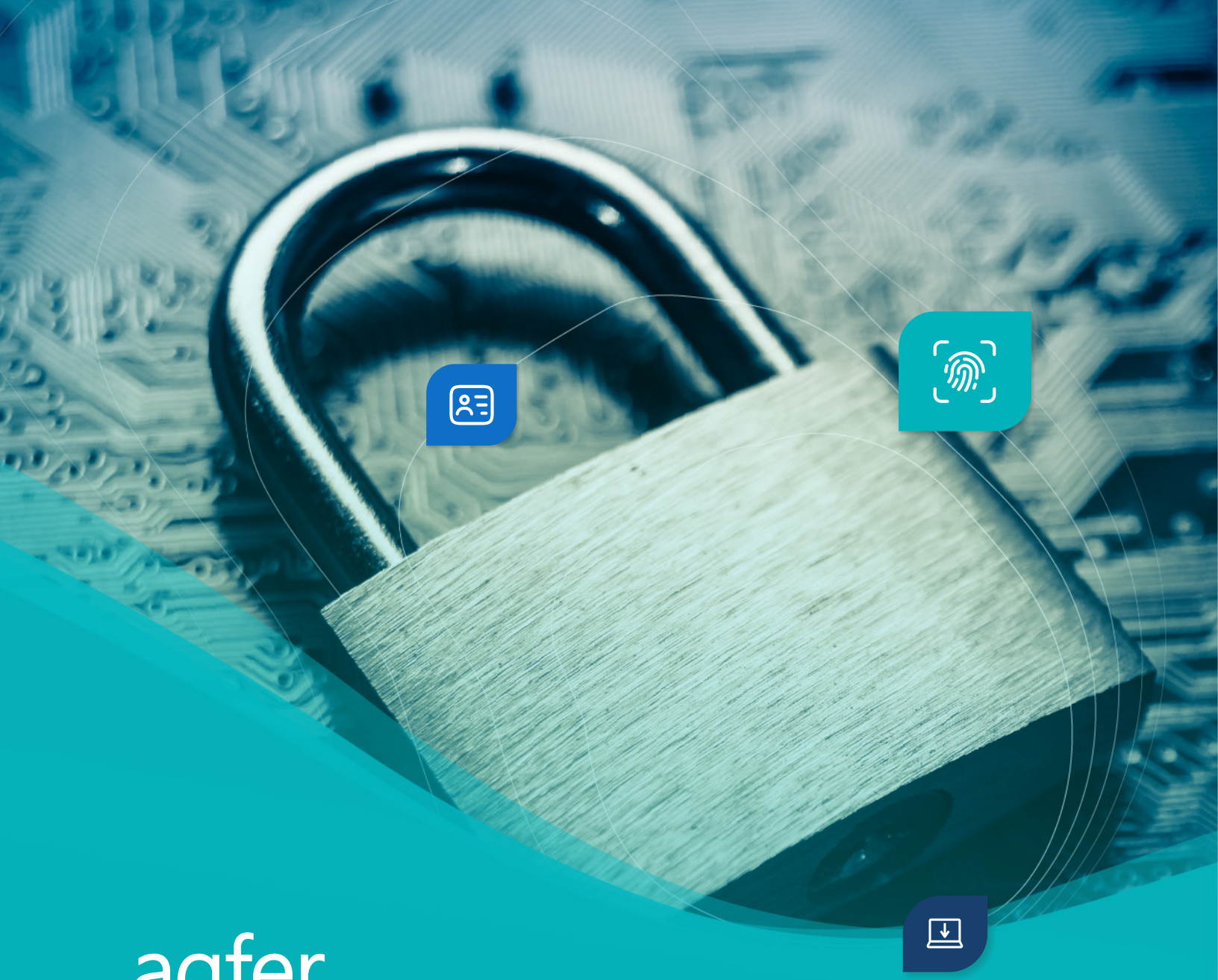


aqfer

State of Data Privacy & Security 2025

Table of Contents

aqfer

Executive Summary

Data security and privacy has never been more top-of-mind topics for modern consumers. Now, coming out of a decade full of large scale security breaches such as the 2013 hack affecting 3 billion Yahoo users to the more recent 2021 cyberattack on Microsoft affecting 60,000 global companies, individuals and businesses alike are more aware - and cautious about how their data is collected, secured and used.

