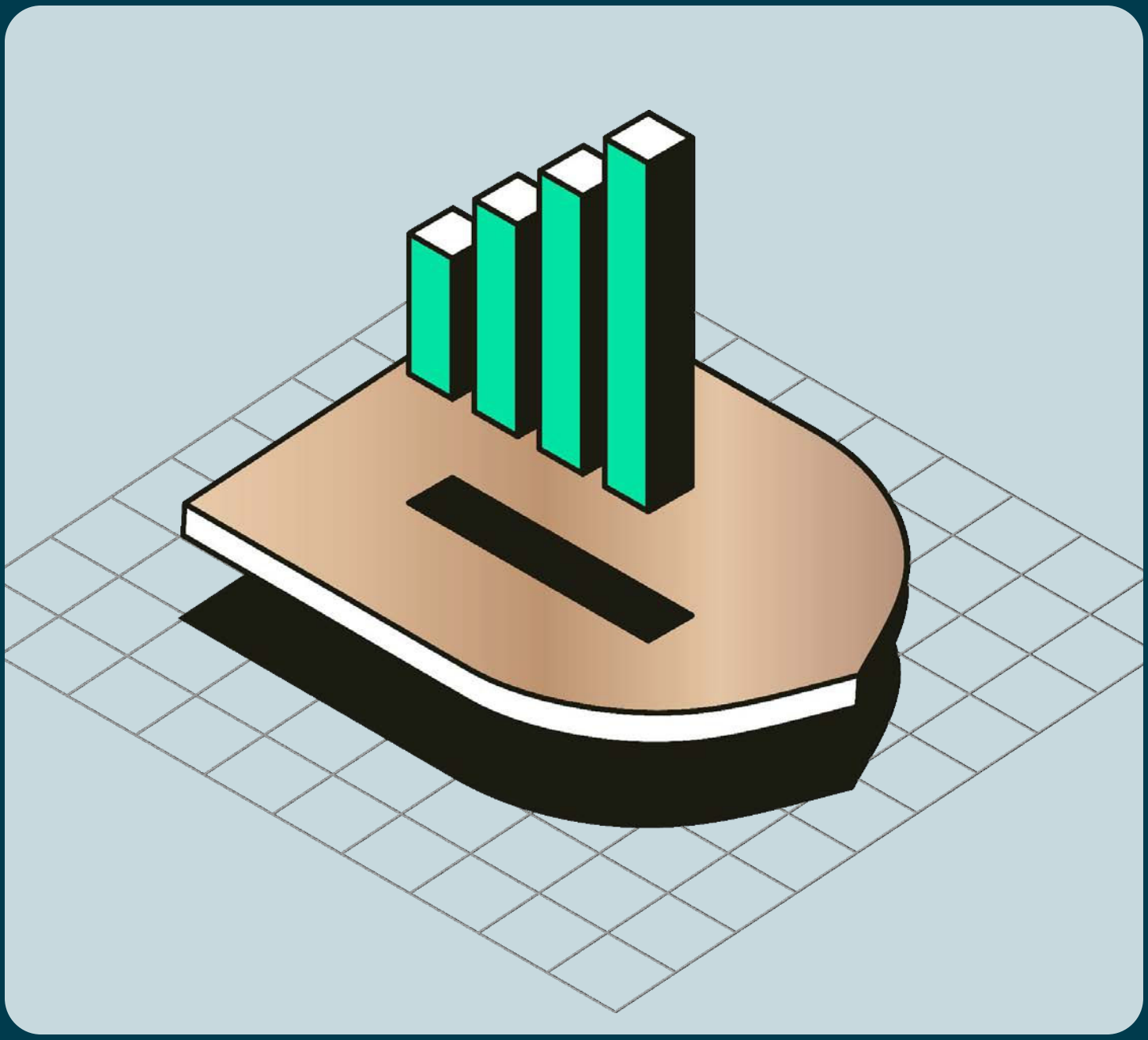
DataGrail

REPORT

2024 Data Privacy Trends

DataGrail's Data Privacy Trends Report



Executive Summary

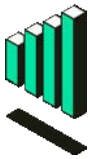
Consumers are more aware of the risks related to sharing personal information online. Data privacy laws are getting stricter. And data privacy is more important than ever, especially as GenAI becomes the new standard. DataGrail's 2024 Data Privacy Trends Report shows how these factors are playing out on the ground and provides a benchmark for businesses to see how they are tracking.

