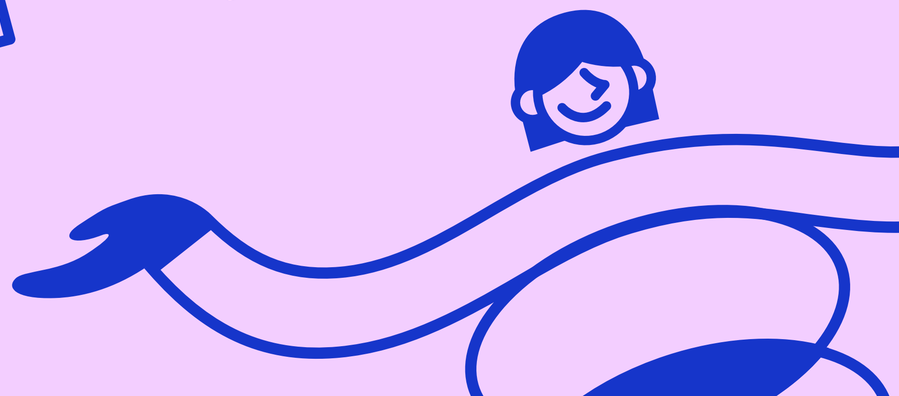
Are you using the right data privacy platform?

Whether you're shopping around or simply taking stock, here's what you need to know about the process of buying a new consent or data rights solution

Ketch



Introduction: the rise of consent management platforms

For modern enterprises, data is the new oil– and like oil, it requires careful handling in order to harness its power without causing a big, ugly, and expensive mess. With the regulatory landscape growing increasingly far-reaching and complex and consumer expectations around data privacy on the increase, enterprises simply can't afford to take chances when it comes to managing the data flowing through their operations.

To protect your customers and your business, it's vital to put a smart consent management solution in place to ensure you're using data in ways that the data owner, your customer, and your audience intended, with respect for both their security and the changing demands of local and regional regulatory bodies. But the privacy technology industry is constantly evolving, and the solution that suited your business a year ago may not be the right option for the challenges and opportunities you're now facing. How can you ensure you're using the optimal privacy platform for your current needs?

The key is to implement a simple but systematic review process to identify your priorities, assess whether they're being met by your existing provider, and explore what else is on the market. Think of it as going for an annual physical: dedicate a couple of days to this every year and you can ensure that your privacy infrastructure is healthy, up to date, and ready to withstand the challenges it will face over the next 12 months.

The key is to implement a simple but systematic review process to identify your priorities, assess whether they're being met by your existing provider, and explore what else is on the market.

In this guide, you'll learn how to monitor the health of your existing data privacy tools, how to assess the countless options that are now on the market, and how to figure out which solution is best for your needs.

First, know yourself

Finding the right data privacy solution begins with understanding the nature and scope of the problem you're trying to solve. Of course, the core challenge is to manage consent and data subject requests across your data ecosystem—but what does that mean in practice? How many people visit your website? Do you need a solution that works across apps and mobile devices, or just desktops? How do you collect and process consent signals and data subject requests, and which systems need to honor this information? And have your answers to any of these questions changed since you first implemented your existing privacy tools?

> ...you'll likely realize that what you need isn't simply a series of point solutions for a static constellation of regulatory requirements, but rather a dynamic system that allows you to adapt and change to the shifting regulatory landscape in which your business operates.

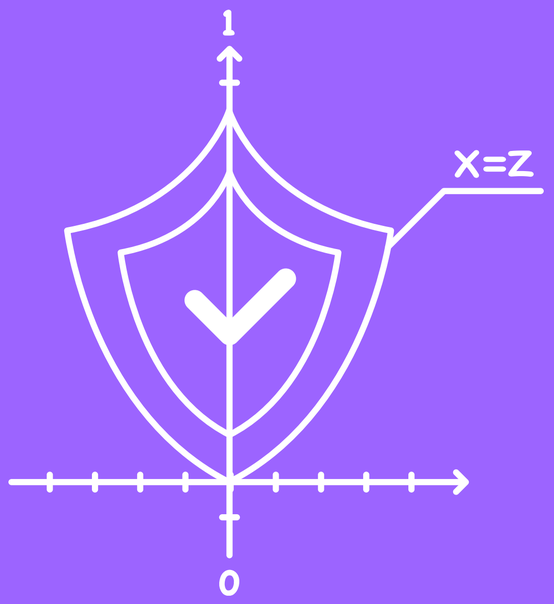
First, know yourself

Once you've taken the pulse of your existing privacy operations, it's time to look at the regulatory rulebook. You already know privacy is important, but what specific regulatory requirements are you trying to solve for?