In a challenging and evolving technology landscape, the brands that win will have a nuanced understanding of consumer preferences and priorities. Simply put: what's important to consumers must be important to brands. For the technology and marketing service providers companies that help brands better serve their consumers, data privacy and security must be prioritized.

This report digs deep into 2024 trends around data privacy and security given market factors like the deprecation of the third-party cookie and the rise of data clean rooms. We also share the privacy features and capabilities of technologies ready to handle the cybersecurity challenges of the future. Finally, we explore all of the data privacy and security features built into Aqfer products that help our customers build technology that's both flexible and future-ready, but also compliant and secure.

Dan Jaye
Aqfer Co-founder and CEO

Data Security and Privacy Have Never Been More Important to Brands & Consumers

Consumers in 2023 and beyond are more careful about how their data is handled. And it's easy to see why. Almost any digital action comes with risk. From downloading apps to joining new platforms to visiting websites, every interaction online asks users to trade data for services – either in the form of Personal Identifying Information (PII), collected behavioral data, or both.

With the pace at which technology evolves, it can be difficult for legislative bodies to enact privacy laws and regulations that adequately protect consumers. The onus is on technology providers to ensure the safety and security of the data they handle. Meanwhile, data breaches continue to occur at alarming rates. In 2023 alone, Firewall times reported on 40 major data breaches, spanning consumer, company and government data.

Today, consumers are more knowledgeable of data security and privacy than ever before. And they're worried about how their data is handled. According to a 2022 Norton study of cyber safety, 69% of global adults are more concerned than ever about their data privacy. But they don't believe it's possible to exist online without sacrificing their data. Studies show that the majority of Americans feel it's almost impossible to go through daily life without companies collecting their data.

MODERN CONSUMERS FEEL CONCERNED ABOUT DATA PRIVACY AND SECURITY

69%

of global adults are more concerned than ever about their data privacy
(Source: Norton, 2022)

90%

of consumers say online privacy is important to them
(Source: Surfshark, 2022)

81%

of consumers want to know more about how their data is being used
(Source: Surfshark, 2022)

55%

of consumers believe it's impossible to fully protect their online privacy
(Source: Norton, 2022)

For brands that love – and need – consumer data to run more efficient and targeted campaigns, studies like these should be a wakeup call. As we move into a more connected future, largely enabled by access to real-time data on consumer preferences and behaviors, keeping data safe and secure must be a top priority.

The good news is that consumers largely understand why and how their data is being used. And they're willing to sacrifice their data in exchange for better digital services and experiences.

Today's consumers don't just want personalized digital experiences – they actively expect them. According to a 2020 Salesforce study, 66% of customers expect brands to understand their needs and expectations. And they recognize that their data is the key to helping brands deliver those experiences.

CONSUMERS ARE WILLING TO TRADE DATA TO INFORM BETTER DIGITAL EXPERIENCES

61%

say they willingly sacrifice data privacy in exchange for convenience

(Source: Norton, 2022)

80%

of consumers will share personal data in exchange for deals or offers

(Source: Sailthru, 2022)

83%

of consumers are willing to share their data to create a more personalized experience

(Source: Accenture, 2022)

The Data Security and Privacy Stakes are High for Brands and Technology Providers

As governments regulate data usage, remaining compliant is becoming increasingly difficult for brands and technology providers that manage consumer data. Today, data privacy standards change seemingly by the minute. General Data Protection Regulation (GDPR) rules and regulations are ever-growing. And while GDPR is now ubiquitous in Europe, regulations evolve on a state-by-state basis in the US as well.

In recent years, headlines have been fraught with technology giants who've paid massive fines related to GDPR.