Businesses are receiving more privacy requests, also known as Data Subject Requests (DSRs) every year; **we saw a 246% increase in requests from 2021 to 2023.** For every one million consumer identities, manually processing DSRs costs about $800K. Consumers are taking more control over their personal data by, among other things, accessing it, deleting it, or requesting businesses not to sell or share it.

With this report, we hope to provide insights into how many DSRs businesses are getting (spoiler: it's a lot more than last year), reveal which types of DSRs are most common, uncover the costs of dealing with privacy requests, and reveal one important area in which businesses risk violating the law. Legal and cultural trends mean every company should be taking privacy seriously, and this report can help you navigate this fast-developing landscape.

Highlights

An overview of key privacy trends to watch



246%

Increase in total DSR volume per 1M identities from 2021 to 2023

38%

YoY cost increase for DSR management from 2022

40%

Of DSRs are deletion requests, far outpacing access requests

859

Average number of DSRs per 1M identities in 2023

75%

Of organizations fire 3 or more cookie trackers despite not consenting to tracking; discovered after auditing 5000 websites

$881K

Per year cost of processing Deletion & Access requests per 1M identities in 2023

80%

DSRs come from the global community—from regions not protected by privacy laws
Requests come from every state and every country — not just those with privacy laws protecting its citizens. 34% of requests in the U.S. are made by people in states that didn't have privacy laws in effect.

Methodology

DataGrail analyzed the Data Subject Requests (DSRs) it helped process on behalf of customers from January 1 - December 31, 2023. The customer set has more than 700 million records, where a record is defined as a single, individual record associated with a unique identifier within a customer's database. To determine the cost of processing requests, we used Gartner's manual processing estimate of $1,524 per DSR. This statistic comes from Gartner's 2023 report, Market Guide for Subject Rights Request Automation.

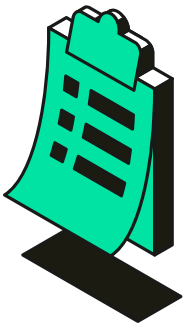
The dataset includes information from companies of all sizes, from startups to publicly traded household names. To normalize the data across various company sizes, we calculated DSRs per one million identities. For example, the data shows the average business in 2023 received 578 Access & Deletion requests per 1M identities per year. Using 578 as a benchmark, an organization with 3M identities can expect 1,734 Access and Deletion requests per year.

If we include California-specific Do Not Sell requests, the numbers rise to 859 requests per 1M identities per year. Following the example above, if the organization holds 3M identities, the industry benchmark would be 2,577 DSRs per year.

We found the number of DSRs a business receives varies greatly due to multiple factors, including whether the company is B2B or B2C, how often company privacy policies change, and several other factors. To account for variability, we used a 10% trim mean calculation to determine our benchmarks. A 10% trim mean calculation excludes the 10% largest and 10% smallest values and takes the mean of the remaining 80%.

The dataset includes DSRs submitted under CCPA and GDPR, along with DSRs received in the US and globally that don't fall under those regulatory umbrellas. As a United States-based company, with primarily US-based customers, our dataset may skew toward DSRs from the US.

To calculate the percentage of organizations not complying with the GPC standard, we audited more that 5,000 websites.



What's a DSR?

A Data Subject Request (DSR) allows an individual to request that an organization takes certain action over the individual's personal data. There are several types of DSRs, but this report focuses on requests to access personal data, requests to delete personal data, and requests that a company does not sell or share personal data ("Do Not Sell" requests).