Are you looking to ensure compliance with GDPR or CCPA? Are there other regulations that affect your business? What future regulatory efforts are on the horizon–do you need a system that can manage data across multiple jurisdictions, or flexibly adapt to new regulatory action? Given the rapid pace of regulatory change, you'll likely realize that what you need isn't simply a series of point solutions for a static constellation of regulatory requirements, but rather a dynamic system that allows you to adapt and change to the shifting regulatory landscape in which your business operates.

Finally, you need to understand the different stakeholders in your own buying process. Privacy is a team sport. Ask your IT team or your head of engineering what they want from a data privacy system and you'll likely get a very different answer than if you ask your CISO, your legal team, or your sales and marketing division. Any one of these stakeholders might take point on the procurement process for your data privacy system, but it's important to understand and account for the needs of all stakeholders as you look for the optimal solution for your business.

Critically, you'll need to ensure that different teams' priorities and objectives are balanced. This is especially important with regard to the tensions that can arise between Technology and Legal teams–the Technology team may hold the budget, and want solutions that can scale with the current tech stack and data systems, but Legal is looking to solve a policy and privacy operationalization challenge. Privacy is no longer solely the responsibility of a single department. In addition to Legal and Technology, Marketing could weigh in on customization available to ensure privacy experiences can reflect brand voice and optimize the user experience. You need a solution that gives every member of every team exactly what they need to do their job.



What’s on your mind?

Run through the checklist below to make sure you’ve covered all the key areas about your own business before you start shopping around for a content management solution.

Understand data use across your business

- [ ] What are the internal systems and partner systems that process your personal data?
- [ ] How do you currently collect consent signals and data subject requests, and propagate them across your data systems?
- [ ] How do you use data?
- [ ] Is your end-goal to create better analytics, to provide personalization, or some other purpose?
- [ ] Who else uses the data you collect, and how do they receive and process consent signals?
- [ ] How have your answers to these questions changed since you implemented your current system?
- [ ] What regulations currently govern your data use and privacy obligations?
- [ ] Have they changed recently?
- [ ] What new regulations are on the horizon that could impact your business?
- [ ] What new jurisdictions have you entered, or might you start to business in over the coming year?
- [ ] Have any of your regulatory interpretations or legal bases changed?
- [ ] How might they change in the future?

Understand who’s using your content-management solution

- [ ] What does your legal team need from your content management platform?
- [ ] What are the areas that are creating roadblocks for your IT and engineering teams?
- [ ] What does your CISO need to keep your organization and your data safe?
- [ ] Have your sales and marketing teams weighed in on the visitor experience and revenue impact?
- [ ] How do these different needs overlap, and are there conflicts you need new tools to resolve?

Understanding the privacy marketplace

Once you understand your specific needs and use cases, you're ready for a workable solution. Begin by taking stock of the tools you're currently using. Perhaps you're using a cheap but inflexible cookie-based consent system, or perhaps you've adopted a third-party solution with its own strengths and limitations. Make sure you understand the way your current system addresses the needs you've identified for your specific usecase, and pay close attention to any new pain-points that have emerged as your business has grown or your usecase has evolved.

Next, research the available alternatives. There are countless sources of information you can leverage as part of this research process, from reference sources to market reports, and from analysts' briefings to user review websites such as G2. Don't neglect the power of personal connections, either: whether by chatting at trade shows, quizzing your LinkedIn or Twitter followers, or simply phoning a friend, you'll often get the most important recommendations from people who understand your needs, and whom you already know and trust.

While you're scouting for new solutions, make sure you don't get fooled by complexity. Many vendors offer up endless laundry lists of features described using highly technical jargon–an approach that helps them justify higher prices, but that doesn't add real value for users. It's true that privacy can be a complex problem, but your solution to that problem should be elegant and simple, not a slew of technical features or optional add-ons that will require you to pay more in the future.

The best technology is transparent and easy to understand—so if you find yourself getting confused, you might be looking at the wrong product.