Recent GDPR-Related Fines for Technology Giants

Meta

May 2023 | Fined $1.3B
for violating the terms of the EU's GDPR by continuing to transfer EU users' data to the US without adequate safeguards

Google

December 2021 | Fined $164M
for violating the terms of the EU's GDPR by continuing to transfer EU users' data to the US without adequate safeguards

amazon

July 2021 | Fined $886M
by Luxembourg's National Commission for Data Protection, claiming their processing of personal data did not comply with EU law

For companies like Meta, Amazon and Google, million and even billion dollar fines could be viewed as an unfortunate cost of doing business. But for marginally smaller companies like Criteo, who was fined $40M in June 2023 by the French Data Protection Authority, accruing fines like these often lead to major operational setbacks.

> **"The company failed to comply with a 2020 decision by the European Union's highest court that Facebook data shipped across the Atlantic was not sufficiently protected from American spy agencies."**
>
> – New York Times, 2023

Cross-Border Transfer Adds Complexity to an Already Difficult-to-Navigate Landscape

Cross-Border Data Transfer is the transfer of personal data by controllers established in the European Union (EU) to recipients established outside the territory of the EU/EEA who act either as controllers or as processors. As a general rule, transfers of personal data to countries outside the European Economic Area may take place if these countries are deemed to ensure an adequate level of data protection.

Fundamentally, cross-border data transfer carries risk. Companies sometimes employ a "transfer the data and figure out the compliance later" approach. The problem is that the rules governing data transfer still vary quite a bit within the EU. GDPR was supposed to harmonize the rules across the EU, but it hasn't yet. Standards change all the time, and companies that think they're following the standard contractual clauses can and do get fined when the rules change.

Beyond GDPR

While the spotlight is often on the EU, they're not the only region with evolving data privacy regulations. GDPR is often the first framework that technology companies seek to master. But as companies scale globally, they'll need to keep a watchful eye on regulations across APAC, the Middle East & Africa and the Americas. While GDPR-like compliance rules are developing in these regions, we can anticipate stringent regulations and similarly heft fines for violations of those regulations in the coming years.

Here are a few to watch:

US States With Comprehensive Data Privacy Laws

STATE	LAW
California	California Consumer Privacy Act (2018)
Colorado	Colorado Consumer Protection Act (2021)
Connecticut	Personal Data Privacy and Online Monitoring (2022)
Utah	Utah Consumer Privacy Act (2022)
Virginia	Consumer Data Protection Act (2021)

Global Privacy Beyond Europe

COUNTRY	LAW
Japan	Act on the Protection of Personal Information (APPI) (2020)
New Zealand	Privacy Act (2020)
South Korea	Personal Information Protection Act (PIPA) 2011 (rev. 2020)
Kenya	Data Protection Act (2019)
Mauritius	Data Protection Act (2017)
Nigeria	Data Protection Regulation (2019)
South Africa	Protection of Personal Information (POPI) Act (2020)
Uganda	Data Protection and Privacy Act (2019)
Argentina	Personal Data Protection Act No 25,326, constitutional protections (2001)
Brazil	General Data Protection Law LGPD (2020)
Uruguay	Act on the Protection of Personal Data and Habeas Data Action (2008)
Canada	Personal Information Protection & Electronic Documents Act (PIPEDA) (2000)

Best Practices for Maintaining Data Security and Privacy Compliance

While consumers develop their own methods for securing their personal information online, brands and technology providers need to be doing more to secure their data, and protect the privacy of their users.

Today, maintaining security and privacy goes beyond double authentication logins and process documentation. From gathering user consent to data collection and sharing techniques, maintaining data security and privacy is an ever-evolving practice. Just as retiring technical debt is an ongoing exercise, so should be your approach to data security and privacy.

Here are a few best practices that brands and technology companies should be developing:

Compliance with data protection regulations

It's critically important to maintain compliance with GDPR in Europe and other privacy laws worldwide. This involves obtaining proper consent for data collection, implementing robust security measures, developing a framework for safe cross-border data transfer, and providing transparent information about data usage.

