Build value while honoring values: a guide to the ROI of data privacy

Maximize the value from your
data privacy platform

Ketch

Introduction

For many businesses, data privacy is still a major expense. Manually implementing privacy programs, and responding reactively to each new regulation, requires a team of lawyers and developers, considerable investments in IT infrastructure, and more. Last year, privacy spending soared 13%, to an average of $2.7MM a year.[1] With businesses collecting, processing, and storing more data than ever before, and new privacy regulations being introduced in jurisdictions all over the world, businesses urgently need new mindsets and methods for data privacy.

Which raises an important question: how can you be sure that you're making the right investments, and allocating your privacy budget in ways that generate real returns? According to Cisco, 94% of companies report privacy metrics to their board of directors, but only 15% report

the ROI of their privacy investments.[2] That's because most businesses still view privacy investments through the lens of risk reduction: a way to achieve regulatory compliance, rather than an opportunity to drive quantifiable positive value for their organizations.

At Ketch, we believe there's a better way. Regulatory compliance will always be an important motivator, but business and citizens have a right to expect more. Your privacy program should also be an engine of tangible revenue growth, brand value, and innovation.

As the saying goes, you can't manage what you don't measure, and in today's business environment data privacy is too important and too expensive to be left to guesswork. To optimize your privacy programs, you need to track their ROI—and that starts with understanding how privacy can create real, scalable value for your business.

To achieve that, it's important to look beyond regulatory compliance. Privacy used to be seen chiefly as a legal issue, but increasingly, companies are seeing IT, data, security and marketing teams take ownership and influence over privacy operations and privacy spending. Coordinating and optimizing these investments requires a clear, top-down commitment to privacy as a way to drive value for your business.

At Ketch, we believe privacy technology generates ROI in three key ways

1

By collapsing compliance costs

With streamlined and scalable processes.

2

By maximizing data utilization

Supporting responsible practices that respect people's data dignity.

3

By mitigating risk

Across multiple axes—such as regulatory, brand, and security risk.

In this briefing, you'll learn how to calculate and capture the potential value these three areas can generate for your business. You should demand real ROI from your privacy tech.

It's time to start measuring, managing, and maximizing the value of your data privacy investments.

