COMPLIANT™

DATA PRIVACY:

THE COMPLIANCE ILLUSION

The Compliant 2022 Report: A Global Audit of Digital Media

CONTENTS

INTRODUCTION:

THE COMPLIANCE CLIFF EDGE

Global privacy regulations are forcing advertisers and publishers to transform how they collect, process and protect the personally identifiable information (PII) of website users. For legal and ethical reasons, protecting people's privacy is non-negotiable and consent has become the ultimate currency in digital advertising. However, notwithstanding the proliferation of privacy laws, consent is often little more than an illusion.

The Compliant™ 2022 Report summarises the findings of the largest global audit of advertiser and publisher-owned websites. The comprehensive audit objectively measures privacy compliance across the media supply chain and provides a reality check for the industry.

In the report, we reveal the true scale of the compliance challenge facing advertisers and publishers. We have used our Compliant Audit Technology™ (CAT) and our proprietary Data Safety Index™ (DSI) to measure systematic privacy and compliance risks, and benchmark the results by market, category and brand.

"Notwithstanding the proliferation of privacy laws, consent seems little more than an illusion."

THE ELEPHANT IN THE ROOM

The findings are stark: despite the concerted efforts of brands, publishers, and their CMP providers, the vast majority of the 500+ EU and US sites audited are acquiring data without the appropriate consent. Moreover, unauthorised third-party cookies and tags are collecting PII and leaking data into the website ecosystem, often without the site owner's permission. In some cases, third-party resellers are routinely collecting consumer data to build audience segments which they sell back to advertisers for targeting purposes. All too often, advertisers are buying data about their own consumers collected from their own sites.

This should concern all companies, regardless of their size, sector or business activities. Regulators have been investigating big tech (Amazon, Google, Instagram, and WhatsApp) and adtech (Criteo and the IAB's Transparency Consent Framework) for some time.

In September 2022, the EU set up its first office in Silicon Valley specifically to help the tech sector comply with European regulation. Data Protection Authorities are now broadening their scope, with advertisers and publishers firmly in the crosshairs as well. Significant fines have been levied against Grindr, H&M, Marriott, Sephora, and Saga to name a few, and new investigations are underway against others, including SkyBet.

While it is difficult to overstate the financial and reputational consequences of privacy compliance failures, regulatory fines are just one element to consider. In the face of data breaches, companies incur a host of other costs including legal fees, forensic investigations, improved security measures, lost data and, in some cases, irreparable brand damage. Time spent by employees responding to regulatory investigations can put significant pressure on limited resources.

THE TRUE VALUE OF COMPLIANCE

It is equally important to acknowledge the commercial benefits of privacy compliance – a transparent, well-managed media supply chain creates certainty, confidence, and agility:

- When questions arise, teams are faster to the answers. The easier it is for cross-functional groups to interrogate issues, clarify the data flows and assess the risks, the easier it is to be decisive, to experiment and, ultimately, to adopt new solutions. The converse is also true: uncertainty and ambiguity encourage risk aversion.

- Innovation in the media supply chain is resource intensive, requiring highly skilled and experienced talent. Robust compliance provides discipline and control, making it easier for teams to address inevitable tensions between commercial opportunities and people's rights and expectations of privacy. Poor compliance, on the other hand, is a drain on resources as employees are tied up resolving internal friction and building retro-fixes.

- Automated, always-on compliance monitoring ensures that issues and anomalies are quickly identified, allowing companies to react before problems snowball. Furthermore, if an issue is found on one website, companies can search for and address the same issue across their entire web estate. It is also easier to respond to complaints, enquiries and investigations, with demonstrable proof of compliance progress over time.

Put simply, businesses with privacy compliance technology and processes that are fit for purpose are faster, more innovative, more agile, and better able to grow with confidence.

> ***"Put simply, businesses with privacy compliance technology and processes that are fit for purpose are faster, more innovative, more agile, and better able to grow with confidence."***

DISPELLING THE ILLUSION OF COMPLIANCE

A HOUSE OF CARDS

In Europe, where GDPR-grade consent is required from website users before data is collected, a new market has emerged for Consent Management Platforms (CMPs). CMPs are an important element of privacy compliance as they help website owners secure consent to collect data and share it with a wide range of partners and third-party vendors in the digital advertising ecosystem.

With a CMP in place and consent secured, many advertisers and publishers collect and share user data believing that they're complying with privacy regulations. However, the Compliant™ 2022 Report suggests that the vast majority are living under a false sense of security because their CMP has not been implemented correctly.

CONSENT FAILURES ARE RIFE

Our audit reveals that many organisations have not yet implemented a CMP on their websites. Nine percent of EU advertisers and eight percent of EU publishers have no effective means of securing customer consent for collecting and sharing data. In the US the number is higher still, with 30% of advertisers and a staggering 91% of publishers lacking a CMP.