Data encryption and secure storage

Technology companies should adopt industry-standard encryption techniques to safeguard data in transit and at rest. Additionally, storing data in secure environments with access controls, firewalls, and intrusion detection systems is critical

Strong access controls and authentication

Implementing strict access controls and multi-factor authentication mechanisms helps prevent unauthorized access to sensitive data. Limiting user privileges and regularly reviewing access rights are essential practices.

Regular data audits and risk assessments

Conducting comprehensive data audits and risk assessments enable B2B technology companies to identify vulnerabilities, assess potential threats, and implement appropriate security measures. Regular monitoring and updating of security protocols are also necessary.

Employee training and awareness

Data privacy and security practices should be ingrained in the company culture. Regular training sessions for employees can help raise awareness about potential risks, teach best practices, and ensure everyone understands their role in maintaining data security.

Incident response and data breach protocols

Having well-defined incident response plans in place is crucial. This includes a clear chain of command, notification procedures, and steps to mitigate the impact of a data breach, such as informing affected parties and cooperating with regulatory authorities.

Third-party vendor management

Many B2B technology companies often collaborate with third-party vendors. It is crucial to ensure that these vendors have robust data privacy and security practices in place. Contracts should clearly outline responsibilities, including data handling and protection.

Privacy by design

From the earliest stages of development, privacy should be built into the fabric of every product. Implementing privacy-by-design principles ensures that data protection measures are integrated into the product architecture, rather than added as an afterthought.

Security and Privacy In Context

Keeping user data safe is certainly a noble goal. And maintaining compliance to avoid fines is just common sense. But many companies have more ambitious reasons for developing, maintaining and evolving solid practices for data security and privacy. These fundamental frameworks are critical for competing in today's technology landscape.

Between monumental operational changes demanded by the deprecation of third-party cookies and technology trends like AI and data clean rooms, companies need to collect and activate more data than ever before. And it simply can't be done if you don't have the future-ready data security and privacy frameworks in place first.

The old adage is "You can't put the cart before the horse." In this analogy, brands and technology companies are excited to push their next-gen technology cart forward... but that can't be accomplished without a strong horse bred to securely and compliantly collect, organize and activate the data required to power the cart.

On the Cookiepocalypse

As third-party cookies deprecate, collecting more, better first-party data is more important than ever before. A 2023 survey of technology leaders across Martech, AdTech and DaaS revealed that many companies don't feel prepared to weather the third-party cookie storm.

50% of respondents say that their own company and/or clients will be seriously affected when Chrome terminates support for third-party cookies. However, only 5% think their peers and competitors will be affected, suggesting a widely held belief that others are more prepared for the Cookiepocalypse.

Getting through the transition between reliance on third-party to the reliance on first-party will require an incredible amount of discipline when it comes to the collection and activation of data. Proper data security and privacy measures will be critical to ensuring companies are able to collect and organize the data required to power first-party data operations.

THE STRUGGLE TO MAKE USE OF FIRST PARTY DATA

51%

of organizations say third party data makes up the majority of data their company uses

(Source: Statista, 2021)

#1

technical priority for tech companies in 2023 was activating data in real time.

(Source: JBF Research, 2023)

70%

of tech leaders

say organizing data for activations such as analytics and marketing is time-consuming and difficult

(Source: JBF Research, 2023)

On Artificial Intelligence

Thanks to the overnight success of ChatGPT, AI is the unofficial technology buzzword of 2023. AI is here, it's mainstream, and people are using it for everyday tasks like planning vacation itineraries, writing emails and creating professional headshots. While governments scramble to regulate AI, technology leaders are already starting to warn against the dangers of unchecked AI.

Companies across industries are scramble to develop AI-powered feature sets. But due to the massive amounts of data required to power AI, it can pose an incredible risk to data privacy. Before developing AI-powered capabilities, companies must understand not only how to collect the unfathomable amounts of data required to feed their AI models, but also how to keep that data safe and secure.

"The importance of privacy in the digital era cannot be overstated. It is a fundamental human right that is necessary for personal autonomy, protection, and fairness. As AI continues to become more prevalent in our lives, we must remain vigilant in protecting our privacy to ensure that technology is used ethically and responsibly."