1 /
Collapse compliance costs
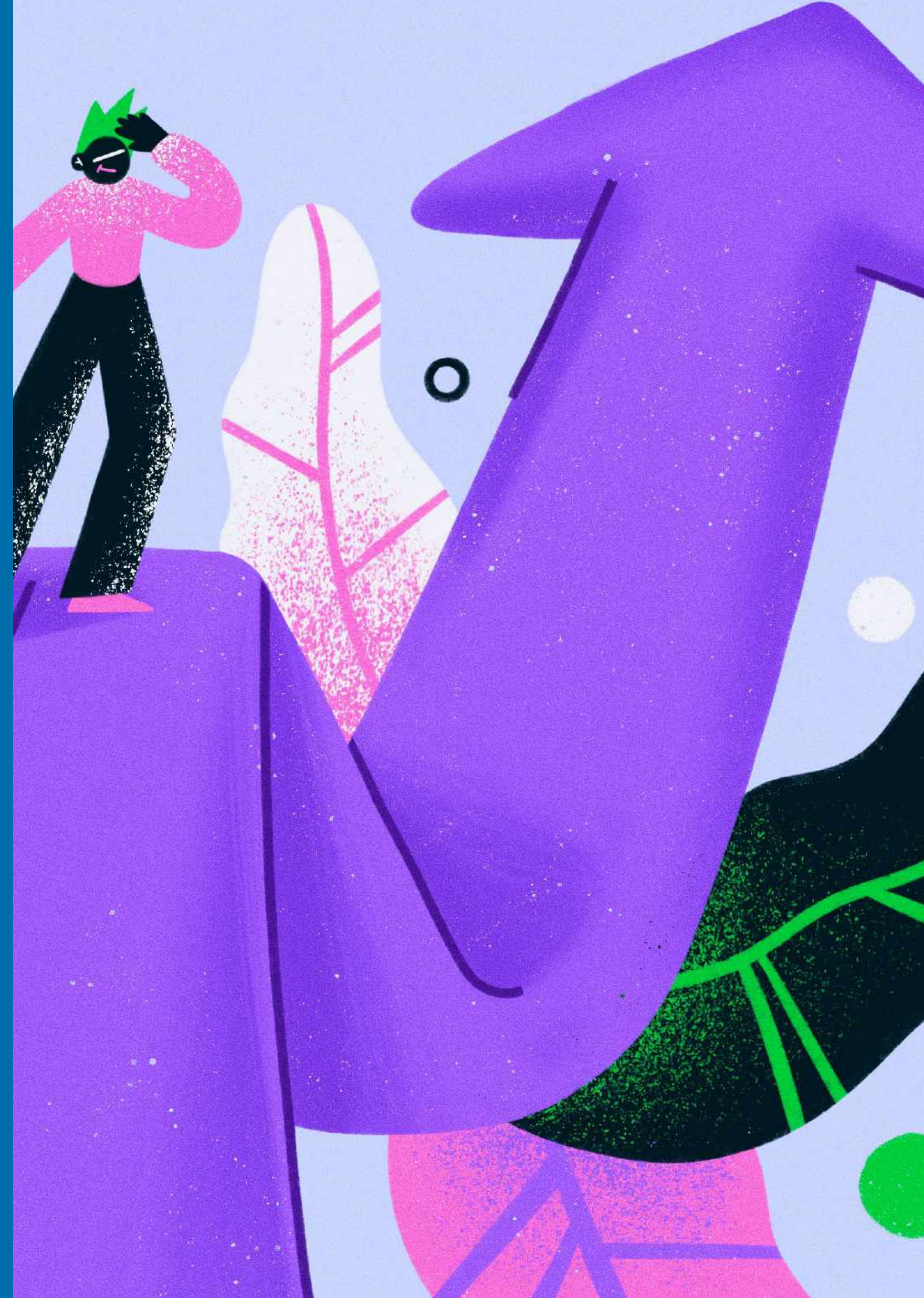
You need a flexible solution that can rapidly adapt to *new* regulatory requirements, and efficiently manage privacy across *multiple* jurisdictions.

That's crucial because we're close to a world with ubiquitous privacy legislation.

By year-end 2023

75%

of the world's population will have its personal data covered under modern privacy regulations*

3X

increase over current levels—and businesses will be forced to juggle the requirements of dozens of privacy laws and regulations, each with unique demands.

As a result, businesses will have to dramatically scale up their legal, data, and IT capabilities in order to remain compliant with a growing body of global regulations.

Privacy costs will skyrocket—unless businesses radically simplify, streamline, and automate their compliance efforts in the following ways ↓

Adopt a responsive compliance strategy

Complying with the European Union's General Data Protection Regulation (GDPR) was time-consuming and costly: three-quarters of companies reported costs in excess of $100,000, and 20% spent over $1MM on compliance. In a world of proliferating privacy regulations, businesses can't afford to pay $1MM, or even $100,000, to recalibrate and realign their data infrastructure to each new regulation that impacts their business.

That's where **responsive compliance** comes in. Where conventional compliance tools simply work their way down a checklist of requirements for each regulation, the programmatic approach views each new regulation as assembling its various requirements from a common stock of underlying **privacy primitives**. In much the same way as many recipes can be made from a single collection of ingredients, programmatic privacy gives you the tools to manage compliance with any possible regulatory framework using a single backend privacy toolkit.

For instance, every privacy regulation assigns certain rights to data subjects; requires an understanding of the purpose of processing data; and of the legal basis for collecting and utilizing that data. Responsive platforms incorporate privacy primitives like these for a repeatable, scalable solution.

36%
reduction in compliance costs for each new regulation

By mobilizing these privacy primitives, a programmatic solution can then seamlessly map them back onto the specific requirements of any given regulatory framework—without requiring you to start from scratch, re-catalog your data holdings, or rethink your data and IT infrastructure.

