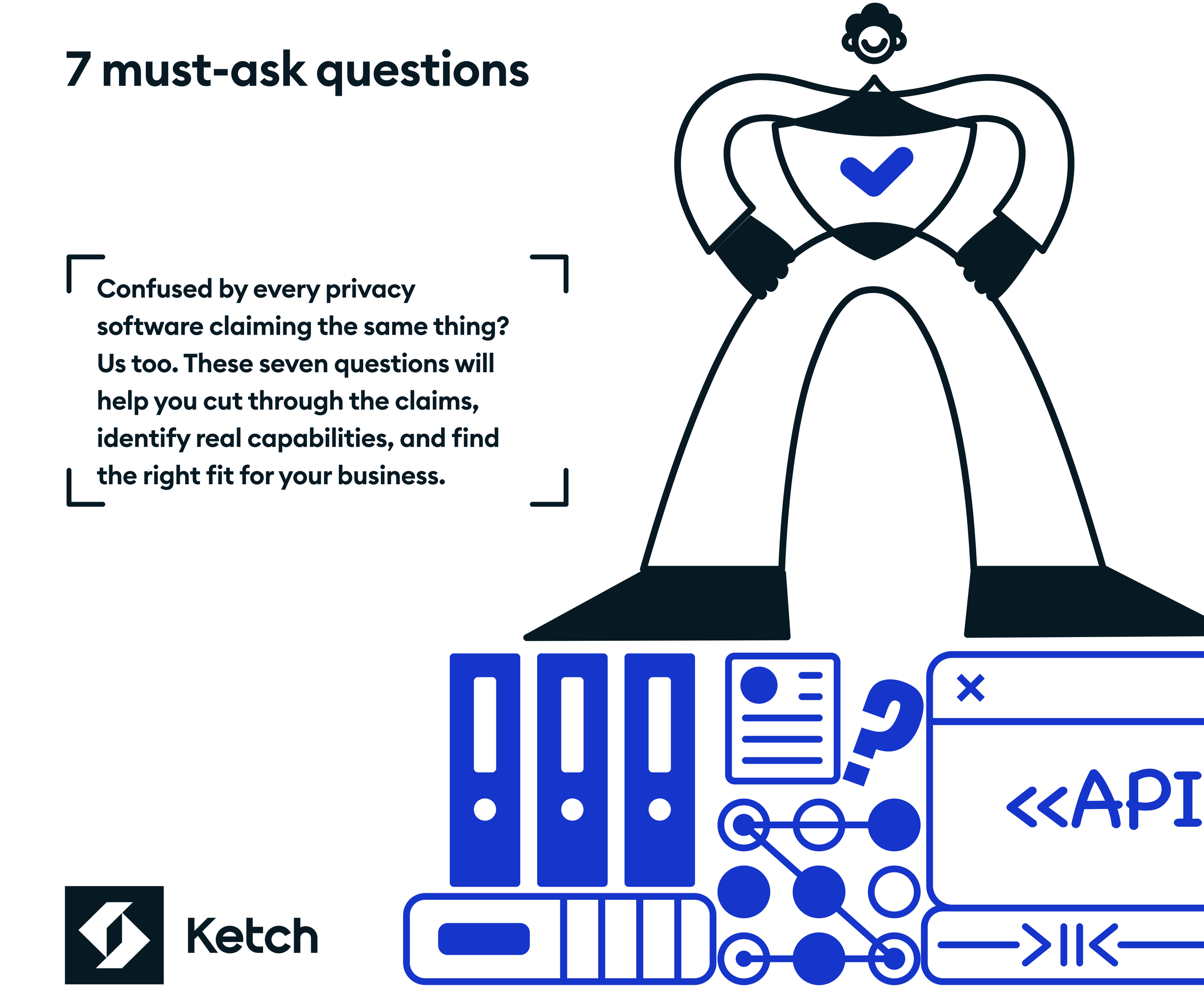
The no-BS guide to choosing privacy software

7 must-ask questions

Confused by every privacy software claiming the same thing? Us too. These seven questions will help you cut through the claims, identify real capabilities, and find the right fit for your business.



Ketch

1

How do you define automation of a data subject request (DSR)? Can you describe your workflow customization and automation options, from DSR intake to fulfillment?