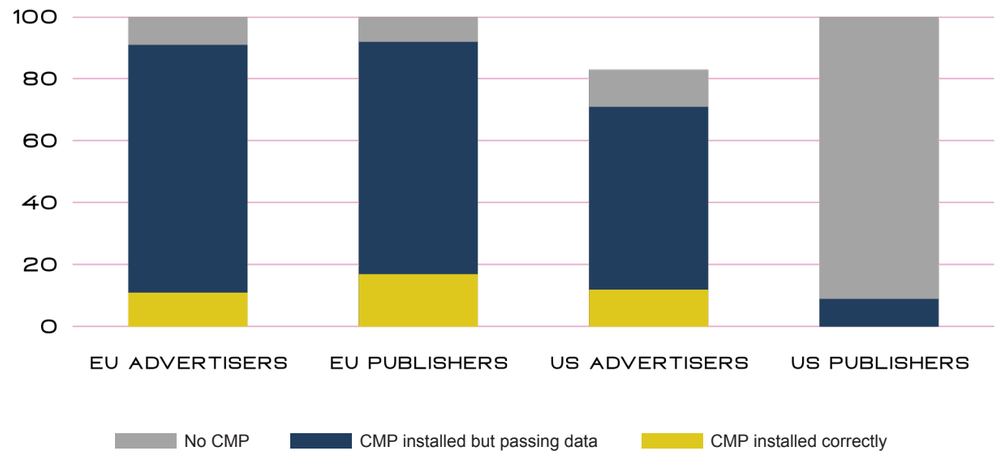
It may come as a surprise to those who have deployed a CMP that its existence is no guarantee of compliance. Far from it. Our analysis shows that of the 91% of the EU advertisers using a CMP, 88% are passing user data to third-parties *before* receiving consent from the data owners.

Similarly, of the 92% of EU publishers that have implemented a CMP, 82% are passing data before receiving consent.

All of the 9% of US publishers using a CMP pass on data before CMP choices have been made, as well as 84 % of the US advertisers with CMPs in place. Unlike the GDPR, US legislation does not require prior opt-in for certain cookies and tags. Nevertheless, if a US company collects PII from EU citizens, the GDPR consent requirements will apply by virtue of its extra-territorial reach.

"Consent does not equal compliance"

CMP IMPLEMENTATION BY REGION AND WEBSITE OWNER



KEY FINDING:
Advertisers across the EU and US that have deployed a CMP are operating under a false sense of security. While a well-placed CMP is one of the best tools in the box, compliance efforts must go further to address multiple risks across every part of the digital advertising ecosystem.

KEY TAKEAWAY:
CMPs are the current standard for securing consent. However, if they are not implemented correctly – and the vast majority are not – then privacy and regulatory compliance is impossible, both for the website owner and for anyone subsequently using that data.

"Given the uptick in regulatory scrutiny around GDPR, it's reasonable to believe that firms without CMPs will be the first to come under the spotlight. These organisations should move fast to ensure their data activities are legal."

PIGGYBACKING IS ENDEMIC

There are many other compliance issues for brands to consider, even if they have implemented a CMP correctly. One particular danger is the practice of "piggybacking."

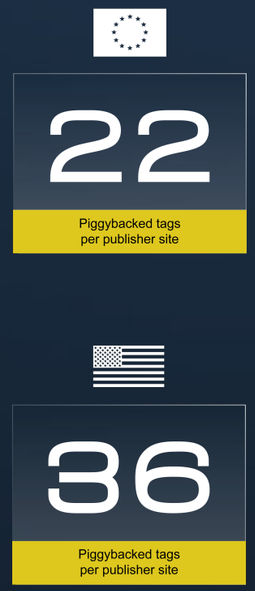
Piggybacking occurs when unauthorised cookies and tags collect data from brand and publisher websites without the site owner's permission. Piggybacking can lead to unconsented data being shared far and wide across the adtech ecosystem.

It is of huge concern that EU publisher websites support an average of 22 piggybacked tags. The average US publisher site is even worse off, with 36 tags piggybacked onto their site. The number of tags carried by advertisers varies widely between sectors, as does the difference between the average number of tags and the maximum recorded for a single site.

Tech/Telecoms, Entertainment and Automotive are the sectors with the highest prevalence of piggybacking in Europe, while Retail, Tech/Telecoms, and CPG are the sectors in the US most badly affected. At the extreme, the audit revealed that one UK publisher's site activated an astonishing 427 unauthorised tags/cookies.