Segmenting the players

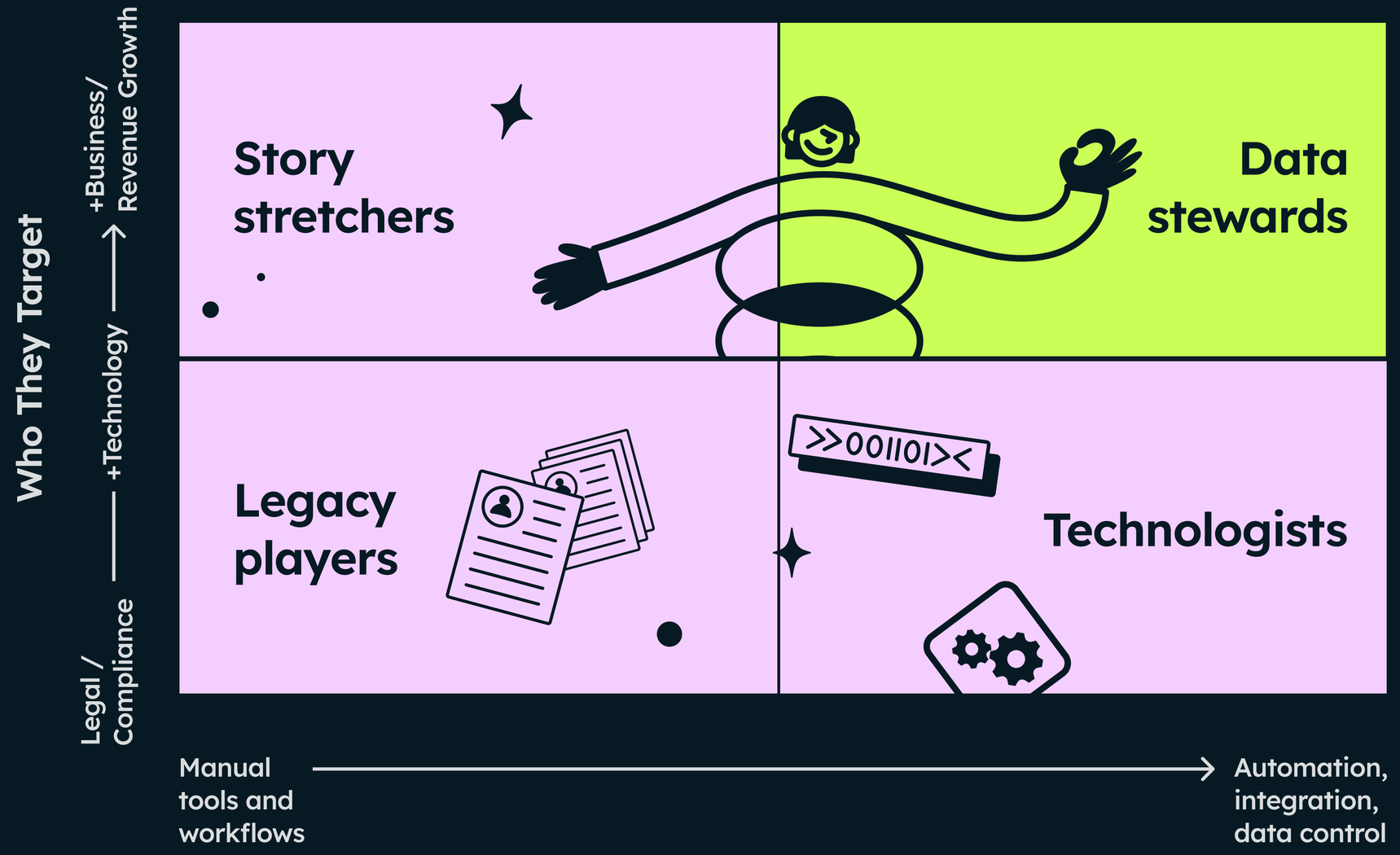
The data privacy software market has many companies making similar capability claims. Here's how we break it down:

Legacy players: First to market, often bloated through acquisition and tech debt. May not be purpose built for regulatory pace today. Selling to legal teams only.

Story stretchers: Similar to legacy, but modernizing their messaging to appeal to data/growth-oriented buyers. Check behind the curtain!

Technologists: These vendors are applying modern tech to legal challenges. A better option than legacy tools, but shortsighted in connecting privacy to business requirements.

Data stewards: The best of both worlds. Vendors creating purpose-built tooling for modern regulatory and privacy needs, with a keen eye towards how privacy should support broader business data goals.



5 must-haves for your privacy solution

Many privacy management platforms address only subsets of the challenges faced by modern enterprises. It's important to look for a more comprehensive solution that delivers all the critical functionality that you need. Let's take a look at five of the key capabilities that any consent and data rights platform should be able to deliver for your business.

The key, as always, is to know what you need, and methodically seek out products that deliver precisely that functionality. No matter how many bells and whistles it has, a consent management platform's core task is to ensure you and your partners only use data in legal ways that align with your user's expressed preferences. While that requires a powerful and well-designed tool, it's a fundamentally simple goal. If you aren't completely sure how your privacy software achieves that, the odds are that your solution is falling short. The bottom line: as with any transaction, you're paying real money and you deserve to get good value. Don't get boxed in by needless complexity, or let yourself be tied to a single approach. Remember: you're in the driving seat, and if the vendor you're working with can't provide the solutions you need, then there are plenty of other options to consider.