What do we mean by identity?

Mentions of an "identity" refer to information associated with a unique **record** of a single customer or employee at a company. A single "identity" accounts for one customer's personal data within multiple systems across an organization.

The 2024 State of Data Privacy: US & Europe

Since our 2023 report, privacy has continued to become one of the most important focuses for businesses across the world. This year has seen even more privacy legislation, data-related legal activity, and awareness of privacy rights among consumers.

United States

- State privacy laws: By the end of 2023, 12 states passed "comprehensive" privacy laws. So far in 2024, New Jersey, New Hampshire, and Kentucky have joined the privacy club, and Maryland and Nebraska should be enacting such laws soon.
- California privacy enforcement: In February, Attorney General Rob Bonta settled a California Consumer Privacy Act (CCPA) complaint accusing DoorDash of unlawfully selling personal information. That same month, California Privacy Protection Agency (CPPA) also gained its enforcement powers, so expect more California action soon.
- Federal privacy enforcement: Following an extremely busy 2023, the Federal Trade Commission (FTC) continues to push hard against unlawful tracking, issuing an average of one privacy enforcement order per month throughout the first quarter of 2024.
- Federal privacy bill: In early April, the US House of Representatives unexpectedly revealed a draft federal privacy law with strict rules on data minimization, transparency, and data sharing. Whether or not the American Privacy Rights Act (APRA) passes, the bill shows how privacy is becoming an increasingly crucial issue in the US.