– Dr Mark van Rijmenam, CSP, Futurist

THE RISE OF DATA CLEAN ROOM TECHNOLOGY

The total Data Clean Room market size was estimated at USD 3.6 billion in 2022 and is expected to grow at a compound annual growth rate (CAGR) of 5.58% from 2023 to 2030

83% of technology leaders agree it's critically important to have a clean room that can ingest data from any platform in order to meet the needs of advertisers, publishers and industry partners

80% advertisers with substantial media budgets will utilize data clean rooms by 2023

On Data Clean Rooms

As the cookiepocalypse looms, one highly anticipated salve is the data clean room. A data clean room is a data collaboration solution that allow brands to safely and compliantly share data with vendors, partners and collaborators. Personally identifying information (PII) or restricted attribution data of individual users is not exposed to any contributors, which makes it impossible for them to identify and activate user groups without unique identifiers.

Data security and privacy are a hallmark of data clean room tech - but that doesn't mean most are doing data security and privacy right, or even well. A 2022 Insider intelligence survey showed that 45% of publishers believed that privacy was a concern that clean rooms need to overcome.

Cross border data transfer has become one of the biggest challenges and sticking points for clean rooms. Keeping up with international regulations is time consuming at best, and almost impossible for engineers to navigate.

Deploying a Future-Ready Data Security and Privacy Solution

Clearly, there's a lot to consider when building data security and privacy frameworks into software solutions. We're operating in a complex, ever-changing landscape. And the demand to bring new innovative solutions to market at record speeds has never been higher.

When deploying a future-ready solution, it's important to build not only for today's landscape, but for tomorrow's too. The Six Elements of Privacy Governance provide a helpful framework for planning privacy solutions.

6 ELEMENTS OF PRIVACY GOVERNANCE

Data collection: understanding current rules and regulation concerning the collection of data protocols, including cross-border data transfer concerns

Data Storage: Providing secure, customizable storage of pseudonymous or de-identified data

Enforcement: Ensure all policy restrictions are enforced with automated rules at the point of data distribution to partners and other external endpoints

Consumer Choice: Supporting consumer 'Right to Access' and 'Right to be Forgotten'

Data Processing: Ensuring that security best practices are followed (e.g., SOC 2) and adhering with regulatory compliance related to consumer privacy (GDPA, CCPA, etc.).

Data Auditing: Maintaining an audit trail of data subject record access

A Composable Approach to Data Security and Privacy

So how should a technology leader approach developing these extremely important privacy and security frameworks? Due to the ever-evolving nature of the technology landscape, international privacy regulations, and mounting consumer security concerns, taking a composable, "best-in-class" solution lens can be helpful.

Aqfer is a one-stop-shop that works together with best-in-class partners to bring our customer truly future ready, compliant solutions. Our build-it-together approach to developing novel technology offers customers a secure foundation on which to build their solutions, allowing our customers to focus on unique value, rather than critical, yet table-stakes functionality.

Let's dig deeper into the Aqfer approach to data security and privacy.

The Aqfer Approach to Data Privacy & Compliance

Data privacy, security, and cross-border compliance are topics that our teams think about constantly. Perhaps that's the influence of our CEO and founder, Daniel Jaye, who was part of the teams that pioneered digital privacy standards and technologies from the outset of the Internet.