Why this matters:

If your data subject requests are increasing, you likely know the repetitive, unscalable nature of manually routing and fulfilling DSRs across stakeholders and systems. The right DSR automation software can help ease this burden for your team.

> **The Ketch privacy request workflow builder did more than streamline our processes–it enabled us to fundamentally redesign how we handle DSRs... unparalleled options for task routing, system integration, and automation.**
>
> **Adam Keephart,**
> Senior Manager of Information Security, TIME

What to watch out for:

Most privacy vendors claim they can automate DSR workflows. When you hear this, dig deeper. They're usually referring to **process automation, not task automation.** This means:

- In the product, you build a process that documents the steps to complete a data subject request.
- The process can be automated, **but not the tasks themselves.** A task = email notification to the stakeholder. Your people will still need to manually retrieve or delete the desired information.
- In many cases, the product is pre-programmed with templates for DSR processes. Your business processes may need to adhere to their tasks and step order to effectively implement the product.

If automation and flexibility in fulfilling DSRs are important to you, require the vendor to walk through their process builder in granular detail. Select a tool that maps to your desired business processes–not the other way around!

How Ketch does it:

Ketch DSR automation covers the complete lifecycle of the data subject request, from consumer intake to fulfillment in your data systems. Capabilities include:

- Customizable, frontend intake form to capture requests
- **Drag-and-drop workflow** builder to design processes that map to your business stakeholders and systems; a visual system of tiles and connectors support limitless customization and flow possibilities
- **Smart routing** to customize DSR routing to specific stakeholders
- **Pre-built API connectors to hundreds of business systems and apps**, so you can automatically fulfill DSRs in your systems without human intervention; all possible with no-code configuration
- Webhooks for custom integration requirements

2

Can you describe the step-by-step process of setting up a DSR integration with one of my systems, including any professional services required?

Why this matters:

Most modern privacy regulations and laws require fulfillment of data subject requests (DSRs) in a timely manner. Setting up integrations to your systems with personal data is the best way to ensure seamless DSR fulfillment without manual errors or delays. The required steps and skillsets to set up an integration vary widely across privacy vendors. You need a repeatable resource plan in place to support initial go-live and ongoing support, as new data systems are added to the business tech stack.

What to watch out for:

Many vendors claim to have hundreds, even thousands of "easy" integrations to data systems and apps. **Before you buy, insist on seeing step-by-step documentation for setting up these integrations.** For example:

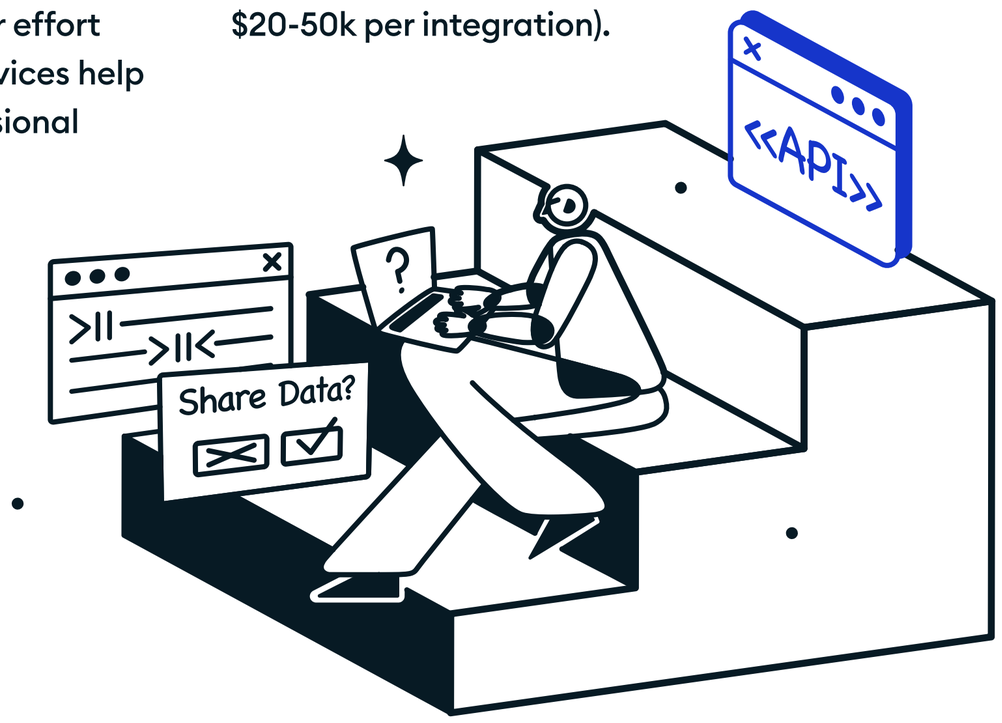
- OneTrust's quick start guide is a series of technical coding steps that will require developer help.
- Transcend's documentation outlines extensive code and architecture requirements, indigestible for a non-technical stakeholder.
- Security AI is unable to establish automated DSR integrations with popular database tools like Cosmos DB and Mongo DB, leaving privacy teams to figure out integrations for themselves.