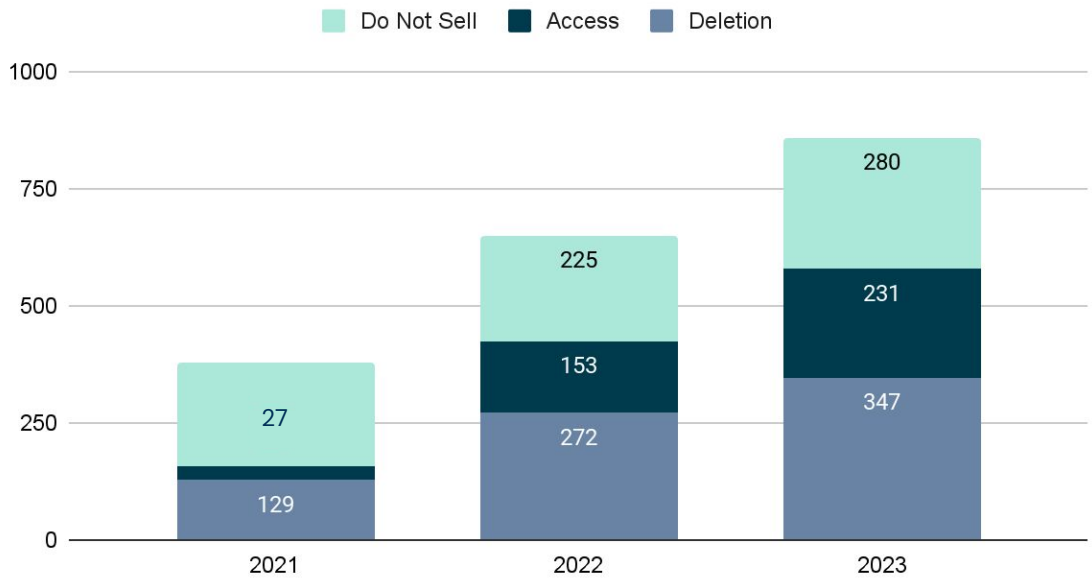
European Union & United Kingdom

- EU court rulings: After countless GDPR judgments throughout 2023, the Court of Justice of the European Union (CJEU) began 2024 with further important data protection rulings, including on:
    - Digital advertising (Case C-604/22 involving the Interactive Advertising Bureau, IAB)
    - The wide scope of the GDPR (Case C-740/22, "Endemol Shine")
    - The broad definition of "personal data" (Case C-479/22 P, "OC")
- GDPR fines: Penalties under the GDPR continue to bite, with significant regulatory decisions issued:
    - Meta: $1.3 billion (data transfers)
    - TikTok: $415 million (privacy by design)
    - Criteo: $42 million (failure to obtain consent)
- UK reforms advance: UK lawmakers are debating plans to reform data protection and privacy law, which could complicate compliance for UK businesses.
- AI Act finalized: The EU's institutions agreed landmark rules regulating artificial intelligence, adding to a barrage of complex digital regulations passed in recent years.

Privacy Requests Increased 246% in Two Years

Businesses received nearly one-third more Data Subject Requests (DSRs) in 2023 compared to 2022. Requests of all types—access, delete, or sale opt-outs— increased.

DSRs per Million Users 2021-2023



On average, businesses received **859 DSRs per one million identities in 2023**

Why are the number of DSRs continuing to climb?

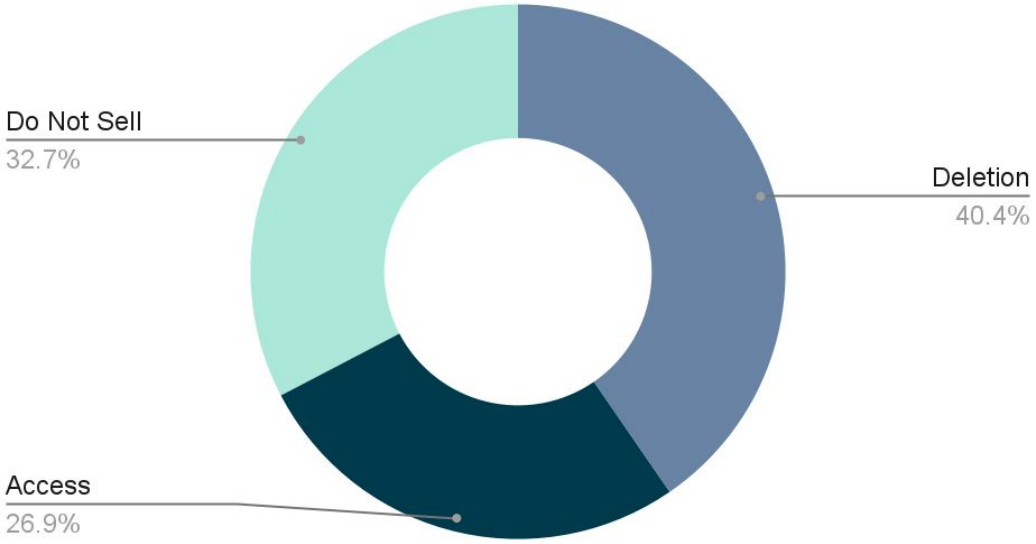
Across the US, five new state laws took effect last year that give consumers new rights over their personal data. Many similar laws passed in other states that will take effect over the next few years. This trend suggests a growing privacy awareness among consumers, partly due to these new laws passing, frequent privacy enforcement action from the FTC, and increased media attention on privacy.

Deletion Is the Most Common Type of Request

Privacy Requests to delete personal data exceed access and 'do not sell' requests for the third year running

Consumers continue to ask businesses to delete their personal data, making it the most common type of DSR, accounting for more than 40% of requests on average across businesses. While deletion requests remain most common, access requests have increased most significantly, booming by around 50% since the previous year.