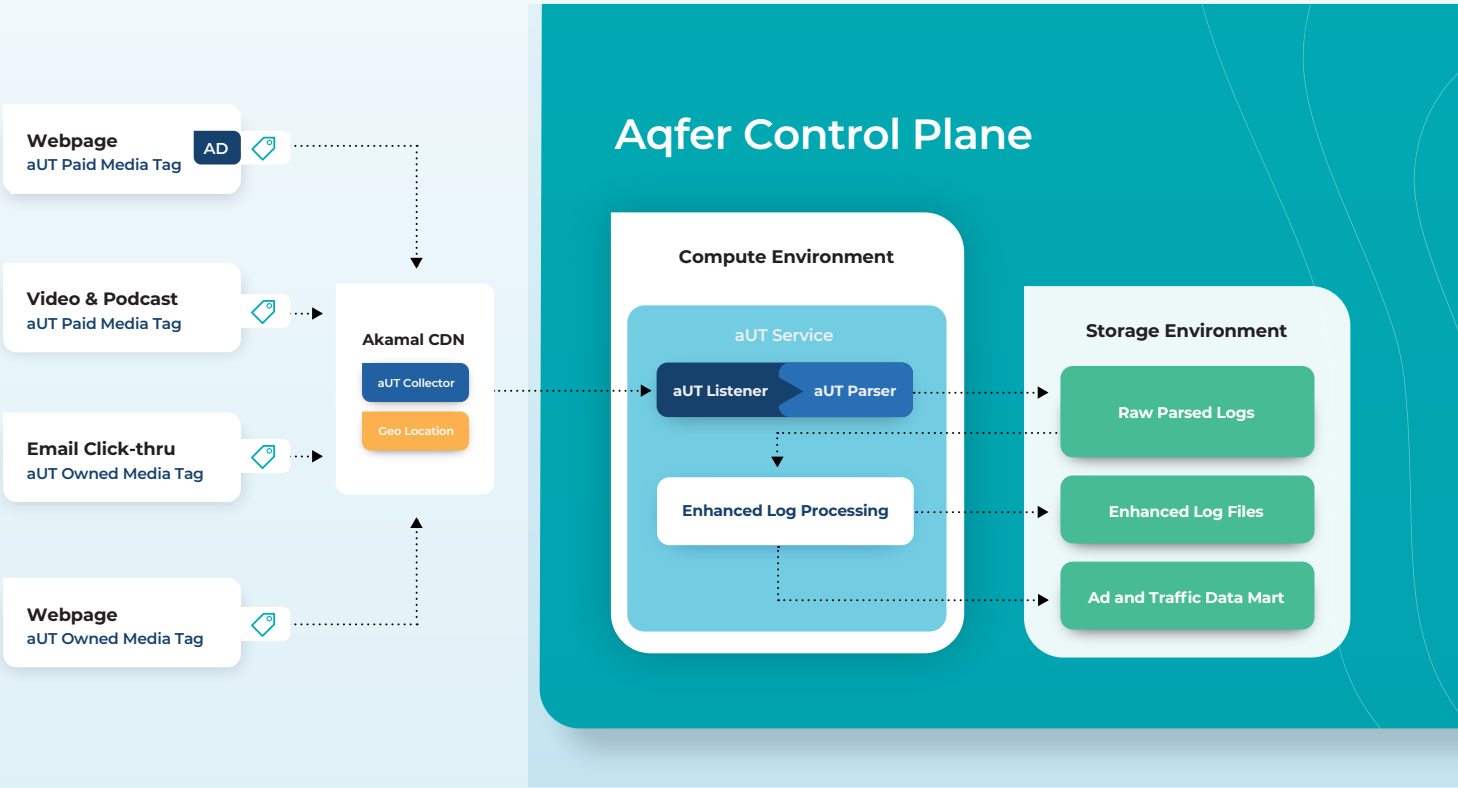
As a result, Aqfer made privacy governance an intrinsic part of the DNA of our Marketing Data Platform-as-a-Service (MDPaaS). Strategic and tactical data use and governance are inseparable, thus Aqfer's products are built around a proactive transactional privacy framework as opposed to the typical, more reactive administrative privacy governance. Essentially, Aqfer manages, governs, and audits as part of the "data plane" versus the "control plane."

MDPaaS provides clients with cost-effective, secure, and regulatory-compliant approaches to collecting and managing consumer data and tracking consumer behavior. MDPaaS does not require expensive technical resources to manage, develop, or support, and Aqfer's privacy compliance framework is built directly into the core products that make up MDPaaS: Aqfer Universal Tag (aUT) and Aqfer Marketing Data Platform (aMDP).

Here's a look at how data privacy, governance, and security are seamlessly managed by MDPaaS.