5 must-haves for your privacy solution

01

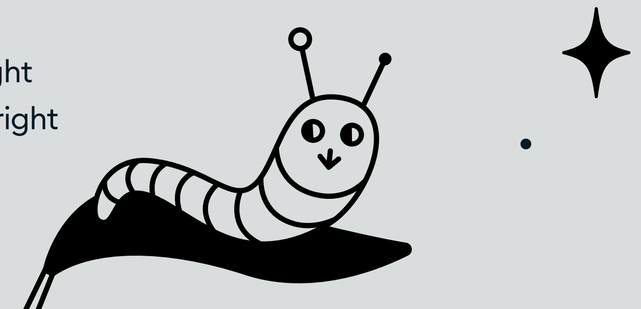
At its simplest, a data privacy solution needs to **manage the way data flows** through your business, and ensure that it's handled in ways that simultaneously respect user preferences, align with internal policies, and comply with external regulatory requirements. Achieving that requires a solution that can integrate seamlessly into your workflows and dataflows, ensuring that your team can leverage data to deliver functionality, while still adhering meticulously to your customers' expectations.

02

Achieving this requires **the ability to handle multiple regulatory regimes**. The modern regulatory landscape is a patchwork, and data often flows between jurisdictions. If you're selling to customers in the European Union, you'll face very different challenges and requirements than if you're selling to customers in California. You may also find your regulatory obligations change as your business model evolves, the rules get rewritten, or you move into new markets. You'll need a system that's flexible enough to adapt to your changing needs, granular enough to be localized depending on the markets you're selling into, and comprehensive enough to apply the right regulations in the right way and at the right time, every time.

03

Your solution doesn't just need to be robust and flexible–it also needs to **deliver streamlined, onbrand experiences** for your customers. Don't settle for boilerplate privacy notifications: demand tools that can be customized, and that let you make mindful decisions about the language you use, the way notices are styled, and how they're timed. Your marketing team will love the way your messages match your brand voice, and you'll find it far easier to build trust and create a transparent, hassle-free experience for your customers and audiences.

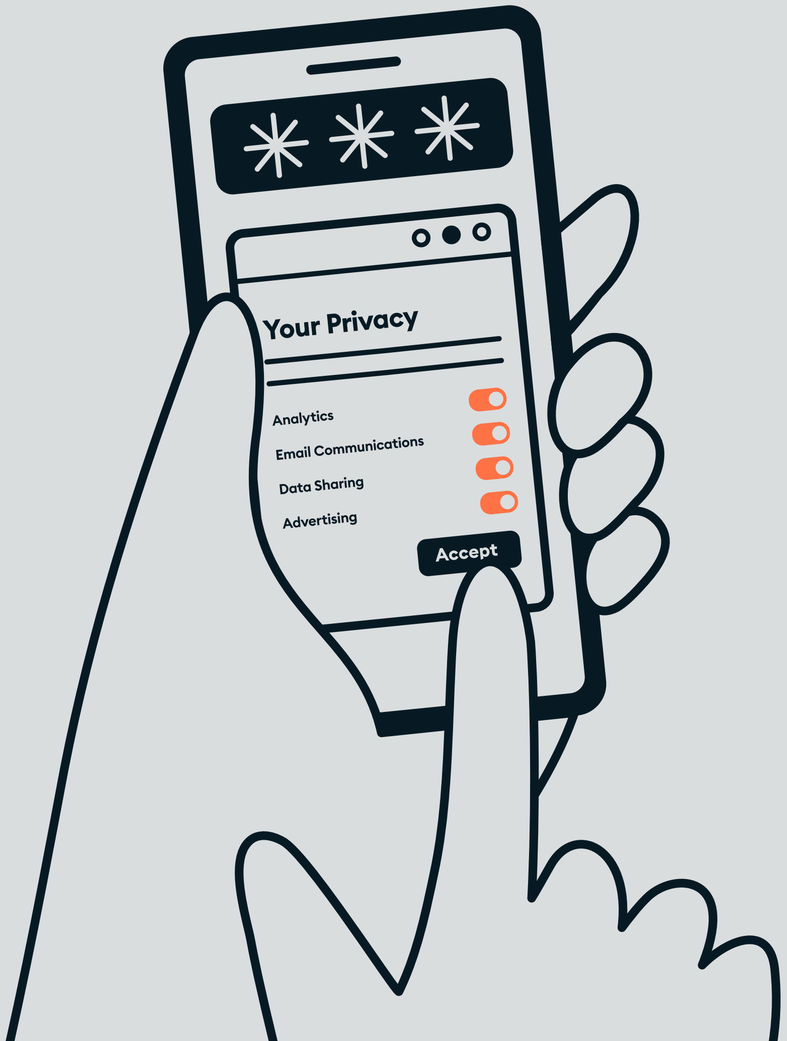


04

It's not just the regulators who make life complicated–it's also the way today's businesses operate across multiple channels, including websites and mobile apps, and connect with third-party partners to deliver services to their customers. You need a solution that can **orchestrate consent and data subject requests** across all those touchpoints, as seamlessly and automatically as possible. Human error is unavoidable, so don't create opportunities for people to make mistakes. Updating external stakeholders shouldn't involve sending an email that needs to be manually processed–consent changes and data subject requests should propagate automatically across the whole ecosystem, with as little human involvement as possible.