2023 Breakdown By DSR Type



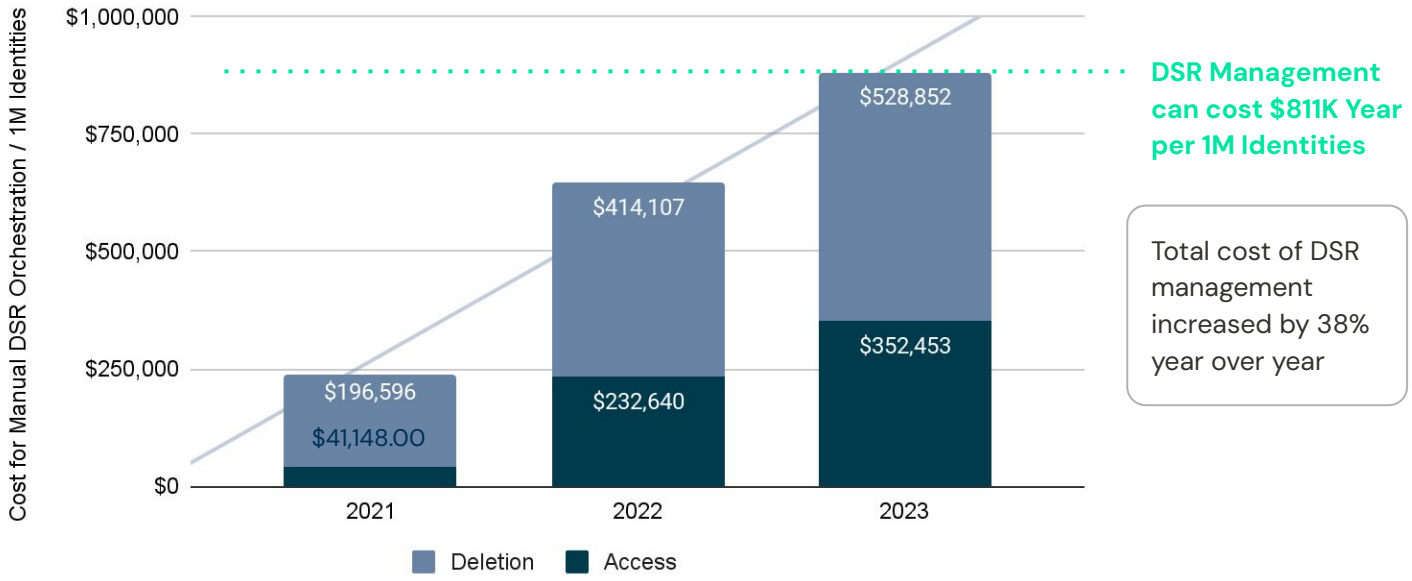
We focus on three main types of DSR: Requests to access personal data, delete personal data, and requests opt out of the sale and sharing of personal data ("Do Not Sell" requests)—as these are the most popular requests. Every comprehensive privacy law in the US includes the right to delete personal data under certain conditions. We also saw requests to correct inaccurate personal data and requests under the "right to data portability," but not enough to establish any trends.

The Cost of Data Privacy Continues to Rise

Manual processing of DSRs can cost $1M per year, or more.

Businesses manually processing DSRs face high costs as the number of requests increases. According to Gartner, a single access or deletion request costs around $1,524 to complete. Our data suggests that a company handling one million identities receives 578 access and deletion requests in an average year. Based on Gartner's estimate, manually processing DSRs could cost around $811,305 per every million identities.

2023 Cost of DSR Management Over Time



As businesses collect more data and privacy requests increase, handling DSRs becomes difficult and expensive. Companies can struggle to locate data stored in different formats across different systems, all while ensuring they do not violate the rights of other consumers. Businesses face a huge rise in costs unless they automate parts of the DSR process. These costs estimates ***do not include*** requests relating to other rights, such as requests to opt out of the sale and sharing of personal data.