The bottom line: programmatic privacy unlocks massive economies of scale. Businesses can expect at least a 36% reduction in the cost of complying with any new privacy regulation.

Use dynamic data discovery for maximum efficiency

Programmatic privacy delivers full visibility into your data, using dynamic real-time data discovery to identify and track potentially sensitive information as it flows through your organization and your broader ecosystem. That enables robust and scalable compliance, with no need for laborious manual data surveys each time the regulatory landscape changes, reducing compliance-related data monitoring costs by as much as 70%.

Data discovery also delivers incredible efficiencies across your organization.

First, automated data discovery **makes risk assessments a breeze**. If your team wants to introduce a new technology or process, you can execute a Data Protection Impact Assessment (DPIA) quickly and efficiently, with complete confidence that you've

identified any and all sensitive data holdings that could be impacted by the change in direction. The result: a more agile organization, with no friction and no potential for unpleasant surprises.

Secondly, data discovery **enables your team to respond effortlessly to data subject requests**. Typical legacy systems still require up to 5 hours of work to identify affected data and enforce a single DSR, costing companies an average of $1,500 per request. With DSR volumes growing 50-100% per year, those costs soon add up—unless you implement a programmatic solution capable of tracking data and seamlessly executing incoming requests.

Finally, data discovery enables you to prune stale or unused data, reducing data bloat by up to 30%, with a corresponding reduction in risk.

70%

reduction in data mapping costs over manual, survey based solutions

Leverage APIs that enforce privacy choices across systems

Your data flows through an ecosystem of third-party vendor and partner systems, creating complexity. Businesses struggle to ensure that data subject requests (DSRs) and people's privacy choices are properly enforced. Perhaps your business shares user data with Facebook: now, when a user chooses to revoke consent or have their data deleted, you need to ensure that their choice is reflected not just in your own datasets, but also wherever you're shared that data.

Trying to solve that problem on your own is a tall order. In fact, **only 15% of businesses currently have visibility into how data is used by downstream vendors**.[3] But you can't wash your hands of the problem, either: your customer has made a decision, and they expect you to ensure that decision is properly enforced across your entire data ecosystem.

[3] Ponemon Institute (2018) Data Risk in the Third-Party Ecosystem. https://www.ponemon.org/userfiles/filemanager/nvqfztft3qtufvi5gl60/

The only practical way to meet that goal is by **building APIs that connect directly with your service providers**, so that when your user makes a decision, you automatically let Facebook—and any other affected providers—know what's needed.

The problem is that building those connections and maintaining them on a partner-by-partner basis is cumbersome and inefficient for most businesses. Even if you can convince Facebook to work with you on an API, you're looking at a significant investment. **We conservatively estimate the cost of creating a third-party API at $50,000**, plus hundreds of developer-hours to orchestrate privacy choices to your own internal databases. A company with even a small number of service-provider connections could easily see their API and developer costs balloon to hundreds of thousands of dollars per year.

That's where the right programmatic privacy vendor adds value. Because they represent thousands of businesses, they can work with providers to build and maintain effective APIs at scale, ensuring users' privacy decisions are reflected across the entire ecosystem.

That frees your dev team to focus on delivering real value, and frees you to grow your ecosystem without worrying about the spiraling cost of privacy compliance.

We conservatively estimate the cost of creating a DIY third-party API at $50,000, plus hundreds of developer-hours to orchestrate privacy choices throughout your own internal databases.

$50,000

Saved in connectivity costs per service provider used

400 hours

of dev time for orchestration into internal data systems

2 /

Maximize data utilization

Data is a powerful resource for any business—but privacy regulations can be seen as inherently limiting companies' ability to gather, store, process, and use their customers' data. **That's wrong.** Data privacy solutions built with data control as the foundation, can foster trust and transparency in ways that can significantly boost the overall availability and utility of data across your business.

By enabling businesses to earn, amplify, and capitalize on trust, a modern data–privacy solution creates value by giving your team access to more of the data they need to drive innovation and growth.