05

Finally, your solution should **empower legal, IT, and marketing teams** to do their jobs effectively but independently. Your marketing teams shouldn't have to worry about understanding code, and your engineers shouldn't have to understand the minutiae of statutes and rulebooks; each should be able to tackle their own piece of the problem without needing to fret about the rest. Making changes to a regulatory interpretation shouldn't require you to get under the hood and rebuild your data tools, and tweaking or overwriting blocks of code shouldn't have any impact on the way consent signals flow through your business.



Different solutions will address many of these capabilities in different ways and to different degrees, so it's worth giving some thought to which functionalities are most important to your business–and how they interact with other factors such as price, customer support, or ease of implementation.

Before you move on, take a second to fill out this scoring sheet–assign a high weighted score to the factors that are front of mind while you're shopping for a privacy solution, and a low weighted score for those solutions that aren't such a big deal for your business. You might feel that all of these factors are pretty important, and that's okay–it's important to aim high as you're shopping for such an important piece of your data infrastructure.

Even so, thinking this through and weighing your priorities will help to focus your mind as you review the available options.

5 must-haves for your privacy solution

		Weight	Tool 1	Tool 2	Tool 3
Current Requirements	Ease of deployment				
	Regulatory management				
	Data processing control				
	Customized experiences				
	Web infrastructure tools				
	Consent orchestration				
	Customized data purposes				
	Identity across devices				
	Ease of use				
	Available integrations				
	Customer support				
	Security protocol				

		Weight	Tool 1	Tool 2	Tool 3
Future Requirements	Policy flexibility				
	Interoperability				
	Innovation & roadmap				
	Ecosystem				
Price	Set-up costs				
	License costs				
	Maintenance costs				
Weighted Score					

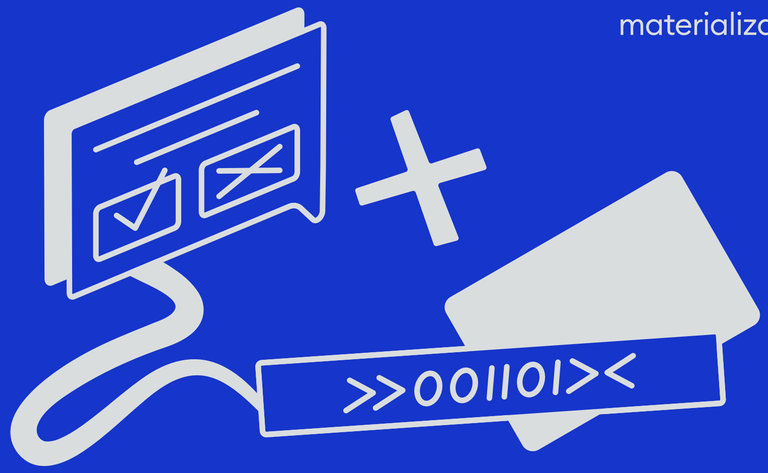
7 key questions to ask a potential vendor

Once you've found a solution that looks good on paper, you need to dig a little deeper–and that means getting to know the vendor. Not all vendors are born equal, and solutions that sound similar in theory often work very differently in practice, so it's important to ask the right questions in order to figure out what solution is best for you. Here are the 7 key questions you should ask any potential vendor before signing a deal:

Does the vendor provide turnkey tools that handle web infrastructure like tags and cookies so they fire only when appropriate consent is captured?

A common area of non-compliance in Europe happens when service providers such as your analytics and marketing service providers execute data collection on your website before appropriate consent is received from web or mobile visitors. Most privacy management systems leave you in the lurch to figure out this web infrastructure compliance yourself.

At Ketch, we configure your tag manager so that data collection happens only after appropriate consent has been confirmed–a simple approach that ensures you're verifiably compliant and in full control of your web infrastructure.



Does the vendor provide consent orchestration or synchronization? How do they send consent signals to service providers that don't have a privacy API, and can they manage consent across internal cloud systems?

Consent orchestration, which ensures service providers have the most recent consent signal so they can process (or not process) data appropriately, is a vital area for compliance. If third-party providers use the data you provide incorrectly, you could be held accountable–and their mistakes will also reflect poorly on your business and make it harder to build trust with customers.

Ketch offers robust and automated consent orchestration, with a drag and drop marketplace of service providers, workflow tools, and privacy materialization for service providers without privacy APIs.

Are Data Subject Rights requests automated? What is the workflow for ensuring compliance with requests?

When it comes to executing critical tasks in response to rights requests, such as deleting data in a service provider's system, it's important to understand whether a solution offers full automation. Many claim to be automated, but in reality only provide workflow management tools or ping a few emails around and expect you to do the heavy lifting of manually verifying compliance.