Opting-Out Is Becoming Mainstream

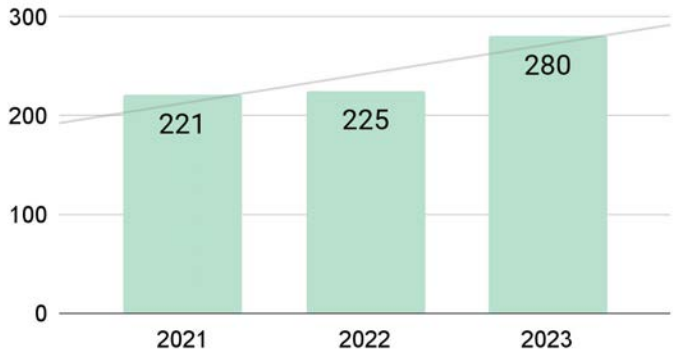
Consumers are automating "Do Not Sell" requests; around 75% of businesses are not honoring them.

Universal Opt Out Mechanisms (UOOMs) enable consumers to automatically tell businesses not to sell or share their personal data for advertising. Until recently, honoring UOOM signals has been optional in the US. This is changing. California already requires CCPA-covered businesses to detect and honor requests made via Global Privacy Control (GPC) and other common UOOMs. A similar rule takes effect in Colorado from July 2024, and many other states will follow over the next few years. DataGrail analyzed over 5,000 websites to check how businesses respond to GPC signals. We found that 75% of websites did not honor "Do Not Sell" requests via GPC.

75%

Our research suggests that 75% of websites do not comply with GPC requests. This means most businesses are not honorings people's do-not-sell privacy requests. Some could be violating current law or be unprepared for upcoming legal changes.

2023 Volume of Do-Not-Sell Requests per 1M Identities



"GPC is a way users can universally express, to all sites, their preference not to be tracked on the web. It is a browser-level signal, maintained either by a browser or browser extension, that a user or privacy-focused technology can set. The easiest way to think of GPC is as a robot that selects the Do Not Sell preference on a site on behalf of a user."

UOOMs automate requests under California's "Do Not Sell Or Share My Personal Information" rules and similar laws. Such requests are rising and will likely increase significantly as new laws take effect.

Additional Resources:

What is GPC

Do-Not-Sell or Share Guide

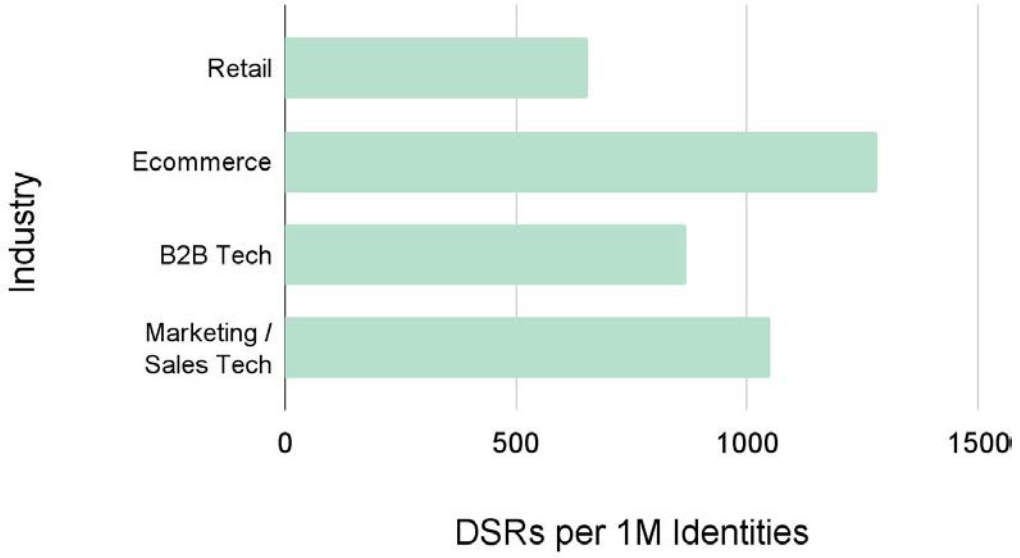
Navigating Privacy: Understanding Consent and Universal Opt-Out Methods

Privacy Requests Across Industries

Industries with a lot of online communications see the most requests

Our data shows how many DSRs consumers make to businesses across different industries. Ecommerce—or brands that have a direct to consumer (D2C) online relationship —typically receive the most DSRs. They receive nearly double the overall average number of DSRs. Marketing tech (MarTech) companies come second. Both these types of companies operate mainly online and can engage in intensive marketing campaigns, meaning they collect a lot of personal data.