There are industries where piggybacking is limited, notably in Online Services (including gambling and e-dating), and Financial Services in both the EU and the US. The former is an interesting case as e-dating websites contain less than one piggybacked tag and a maximum of two piggybacked tags. In all likelihood, this is an industry response to the adverse media coverage and regulatory fines against Grindr (see case study) and Ashley Madison which have fallen victim to large scale data breaches of highly sensitive information.

AVERAGE AND MAXIMUM PIGGYBACK TAGS DISCOVERED ON ADVERTISER-OWNED WEBSITES BY REGION



KEY TAKEAWAY:
Most websites are haemorrhaging data via unauthorised tags and cookies. With every additional tag on a site, the risk of unconsented personal data being shared with third parties increases, as does the corresponding liability of the website owner.

CASE STUDY

CONSEQUENCES OF NON-COMPLIANCE: Grindr

Grindr, a dating app for gay, bi, trans and queer people, was fined $7.1 million by Norway's data protection authority for passing unconsented user data to advertisers. The data included sensitive information related to users' sexual orientation. Grindr was found to be in breach of the GDPR because users were in effect forced to provide consent to share data in order to use the app.

"Piggybacking is a serious concern for most businesses, especially in sectors like healthcare where sensitive data is routinely transacted. All organisations need to be alive to this issue."

THE DATA RESELLER RISK

Data resellers pose additional risk. Data resellers are businesses that collect, organise and sell data to advertisers. Other organisations that are not pure data resellers (like the DSPs) also collect, organise and offer data to the market as part of their offerings. Due to the fact that so many companies are passing data before consent is secured, it's highly likely that data resellers attached to publisher and/or advertiser sites will do so too.

Even in the EU, where concern over GDPR fines is high and where the industry is moving away from third-party data collection, the data reseller risk remains a threat.

Our audit shows that advertisers in several sectors continue to support reseller tags on their websites.

Our data confirms that at least one reseller tag is present on 40% of EU publisher sites and 80% of US publisher sites. The average publisher in the US has five reseller tags collecting data from their site, compared to two in the EU. Certain advertiser categories typically have more reseller tags than others. Automotive, Entertainment and Tech/Telecoms are categories that are consistently allowing reseller tags inside of their data flows in both the EU and US.

AVERAGE AND MAXIMUM NUMBER OF RESELLER TAGS IDENTIFIED ON ADVERTISER AND PUBLISHER-OWNED WEBSITES BY REGION

40%
EU AVERAGE RESELLER TAGS

80%
US AVERAGE RESELLER TAGS

KEY TAKEAWAY:
Unmanaged reseller tags are an unnecessary risk. Advertisers and publishers should consult with suppliers to ensure that data is not collected and sold on to others.

SHARING DATA ON UNDERAGE USERS

In highly regulated industries such as gambling, alcohol, and food and beverages high in fat, sugar, or salt, there are additional sensitivities around collecting data from minors and other people under the legal age for those activities. To avoid collecting data from, or targeting, underage users, many companies deploy age-gating technologies, and will only collect data once a user has verified that they are of age.

However, our research shows that, for many companies, data collection is taking place before the agewall has activated. There's a statistical certainty that some of the data they collect is from people below the appropriate age, leaving them open to significant risk.

CASE STUDY

CONSEQUENCES OF NON-COMPLIANCE: AVAST

Software firm Avast was collecting data on its users' online activity without appropriate consent and sharing it with Jumpshot, a subsidiary that sold the data to advertisers. When this came to light, the result was a 13% hit to its share price, a GDPR investigation, and $25 million in costs for winding down Jumpshot.

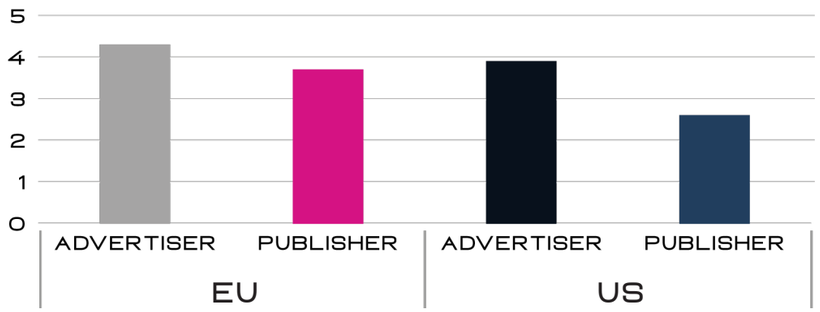
"Incorrectly implemented CMPs which unintentionally expose children to age-restricted marketing for companies in sectors like alcohol or gambling could put advertisers at odds with strict privacy laws and licensing obligations. There's also a clear moral imperative to protect minors from viewing materials that may be harmful to them."