With Ketch, we take automation seriously: instead of simply sending out emails, we dock with service providers' systems to fully automate DSR execution, eliminating a major cost (and potentially a critical point of failure) for your compliance efforts.

What happens when a new regulation is enacted, or a policy position or regulatory interpretation changes?

The regulatory environment is constantly changing, so you need a solution that provides the flexibility and granularity to apply new policies on an as-needed basis, or to change legal interpretations and adapt in real time as the regulatory landscape evolves. Most content management platforms struggle with this: some might make you pay extra for new jurisdictions or regulatory modules, or require you to buy add-ons to support full customization.

The Ketch Policy Center takes the opposite approach: our "Deploy Once, Comply Everywhere" solution means you're automatically covered for all the consumer privacy regulations on the planet, with no need to worry about costly "feature creep". It also gives you full control, and lets you make changes—such as switching legal basis, or determining for yourself how new regulations affect your business—whenever you need to, without any hassle or hidden costs.

Can you customize privacy experiences, and change the language, style, and timing of notices?

Making changes to the specific wording, styling, or timing of a consent notice might sound simple, but many platforms take control out of customers' hands.

At Ketch, we believe that making changes shouldn't require a call to a support desk or exchanging messages back and forth with your vendor's tech team. That's why we offer a built-in CMS for privacy notices, allowing you to make whatever changes you want with no headaches or hassle. We also allow you to optimize delivery timing so that the right notice goes to the right person at the right time—a simple but powerful capability that increases consent rates and gives you improved access to the data needed to drive revenue growth.

Is the vendor's system cookie-based, or a holistic solution that supports compliance with ePrivacy, GDPR, and other global regulations?

Unfortunately, some vendors' offerings are more about keeping up appearances than delivering true consent management capabilities. Many platforms fail to go beyond the "Hollywood facade" of a privacy banner, or are limited to offering cookie-based consent choices that focus on site functionality. To ensure regulatory compliance, however, you need a "soup to nuts" solution that manages data across your entire ecosystem, and it's simply not possible to achieve that merely by asking whether your site can set a few cookies.

Ketch's approach runs the full gamut from creating comprehensive policies to delivering compliant privacy experiences, with full orchestration of consent and rights across all downstream systems.

Does the vendor's solution support identity management?

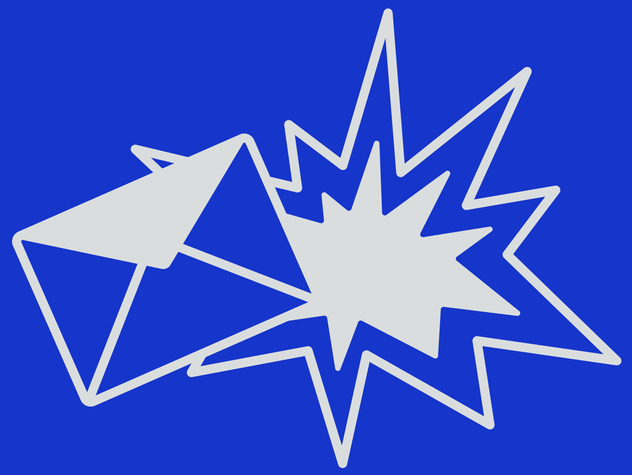
Privacy experiences should be coordinated across platforms, and anchored in an understanding of people as people, not as devices or browser IDs. That's important because repeated consent requests–once on a mobile app, again on your work laptop, and yet again on your home computer–serve to disrupt the user experience. It's also critical for downstream orchestration, since service providers require specific digital IDs or subscriber keys to identify data subjects and execute consent or rights requests.

Ketch delivers seamless user experiences by syncing across platforms, and leveraging identity infrastructure to manage consent on a person-by-person basis rather than a device-by-device basis.

Bonus Question!

Does the vendor's solution outline the purposes for which any given piece of data is permitted to be used, based on the appropriate consent, permit, or legal basis?