2023 Volume of DSRs by Industry



Lots of personal data collected
+
Online communications

More DSRs

Industry descriptions:

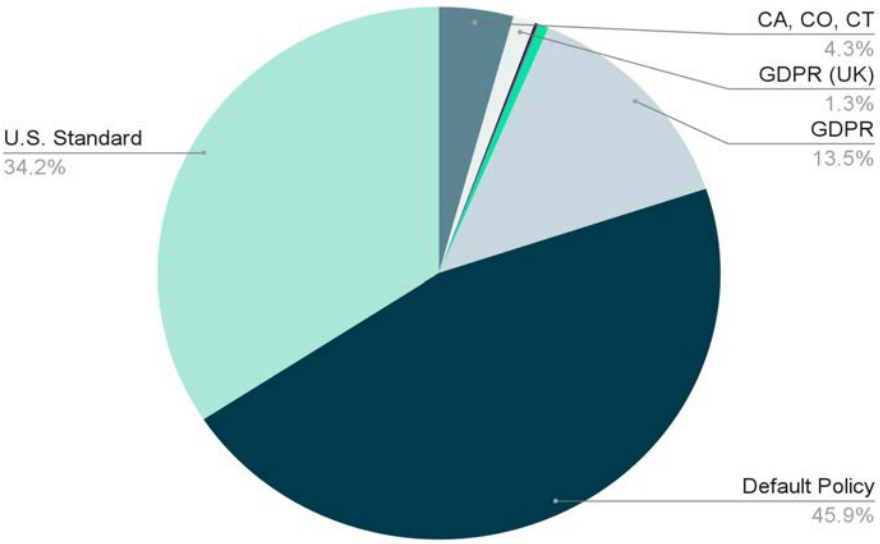
- **Retail:** We distinguished retail brands from ecommerce brands as those who typically sell in a "brick & mortar" setting, vs. online.
- **Ecommerce:** This includes brands whose primary go-to-market model is selling directly online to consumers. This also includes the growing "Wellness" market, MLM companies, consumer marketplaces, and or consumer health companies that may hold a lot of sensitive data.
- **B2B Technology:** This includes several enterprise technology companies. Companies that provide software ranging from database software and APIs to HR system software.
- **Marketing Tech:** Because marketing & sales technology includes email, CRM, surveys, and communications technology, we pulled Marketing Technology out into its own category. Typically this bucket represents businesses who market in a B2B setting.

Privacy Requests Can Come From Practically Anywhere

Consumers worldwide want control over their data even if they're not protected by privacy law; and businesses are honoring their requests.

46% of DSRs arrived from IP addresses located outside the US, Canada, China, Brazile the UK, or the EU (regions with privacy laws). As such, people making these requests might not be covered by strong privacy laws. Around 12.5% of US-based DSRs came from states with laws already on the books (CA, CO, & CT), yet 34% are coming from states without privacy protections, suggesting people from across the US are submitting requests regardless of their level of legal protection. Consumers want more control over their data even if they don't have legally-protected privacy rights.

DSRs By Policy in 2023



80%

of DSRs in 2023 came from jurisdictions that didn't have strong privacy laws, evidence that people around the world want more control over their personal data.

Note: As a United States-based company with a larger regional footprint in the US, our data skews toward privacy requests coming from the US and may not be an accurate reflection of total global requests. Many DataGrail customers apply GDPR-grade DSR processes across the board, which helps to ensure good customer relations and improves the efficiency of their privacy programs.

Data Privacy has arrived: It's time to adapt

Privacy laws are proliferating, awareness of rights is increasing, and the costs could spiral if organizations fail to act

When the EU passed the GDPR in 2016, many countries strengthened their data protection and privacy laws. It took a few years for this legal trend to hit the US, but now around one-third of states have passed comprehensive privacy laws.