Edge-Based Tag Management Prevents Unauthorized Data Collection

Aqfer Universal Tag, the proprietary first-party universal tagging solution within MDPaaS, is deployed as an edge-based tag management solution via Akamai, a global content delivery network (CDN) and cloud services provider. aUT's edge-based deployment on Akamai gives clients (users) the ability to make granular decisions about what data to collect (or not collect) based on the consumers' physical locations. aUT clients can create and deploy customized aUT Tags that adhere to the specific data privacy regulations of the region/jurisdiction where any consumer's data is being captured.



This essentially creates a “privacy firewall” that prevents unauthorized cross-border data collection or transfer that adheres to prominent consumer privacy regulations. Because the logic and data capture both occur on the edge via a transactional approach, the client (user) is never in possession of consumer information they should not have at any point – eliminating concerns about hefty data privacy fines and subsequent business repercussions.

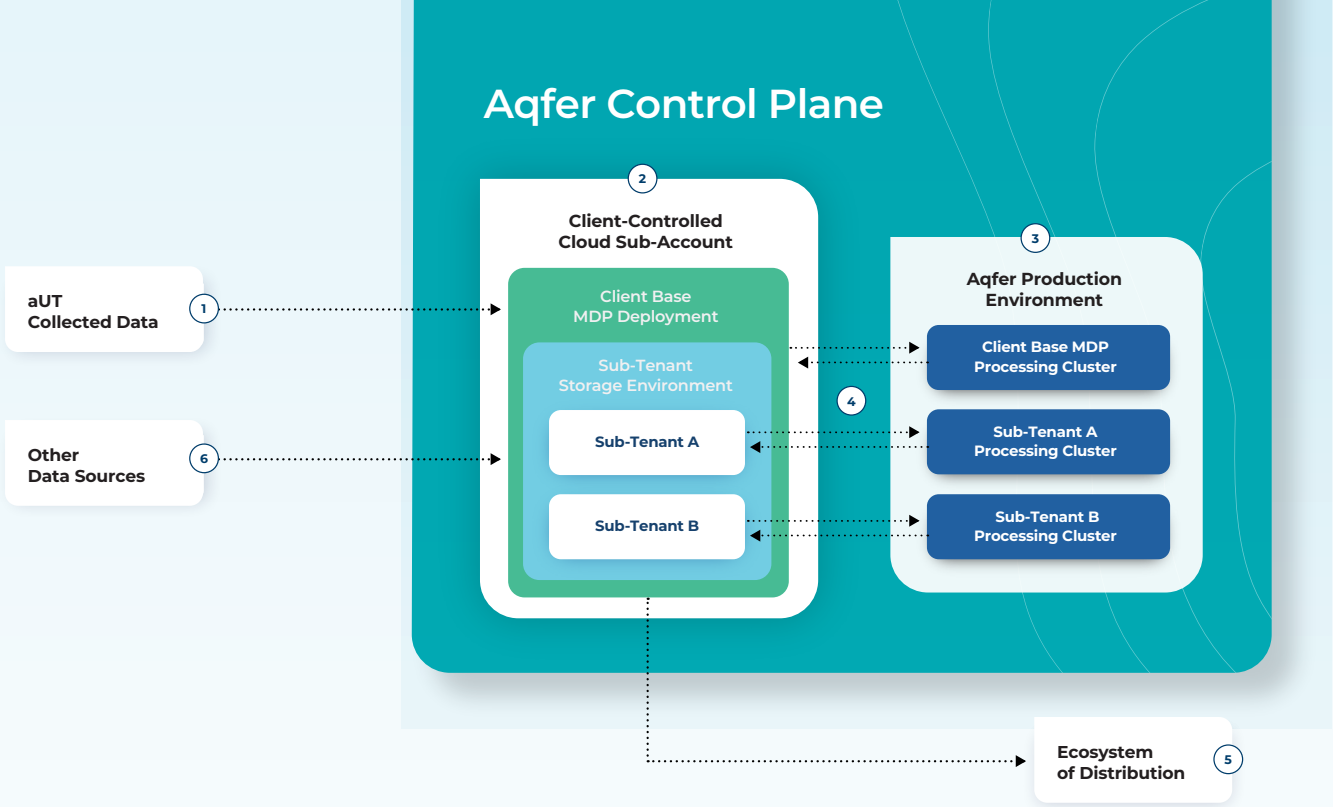
Users can also plug a consent management platform into aUT to further manage consent and permissioning. aUT’s privacy framework is also compliant with the IAB’s recently-established Global Privacy Platform protocol.