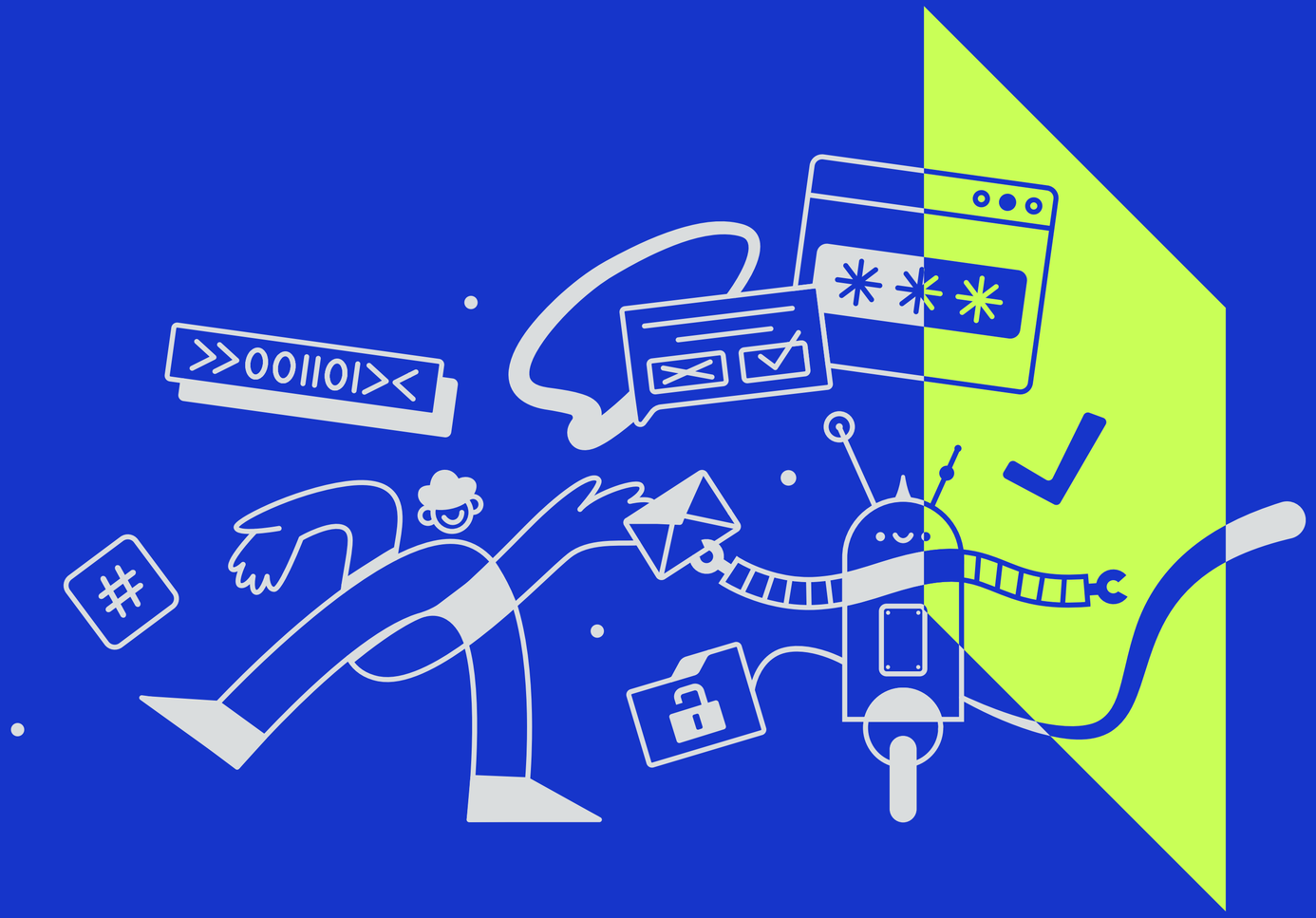
Ketch takes a holistic approach to managing consent and permits across a complete audience dataset, and across all legal bases. We believe your consent-management tools shouldn't force you to use a particular legal basis –instead, they should help you find the right way to responsibly source 100% of your data, and give you complete control of data processing for your entire dataset.



7 key questions to ask a potential vendor

Many of these questions are pretty technical, and that's by design–you'll want to make sure you can feel confident that any vendor's solution will meet your specific use-case, and that you'll be able to deploy a new solution quickly and effectively without unpleasant surprises.

But don't just pay attention to the technical stuff. Switching to a new vendor is like starting a relationship: chemistry matters, so trust your instincts as you listen to pitches and ask these questions. The ideal vendor will show a deep understanding of the challenges that come with consent management, will be forthcoming and responsive to your queries, and will be eager to learn about your organization's unique use-case. Above all, they won't respond to technical questions with jargon and arcane techno-babble–they'll just explain, simply and clearly, how their product can deliver the functionality you need.



Conclusion: Which Data Privacy Management Platform is Right For You?

