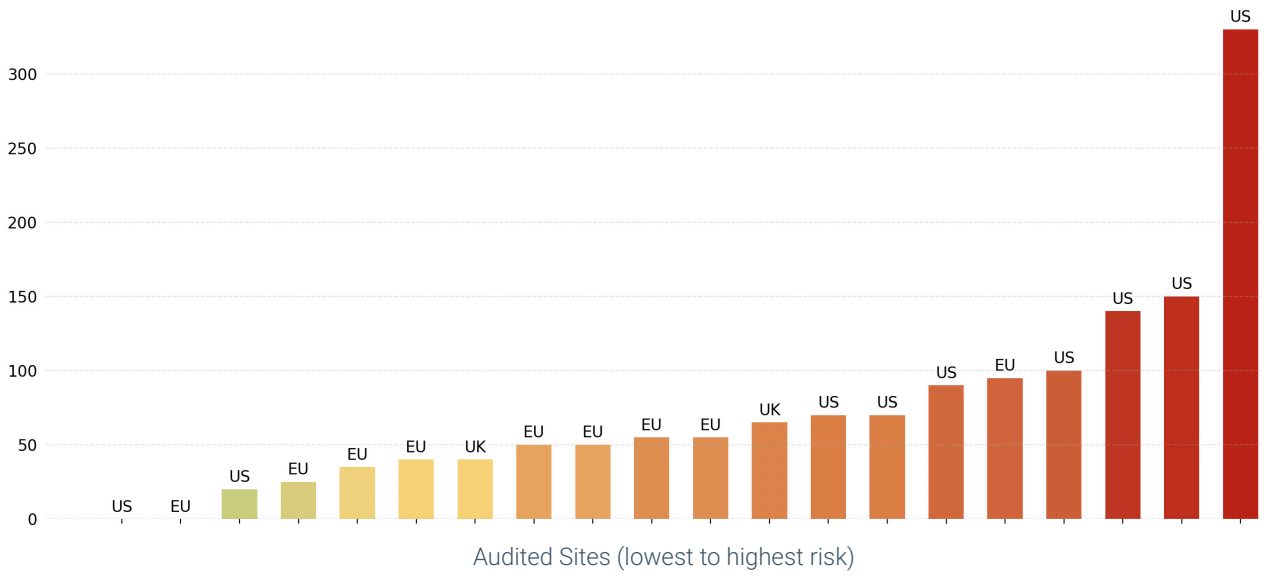
- Analytics platforms
- Advertising technologies
- Third-party marketing systems
- Tracking and profiling infrastructure

Figure 2 ranks each audited website in **Appendix I** by assigning penalty points for every tracker loaded and every cookie set despite consent being rejected. The results show that consent compliance failures were generally more severe among US online pharmacies than their UK/EU counterparts.

Seven of the ten worst-performing websites were US pharmacies, including the four highest risk sites in the study.

Only two online pharmacies — one in the US and one in the EU — were fully compliant, with zero unauthorised trackers loaded and zero cookies set after consent rejection.

Figure 2 - The distribution of Compliance Risk across the audited sites.



The findings suggest that, in many cases, consent banners and privacy controls may create the appearance of user choice without consistently enforcing those choices technically.

Importantly, the study does not conclude that these issues are necessarily intentional.

Modern digital infrastructures are often operationally complex. Common contributing factors may include:

- Misconfigured consent management platforms
- Poor tag governance
- Inherited legacy implementations
- Vendor configuration errors
- Incomplete consent integrations
- Insufficient validation and monitoring
- Limited visibility into third-party script behaviour

However, regardless of intent, the outcome remains the same:

Users who explicitly opted out were still tracked.

05 Industry Engagement Prior to Publication

Before publication, we adopted a collaborative disclosure approach.

The organisations included in the study were contacted privately and provided with:

- Technical findings
- Audit reports
- Supporting evidence
- Opportunities to discuss methodology and validation

The objective was to encourage remediation and constructive engagement rather than public criticism.

While some organisations acknowledged receipt of communications, none engaged substantively with the technical findings prior to publication.