In these cases, you need to either a) ensure your company has the development and engineering resources to support your deployment and timeline, or b) add professional services budget to your project. Do you want to pay professional services hours to get this done anytime you want to change things, or add a new system? This is a critical consideration for your time and budget.

How Ketch does it:

The Ketch Integration Library includes turnkey APIs to hundreds of marketing, ecommerce, analytics, CRM, and data platforms. Every integration can be configured by non-technical stakeholders–**clicks, not code**–with zero developer effort from your team. No professional services help is required. Have a preferred professional services partner today?
You'll be able to eliminate any integration implementation costs from your contract. Ketch software handles it for you.

These pre-built integrations save our customers extensive time (not beholden to any engineering queue or timeline) and cost (depending on complexity, professional services amount to $20-50k per integration).



Contact our team to see exact, step-by-step documentation of the process. Our team is continuously adding new integrations to the library, and our platform includes open webhooks and developer tools if you do have developer/engineering resources that want to get hands-on.

→ Contact us

3

What are the capabilities of a CMP integration? For example, when your CMP records a consumer consent signal–can your integrations push that consent signal to downstream systems? Are professional services required to set this up?

Why this matters:

Modern privacy regulations, like CCPA/CPRA in California, require you to enforce opt-outs and Do Not Sell requests across your business systems and partners (also called "flowdowns"). This means you need to pass consumer consent signals from intake on your digital properties (see: in your cookie banner), to your downstream systems. To accomplish this at scale, you need privacy software that includes integrations with the systems and applications where you store personal data. *What's on the screen (i,e., the cookie banner) vs. what happens behind the screen.*

What to watch out for:

Many privacy vendors claim they can handle integrations, but this usually refers to DSR integrations only. Integrations for the purpose of passing consent signals downstream–**AKA consent orchestration**–are overlooked.

Enforcing consent signals isn't just a regulatory requirement, it's what you need to do to respect consumers' privacy choices and avoid consent fatigue: peppering them with obnoxious pop-ups, asking the same questions every time they visit your digital properties. To ensure integrations support consent as well as DSRs, require vendor proof of functionality for these questions:

- Do your integrations that enable data subject requests also enable consent orchestration?
- What fields do you change in the respective system to accomplish consent requirements?
- How do you support IDs outside of email? For example, connecting a "Do Not Sell" selection in a website banner, to your systems that may or may not contain the user's email address?

Without these questions covered, your developers will be left to pick up the last mile; or if you don't have a developer team, an unplanned professional services expense.

How Ketch does it:

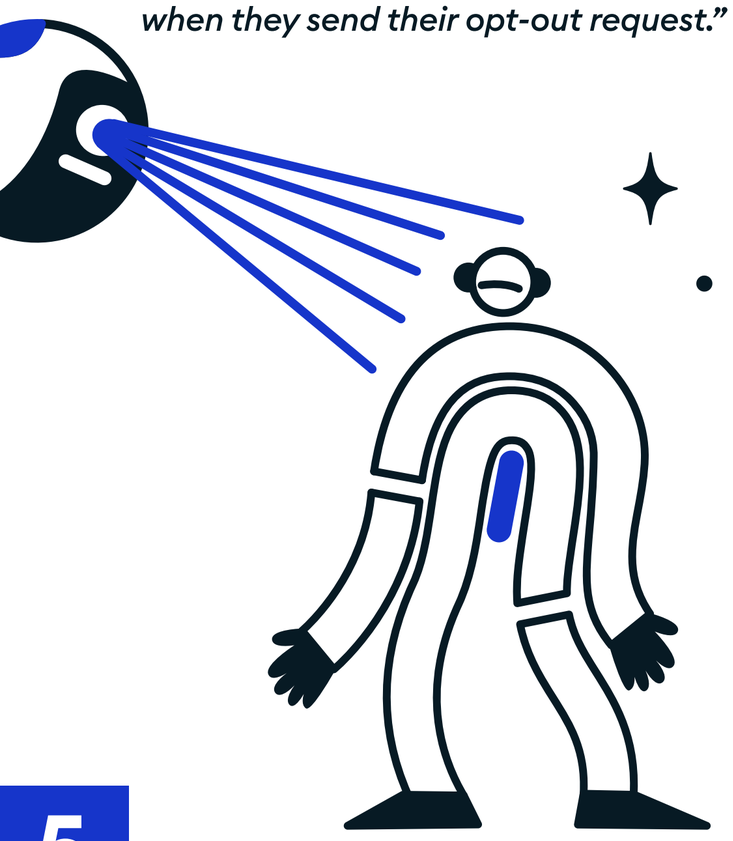
At Ketch, we call this **consent orchestration**–passing consumer privacy choices to your downstream systems and apps, to ensure knowledge of **permissioned data** across your data ecosystem. The Ketch Integration Library includes hundreds of pre-built API connectors that support integration for DSR and consent use cases. Like our DSR integrations, every consent integration can be configured by non-technical stakeholders–**clicks, not code**–with zero developer effort from your team. No professional services help is required.

4

How do you recognize and remember consumer identities? For example, how do you ensure people's consent choices are reflected across devices? How do I use your software to fulfill a DSR in a system that doesn't have email addresses?

Why this matters:

Modern privacy requirements, like fulfilling a data subject request in business systems, or remembering a consumer's opt-out choices across devices, are rooted in an expectation that the business can identify the consumer across systems, devices, channels, and platforms. We saw a recent, specific example of this in the California Attorney General's investigative sweep announcement targeting streaming services: *"Consumers should also be able to have this choice honored across different devices if they are logged into their account when they send their opt-out request."*



What to watch out for:

Many privacy software vendors have overlooked the necessity of sophisticated identity graphing architecture in the foundation of their product. Why? First-generation tools were built mostly for lawyers, solving legal privacy compliance problems. They didn't address the data management complexities and internet challenges that come with handling consumer identity across screens and touchpoints. Consumer device proliferation, the variety of tracking mechanisms on the internet, and pseudonymous identifiers create a complex web of data that is difficult to reconcile. This is a different capability that requires deep martech and adtech expertise. You must ask specific, scenario-based questions to uncover these gaps, not limited to but including:

- How do you ensure people's consent choices are reflected across devices?
- How do I use your software to fulfill a DSR in a system that doesn't have email addresses? How do you get the applicable ID to speak to that system? What has to happen to make this all work?

How Ketch does it:

Our founders' successful track record of building data management and adtech platforms, cultivating a deep understanding of the complexity of user identities and tracking, have informed the Ketch **identity synchronization architecture:**

- We begin by gathering the myriad of first-party and third-party identifiers generated by a consumer's interactions across devices and platforms. This is the foundation for understanding and respecting their privacy preferences.
- Through advanced algorithms, Ketch identifies and matches different data points, creating a unified view of the consumer. This ensures that a privacy choice made in one context is respected in all others.
- With a multitude of identifiers and potential conflicts, Ketch expertly navigates the data, ensuring that the consumer's privacy choices are consistently applied, no matter where or how they engage.

5

Can you walk through your implementation process and ongoing support model? What kinds of resources will I need–professional services, developers, engineers–for successful go-live and management?

Why this matters:

If you're considering a privacy software purchase, you likely have deadlines in mind for things like regulatory compliance, or providing permissioned data to advertising partners. To ensure your budget and staffing is ready to support a successful go-live, you need to understand exactly what the software requires.