Let's take a closer look ↓

Maximize data availability with tailored, responsive approaches

In the face of proliferating privacy regulations, many organizations resort to a "GDPR everywhere" strategy: essentially, applying the requirements of the strictest regulatory regime to your entire dataset, even in areas outside of that regulator's jurisdiction. That leads to users being spammed with consent requests, diminishing the user experience and leading many users to reflexively opt out of allowing their data to be used.

A programmatic approach gives you a scalpel instead of a sledgehammer, and tailor your consent and opt-in processes to the specific needs of your audience. With a more personalized and localized user experience, you can ensure that you're requesting consent where you need to, and give your users control of their data without requiring

them to jump through unnecessary hoops. With reduced consent fatigue and full transparency into privacy processes, this approach can boost total data availability by more than 40%.

The result: your business gets the data it needs to make smarter decisions and create more value for customers.

40%

Increase in data availability

Earn customer loyalty with trust, transparency and control

More than 7 out of 10 companies say that increased customer loyalty and trust is a key benefit from their data-privacy investments. Loyalty and trust aren't just abstractions—they directly impact your organization's bottom line.

Consumers **point to** ↗ data security, control over data sharing, and trust as the key factors determining whether they'll share their data. By giving consumers more confidence and control over their data, organizations can ensure that customers feel safe enough to allow the use of their data.

Better yet, consumers who trust your brand and feel secure using your website and online services are more likely to make purchases—and customers who feel their data and their privacy choices have been treated with respect are more likely to become repeat customers.

When weighing the ROI of your privacy investments, don't forget to factor in your customer acquisition and retention costs, and to weigh the value of increased revenues for your business.

Prepare for a privacy–embedded future

As modern privacy regulations grow increasingly ubiquitous, and consumers grow ever more aware of and attuned to the value of their privacy rights, **we will rapidly reach a point where all data will need to be privacy-safe in order to be useful**.

We're already seeing companies struggle to make use of their existing data due to privacy bottlenecks. Consider, for instance, a data science team that wants to access a particular dataset to understand a new product, but isn't sure whether they're allowed to use the data for that purpose. At best, the pace of innovation will slow while the team figures things out. At worst, the product could get shelved, or data could be used improperly.

Programmatic privacy solutions that control how data is used, give your teams the ability to use data with confidence to make smarter decisions, unlock new opportunities, and drive growth. According to Cisco, 68% of businesses see agility and innovation as key benefits from their privacy investments—and with programmatic solutions, it's possible to maximize the value that creates for your business.

As the data revolution continues, and technologies such as responsible AI grow commonplace, **organizations that can't guarantee the privacy of the data they collect and process will find themselves sidelined**. To compete, collaborate, and innovate in the coming world of privacy-safe data, businesses need to put robust programmatic privacy solutions in place today.