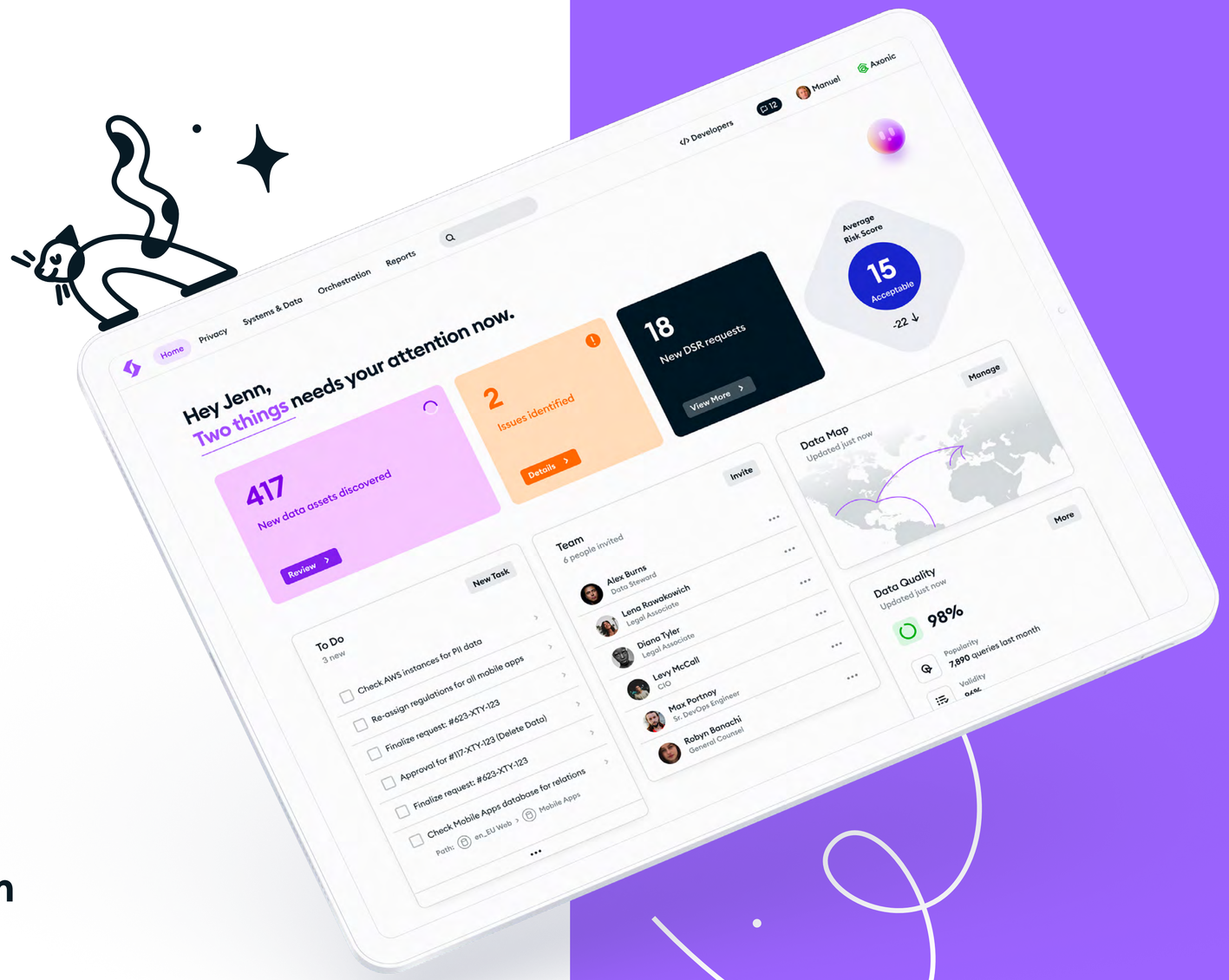
Evaluating your existing consent management solution and the available alternatives shouldn't take more than a few days of your time. The goal isn't to run sophisticated pilot studies or immediately start overhauling your data infrastructure–it's simply to take the pulse of your existing solution, to figure out what else is out there, and to make sure you're using the best possible tools for your specific needs.

Often, you'll find that a solution that was optimal a year or two ago, when you first implemented your privacy infrastructure, has now started to look a bit stale. Technologies, regulations, user expectations, and your own business needs all evolve over time, so it's worth taking some time to identify the gaps or shortcomings that you've learned to live with, and to figure out whether other vendors now offer solutions that would be better suited to your needs.

The way you handle privacy speaks volumes about your brand, so it's important to ensure you're keeping pace with the latest innovations and best-in-class solutions your customers expect. An annual check-up in advance of renewing your vendor contract can save you a lot of time and money in the long run–and if you decide to stick with your current solution, you'll be doing so secure in the knowledge that you've made that decision mindfully, and that you're using the best possible solution for your business.

At Ketch, we're confident that our data privacy technologies are the best on the market for virtually any use-case. We think you'll feel the same. That's why we encourage you to consider your evolving needs, take a long, hard look at our competitors–and then reach out to Ketch. Our team is standing by to help you choose the right platform, and to implement a sophisticated, resilient, and easy to maintain privacy-management solution designed for the unique needs of your organization.

Ketch



Want to learn more?

We'd love to show you how Ketch stacks up in the privacy compliance vendor landscape. Contact us to start the conversation.

Contact us →

ketch.com