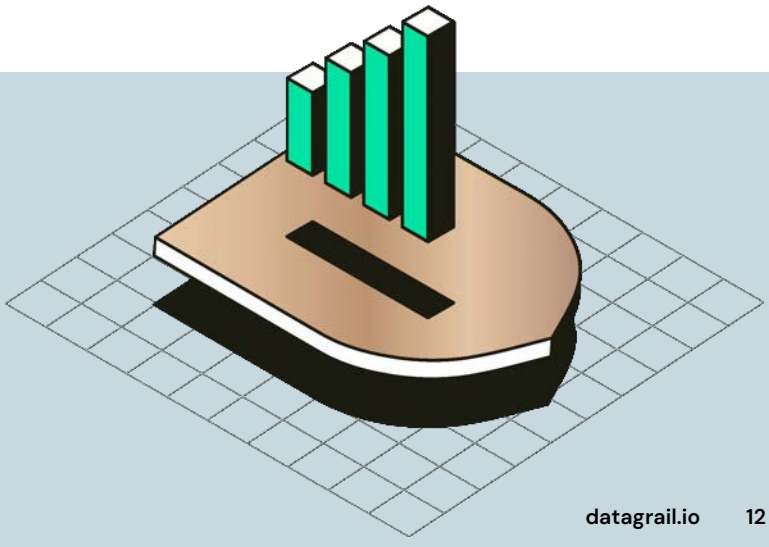
Before our next report in 2025, privacy laws will start to take effect in states like Delaware, Florida, Iowa, Montana, Oregon, and Texas. We'll continue to see enforcement of existing laws in the US, the EU, and elsewhere.

We also expect more consumers to use Universal Opt-Out Mechanisms (UOOMs) to automate "Do Not Sell" requests. In more and more states, honoring these requests will become mandatory—but our research suggests that most companies are not ready for this new landscape.

Against this backdrop, consumers are waking up to how their data is collected, used, and shared online. Privacy requests are booming year on year, with businesses facing on average 859 DSRs per one million identities in 2023 compared to 377 in 2021.

But as our data shows, DSRs can come from anywhere. Whether or not they're covered by a privacy law, consumers want more control over how businesses use their personal data. This "trend" isn't going away. For unprepared businesses, the costs could be eye-watering.

As legal demands and consumer expectations increase, take control of your privacy program with an automated platform that efficiently handles all types of privacy requests.



Learn More About DataGrail

DataGrail is the Privacy Control Center™ modern brands rely on to build customer trust and outsmart business risk.

Security, legal, and executive teams use DataGrail to automate privacy workflows and support compliance with regulations like GDPR, CCPA, and CPRA. With 2,000+ pre-built connections for popular apps and infrastructure, DataGrail offers continuous system detection, responsible data discovery, guided privacy assessments, and automated data subject request (DSR) fulfillment to power the world's most trusted businesses.

DataGrail services millions of consumers through companies like Amazon, Salesforce, Overstock, Instacart, and New Balance, and is a G2 leader. DataGrail is backed by leading VCs and strategic investors, including Third Point Ventures, Felicis Ventures, Next47, Cloud Apps Capital Partners, Operator Collective, HubSpot, Okta Ventures, and American Express Ventures.

Visit www.datagrail.io or follow DataGrail on LinkedIn and Twitter to learn more.

How to Get Started

Learn how DataGrail supports Do Not Sell or Share with GPC opt-out signals through a no-code, bannerless solution. Download the Guide.

Sign up for our Grail Mail newsletter and explore our library of on-demand resources to stay on top of data privacy and business risk.

Connect with other pros to discuss which privacy management models work for them. Join the Community.

Check out a demo of DataGrail to see how it can help you automate DSRs, find Shadow IT and AI, manage consent, or develop privacy risk assessments