68%

of leaders see privacy tools as enabling agility and innovation

3 /
A new approach
to mitigating risk
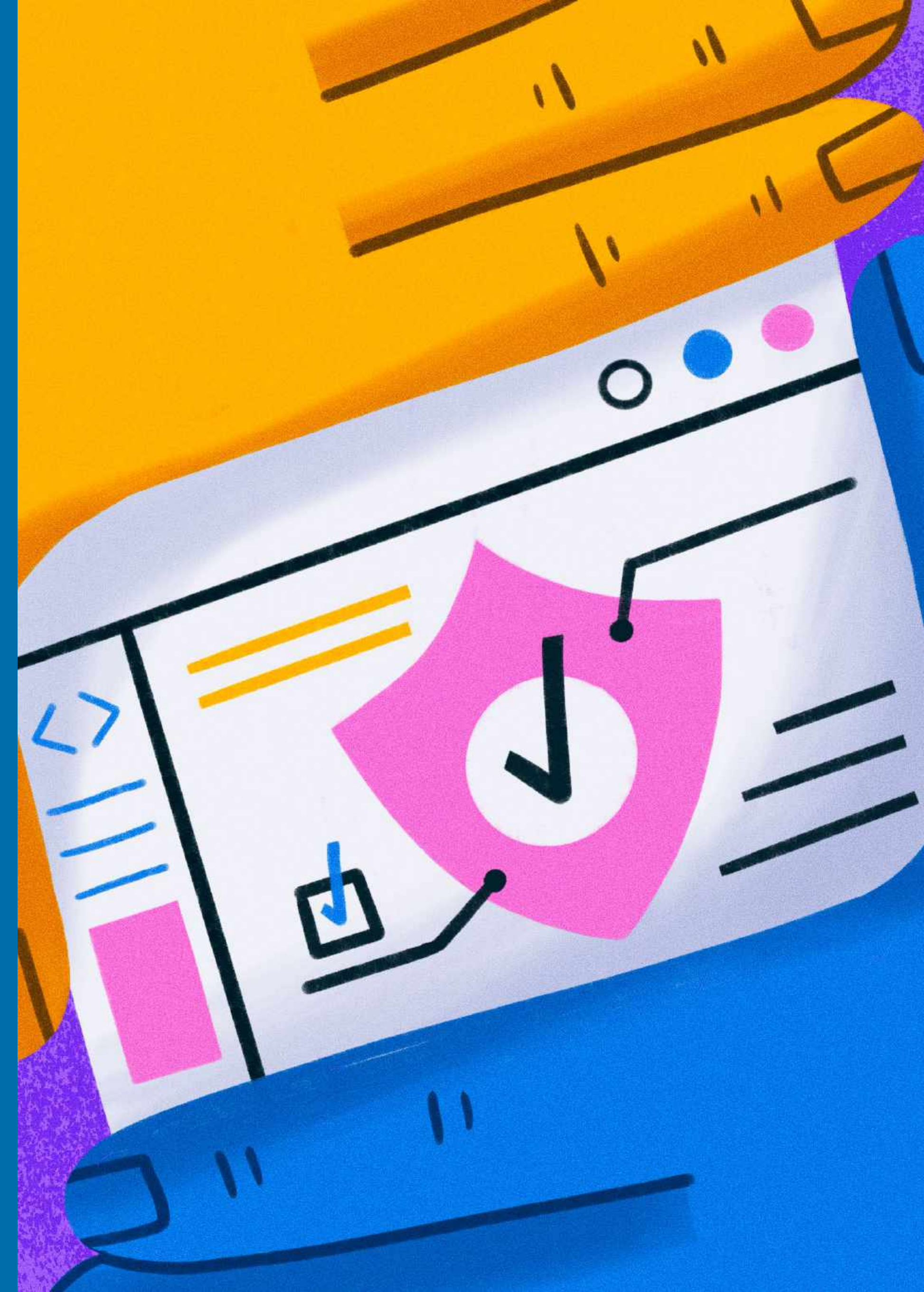
Using data across your business brings benefits, but also risks. When calculating the ROI of your data–privacy stack, it's important to weigh the degree to which your business could be impacted if you fail to manage privacy effectively.

There are three key factors to consider ↓

Reduce your regulatory risk

We're seeing a trend toward tougher data privacy enforcement. In 2021, businesses were hit with more than $1.2B in fines for breaches of their GDPR obligations— a sevenfold increase on the previous year.[4] Other jurisdictions are also imposing significant fines: the CCPA's $2,500-per-user fine can quickly add up to an eye-watering sum for businesses handling large volumes of data, for instance.

With more and more privacy regulators around the world now flexing their muscles, businesses could find themselves on the hook for substantial financial penalties and reputational damage if their data privacy solutions aren't sufficiently robust. Some organizations could even find themselves fined more than once for the same data breach, if the incident falls under the purview of multiple regulatory regimes— and could then potentially find themselves on the hook for additional civil damages relating to the same incident.[5]

Regulators are building powerful new "privacy police"↗ to target violators and working closely with antitrust bodies and other agencies to hold businesses accountable. Even a regulatory wrist-slap can damage reputation and increase the cost of customer acquisition and retention for months or years to come.