This lack of engagement highlights a broader industry challenge: many organisations still lack mature operational processes for investigating and resolving consent compliance issues.

06 The Broader Compliance Problem

The findings of this study extend beyond pharmacy websites alone.

Across the wider digital ecosystem, consent banners have increasingly become standard website components. However, the presence of a banner does not necessarily guarantee compliant technical enforcement.

Where tracking technologies continue operating after an explicit opt-out, consent risks becoming performative rather than functional.

This issue is particularly significant in healthcare-related environments, where the sensitivity of personal information substantially increases both regulatory exposure and reputational risk.

As enforcement activity increases globally, organisations can no longer assume that privacy compliance is achieved simply by deploying a consent banner.

Effective compliance requires:

- Technical validation
- Runtime verification
- Ongoing monitoring
- Independent auditing
- Vendor governance

07 Recommendations for Healthcare Organisations

Healthcare organisations should treat consent governance as an operational compliance function rather than solely a legal or UX exercise.

Key recommendations include:

1. Independently Validate Consent Behaviour

Do not rely exclusively on vendor assurances or CMP dashboards. Independently test whether website behaviour matches declared consent states.

2. Continuously Monitor Runtime Activity

Website behaviour changes frequently due to deployments, third-party updates, marketing scripts, and inherited configurations. Compliance should be continuously monitored rather than periodically reviewed.

3. Strengthen Vendor Oversight

Many violations originate from third-party integrations or poorly governed tagging environments. Organisations should maintain visibility into all tracking technologies operating across their websites.

4. Treat Sensitive Data Environments Differently

Healthcare-related websites should apply stricter controls and governance standards than general commercial websites due to the nature of the data involved.

5. Align Legal, Technical, and Marketing Teams

Consent compliance failures frequently emerge from organisational silos. Privacy governance requires coordination between legal, compliance, engineering, analytics, and marketing functions.

08 Conclusion

Healthcare organisations are trusted with some of the most sensitive information people possess.

That trust increasingly extends beyond clinical care into the digital experiences patients use every day.

The findings of this study demonstrate that many pharmacy websites still struggle to technically enforce user privacy choices consistently, even when those choices are explicitly expressed through recognised consent mechanisms.

As regulatory scrutiny intensifies globally, organisations must move beyond symbolic compliance measures and ensure that privacy controls function reliably in practice.

Consent should not merely appear to work.

It must work technically, operationally, and consistently.

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.

Appendix I

List of websites audited (in no particular order)

Pharmacy	Region/Country	URL	Consent State
Apo.com	European Union / Germany	https://www.apo.com/	Reject all
Apotea	European Union / Sweden	https://www.apotea.se/	Reject all
Apotheke.at	European Union / Austria	https://www.apotheke.at/	Reject all
Apoteket AB	European Union / Sweden	https://www.apoteket.se/	Reject all
Apotek Hjärtat	European Union / Sweden	https://www.apotekhjartat.se/	Reject all
Chemist Direct	United Kingdom	https://www.chemistdirect.co.uk/	Reject all
DocMorris	European Union / Germany	https://www.docmorris.de/	Reject all
Luitpold Pharmacy	European Union / Germany	https://www.medikamente-per-klick.de/	Reject all
Pharma GDD	European Union / France	https://www.pharma-gdd.com/	Reject all
Pharmacy2u	United Kingdom	https://pharmacy2u.co.uk	Reject all
Zava	European Union / Ireland	https://www.zavamed.com/ie/	Reject all
CenterWell Pharmacy	USA	https://www.centerwellpharmacy.com/	GPC opt out
CVS Caremark	USA	https://www.caremark.com/	GPC opt out
CVS Health	USA	https://www.cvshealth.com/	GPC opt out
Express Scripts	USA	https://www.express-scripts.com/	GPC opt out
Hims & Hers Health	USA	https://www.forhers.com/	GPC opt out
Optum	USA	https://www.optum.com/	GPC opt out
Optum RX	USA	https://www.optumrx.com/	GPC opt out
Pill Pack	USA	https://www.pillpack.com/	GPC opt out
Walgreens	USA	https://walgreens.com	CPC opt out