WHAT IS YOUR PRIVACY COMPLIANCE RISK?

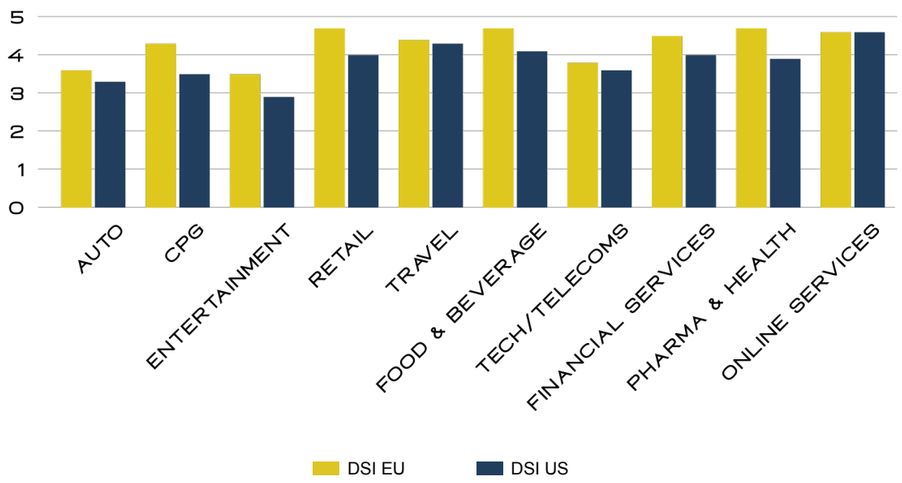
To help organisations monitor, measure and benchmark their privacy risk, Compliant has created the Data Safety Index (DSI). The DSI analyses many variables that impact privacy compliance and provides website owners with a score that shows them how they are doing, and how their efforts compare to benchmarks for their market, category and brand.

The index is measured on a scale of 0 to 5, with zero the highest risk and five the lowest. According to the DSI, advertisers and publishers in the US have a slightly higher likelihood of having issues with their data safety, scoring a DSI of 3.7 to the EU's 4.0. The industries with the lowest DSI scores and therefore with the greatest data safety risk include Entertainment, Tech/Telecoms, and Automotive.

DSI BREAKDOWN BY REGION AND WEBSITE OWNER



DSI BREAKDOWN BY REGION AND INDUSTRY



"There are currently no industry sectors with a DSI score of five. This demonstrates that compliance amongst brands and publishers in every category is still a challenge. It is essential they evaluate their data practices as a priority."

CONCLUSION:

THE IMPERATIVE FOR ALWAYS ON COMPLIANCE

Advertisers, publishers, and their adtech partners have responded in good faith to the requirements of privacy regulations. But as our analysis shows, the sheer complexity of compliance across the media supply chain means that many are unintentionally falling short of the mark.

This challenge is only set to get worse. As websites become more sophisticated and embed value-add functionality, such as personalised ads, augmented reality dressing rooms, shoppable content, AI chatbots, and more, ensuring compliance will become increasingly difficult. For every new feature added, there will be new data streams to audit, and new technologies and partners to review.

In this environment, ad-hoc compliance audits are not enough. As well as being resource intensive, sporadic audits provide little more than a moment in-time glimpse of a company's compliance risk – one which will be out of date the moment new data is ingested, new features and or new intermediaries introduced, deliberately or not, into the ecosystem. They are simply not conducted regularly enough to be of value.

In this complex and dynamic environment, the only way for brands and publishers to ensure that their compliance stack works as intended is through automated, always-on monitoring. This approach provides continuous visibility of the whole system, enabling brands to rapidly identify anomalies and potential sources of risk.

By continually testing the efficacy of their compliance posture, automated assessments can provide companies with peace of mind that their systems are performing as required. This provides a strong foundation on which businesses can rapidly integrate new digital services and experiences, and get ahead of the competition.

RESEARCH METHODOLOGY

The research was conducted from August-September 2022 on more than 500 (n=522) of the world's top advertiser and publisher websites. The research included the Ad Age Top 100 brands and over 200 of the top European publishers in the UK, France, Germany, Spain, Belgium and Austria, making up more than 86 percent of total site traffic in the region. It examined 16 different compliance-focused characteristics of the brand and publisher pages using Compliant Audit Technology (CAT), and the world's largest digital media compliance database (Data Safety Index) to benchmark and score risk and progress over time.

CONTACT US

To find out more about privacy compliance in digital marketing, or to arrange an audit of your owned and operated media, please get in touch:

contact@compliant.global
www.compliant.global
www.linkedin.com/company/compliant

COMPLIANT™

compliant.global