$2,500

per–user fine for CCPA violation

80%+

risk reduction with programmatic privacy solutions

[4] https://www.complianceweek.com/regulatory-enforcement/report-gdpr-fines-surpass-1b-in-2021-breach-notifications-also-rise/31259.article
[5] https://www.itgovernance.co.uk/blog/nis-directive-and-gdpr-double-jeopardy-can-you-be-fined-twice-for-the-same-breach

Protect your data

Data breaches are expensive to remediate: according to IBM, each data breach costs the affected organization an average of **$3.9MM**, and takes 280 days to fully contain.[6] In many parts of the world, the costs are even higher: in the United States, for instance, data breaches cost an average of **$8.6MM** in lost business and related expenses.

An effective data-privacy solution reduces your exposure to such costs by giving you full visibility into your data holdings, enabling you to redact or delete stale data, and to ensure that sensitive information is properly managed. As noted previously, by using automated, dynamic data discovery, modern privacy tools can reduce your organization's data surface area by **30%**—with a corresponding reduction in potential vulnerabilities.

Modern platforms like Ketch offer enterprise data fortification—data level access control and security.

Decide data access policy based on permitted uses of data, and enforce data level security policies such as masking, anonymization and tokenization.

$150

Per-record cost of a data breach

6 IBM Security Cost of a Data Breach Report 2020 (5)
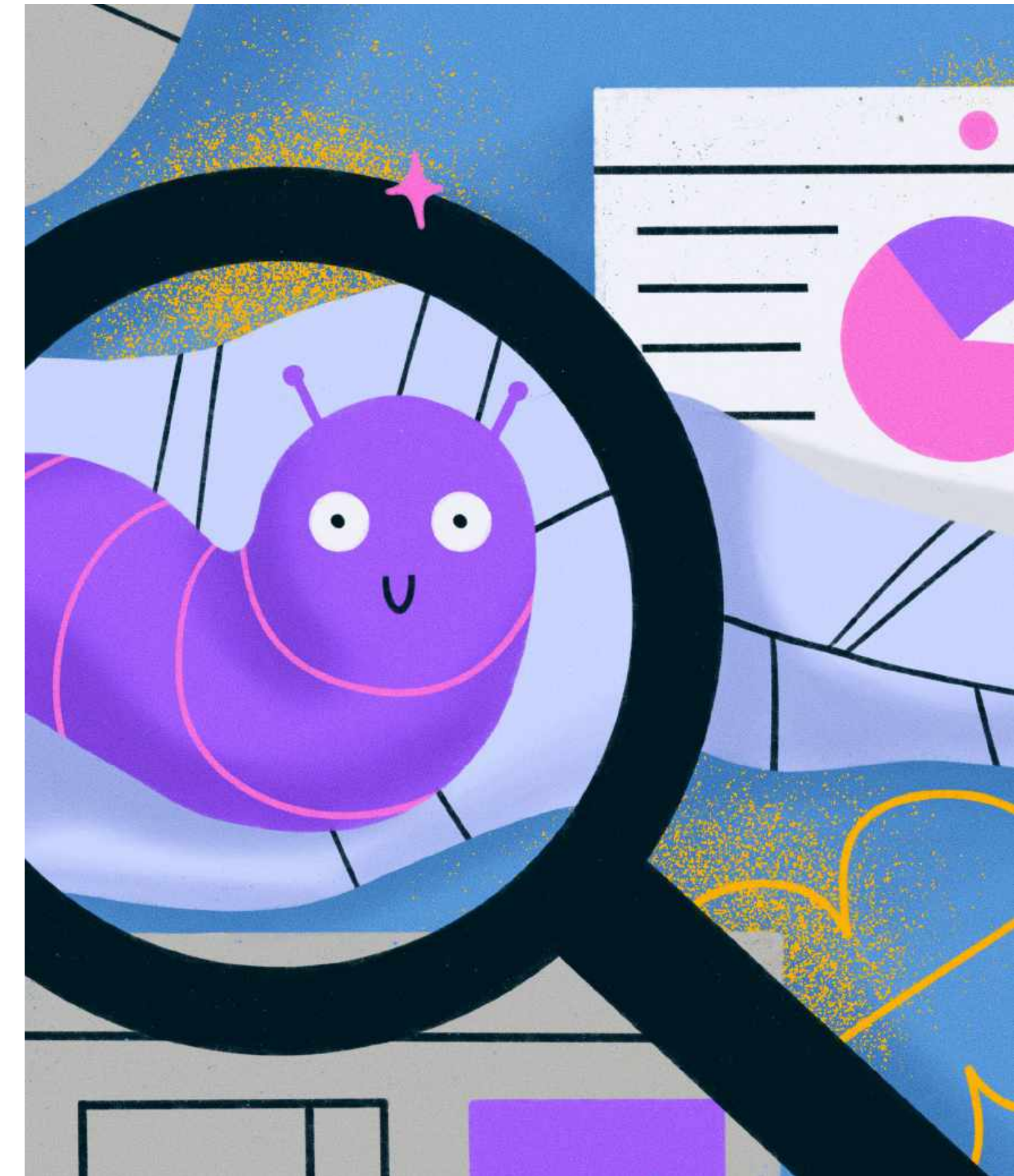
Safeguard your brand—and your revenues