For example, if the consumer is based in the E.U., the aUT Tag can be configured to capture only the information allowed per GDPR consumer data privacy requirements. If consent is given by the consumer, standard aUT data is logged; if consent is not given, then no personal/ pseudonymous data is logged. This same ability also applies to consumer data privacy laws and regulations currently established by various individual U.S. states (CCPA, for example).

A secure, client-controlled environment for data management and data collaboration

With aMDP, all marketing-related data gets managed in its source form (as permitted under governance guidelines and compliance mandates). Most data management solutions can only apply data governance and consumer privacy rules and requirements after data has been imported into the solution. But aMDP’s transactional governance approach allows users to apply any and all necessary data governance and consumer privacy rules/requirements as part of the data import process. This ensures that no unauthorized or unlawful data is stored and used downstream by the client (user).

aMDP’s transactional (time of import) data governance approach ensures compliance with a variety of consumer privacy regulations (GDPR, CCPA, ‘Right to Be Forgotten’, etc.) and makes aMDP ready for any and all future policy/regulation changes.



1

Aqfer's edge-based, in-region privacy controls ensure no unauthorized data collection and/or cross-border data transfer occurs.

2

Client-controlled virtual private clouds isolate data at rest and can be configured for subtenancy with multiple sub-clients with full data encryption.

3

Aqfer's SOC2-certified processing separates storage from compute to improve performance and security as all data in this environment is destroyed after processing.

4

Metadata attached to each record includes audit trails to show when data has been collected, processed, or distributed to external sources

5

Rules-based policies can be set up to match the appropriate privacy consent frameworks in various regions around the world

6

Consumer consent from outside data sources can be merged into the Aqfer MDP to ensure regulatory compliance and adherence to a consumer's explicit choices

Another key differentiator between aMDP and other "similar" data storage frameworks, such as data warehouses and customer data platforms, is that all data that passes into and out of aMDP does so within the client's (users) own virtual private cloud environment. Essentially, aMDP becomes ClientMDP, giving you complete control over the data that passes into and from it at all times. This means that any data moved into and transformed by aMDP is never seen or even accessible by Aqfer or any other third-parties, ensuring the absolute highest standard of data governance and control.

MDPaaS also lets clients (users) create secure data collaboration environments (SDCE), commonly called data clean rooms, for secure data sharing use cases. These SDCEs are created using aMDP's underlying technology and therefore are deployed in the client's (users) virtual private cloud environment. This means you fully own and control the clean room and all data they bring to it, whether that data be first- or third-party. Further, all data brought into an MDPaaS SDCE, like with other clean room solutions, is fully encrypted to ensure that it is only viewable by the party from which the data originated.

Do-It-Together with Aqfer

Aqfer offers a Marketing Data Platform-as-a-Service that empowers marketing solution providers and their customers to bring applications to their cloud data, facilitating ruthlessly efficient data collection and management to deliver real-time insights, decisions, and activation in a privacy-first world.

As a low-code alternative to building everything in house, clients supercharge their intellectual property and accelerate their business with the Aqfer platform. Specifically, Aqfer provides future-ready solutions for identity management and resolution, secure data collaboration via data clean rooms, media analytics and attribution, and universal tag management. Collectively, these solutions enable marketing solution providers to bring configurability, repeatability, and scalability to their own offerings along with substantial cost savings and efficiency improvements.

Ways to Learn More

We're here to help and answer any questions about big data, data integration, data analytics, performance and pricing. We look forward to hearing from you.

Have a question?
Drop us a note at info@aqfer.com

- Guided case study review
- Personalized demonstration geared to the areas of data technology important to you
- Evaluation and road map to seeing better alternatives
- Simple question and answer session with an expert to satisfy your curiosity

aqfer

Contact us to Get Started