Privacy is fundamental to consumer perceptions of your brand, and a regulatory slapdown or a high-profile data breach can make it harder to both acquire and retain customers. In fact, **lost business is the single biggest cost to businesses of data breaches**, according to IBM, accounting for about 40% of all breach-related losses.

How much is avoiding those losses worth to your business? When trying to decide, bear in mind that 90% of companies say their customers wouldn't buy from them if they failed to protect their data,[7] and one in five consumers say they've decided not to buy from a brand because of its data practices.[8]

That means privacy issues can take a big bite out of your bottom line. Consider how much your company generates from its most loyal returning customers—and then ask what it would cost you if just **1%** of those customers decided to make their purchases elsewhere.

Even better, imagine the competitive advantage that responsible data practices give you, and the increased loyalty and revenue that comes from trust and transparency with your customers.

[7] Cisco 2022 Data Privacy Benchmark Study (5).
[8] Conference Board / Nielsen / Forrester.

Case study /
How Ketch creates value

How Ketch creates value

Ketch is the leading data control platform for programmatic privacy, data governance, and security.

Through a coordinated set of APIs, applications and infrastructure, Ketch helps businesses build trust with people, and harness data to fuel core operations and top line growth.

Perfect, granular control of data is the foundation for any privacy and governance program.

Deploy Once, Secure and Comply Everywhere.

At Ketch, we believe there's no excuse for privacy–tech failing to deliver meaningful ROI.

We're confident we can unlock

10–12x

value for our customers when they invest in our platform.

Privacy ROI in the real world

Here is a "by the numbers" look at privacy ROI
for a major online retailer.

Reduced cost of compliance

They are preparing for **6 new regulations** in 2022/23.

Estimated costs to prepare for these regulations is around **$420,000 per regulation.**

Ketch reduces compliance costs by 36% for a **$1MM saving.**

Responsible data practices drive growth

The retailer's **17 million loyalty program members** place orders worth an average of $250 per year.

With a 1% estimated membership increase due to transparent and responsible data practices, **Ketch delivers a $42.5MM revenue opportunity.**

Automated DSR fulfillment

The **retailer receives 1,000+ data subject requests** per year, with manual fulfillment costs of $1,500 per request.

Ketch automated the entire DSR process to deliver **$1.5MM savings.**

No more "GDPR–Everywhere"

The retailer's websites receives **20 million unique visitors per month**, but its GDPR-everywhere privacy approach led to 30% excess opt-outs.

With Ketch's tailored approach, data availability was preserved with **a revenue impact of $500K**

Efficient consent orchestration

The retailer needed to enforce their consumers' privacy choices across **10 service providers.**

Building **privacy connectors** to those service providers would cost $500,000.

Ketch seamlessly automated the entire process: **a $500K saving.**

Ketch

Want to learn more?

Get in touch with Ketch for a customized ROI calculator, and to learn more about how programmatic privacy can drive value for your business.

Contact us →

23 Geary St.,
San Francisco, CA 94108

ketch.com