What to watch out for:

Many privacy software platforms require professional services and developer support for aspects of the onboarding and management process. Go in with eyes wide open. Ask specifically about whether you'll need external/technical support for the following common privacy software deployment tasks:

- Creating responsive, jurisdiction-aware privacy experiences across geographies to serve the right banner or modal to the right consumer, based on their location and applicable data laws
- Setting up integrations to support DSR fulfillment and consent signal orchestration to data systems and apps

How Ketch does it:

Ketch requires no professional services for successful implementation and go-live. Our platform is expressly designed for non-technical stakeholders, like legal and marketing, to accomplish all critical tasks without engineering or developer assistance. Ketch supports your implementation with:

- Assignment of a specific Customer Success Manager upon project kick-off to guide you through the implementation, with regular check-ins
- A detailed onboarding checklist and accompanying video tutorials with detailed instructions for set-up (and all the while, your Customer Success Manager is ready to support any questions)

Following go-live, no professional services are required to successfully maintain or expand your Ketch implementation. This ensures your total cost of ownership is manageable and predictable.

6

Does your consent management platform (CMP) support recognized frameworks and requirements, including: IAB TCF purposes, GPP, GPC, and Opt Out of Sale?

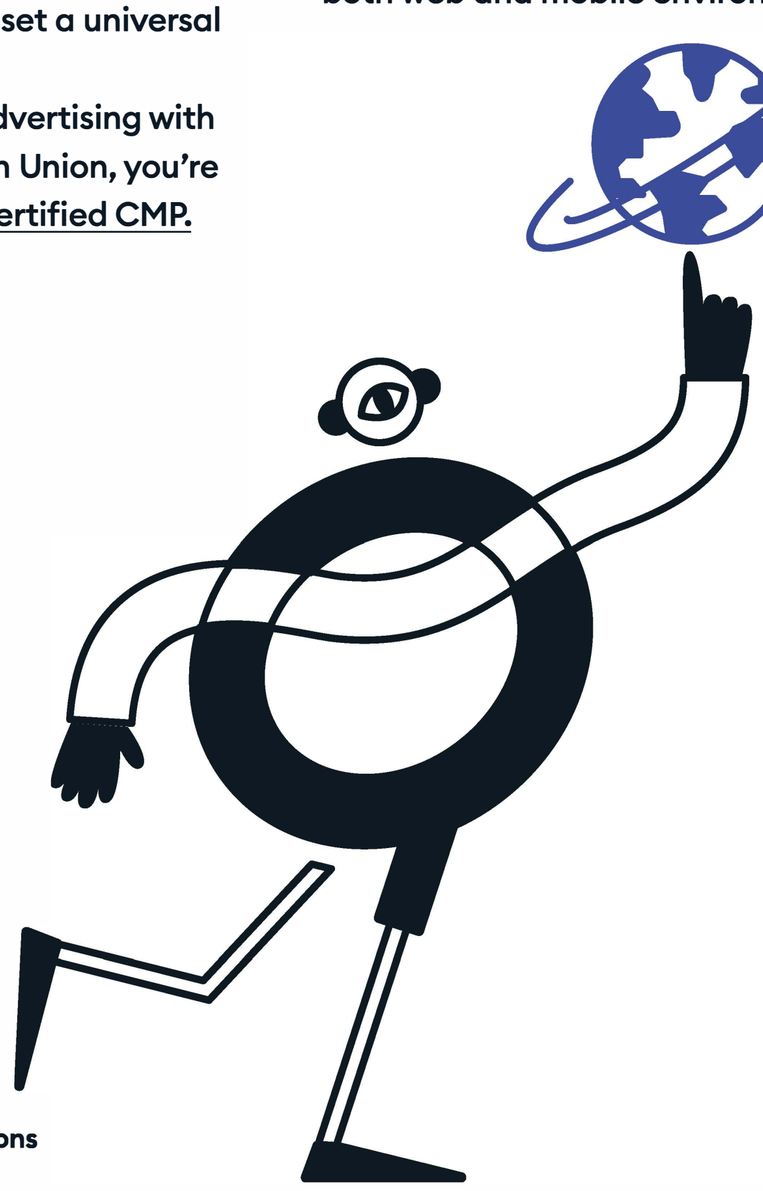
Why this matters:

A good consent management platform (CMP) helps your business comply with global privacy regulations. But beyond the federal and state regulations, there are recognized industry frameworks that require attention and adherence depending on industry sector and location. For example:

- If you partner with digital advertisers, you may need to comply with the IAB Global Privacy Platform (GPP) to pass consent signals to partners and vendors.
- Many U.S. state laws and regulations require compliance with the Global Privacy Control (GPC), a browser-based standard that enables consumers to set a universal opt-out signal.
- If your brand runs digital advertising with Google Ads in the European Union, you're required to use a Google Certified CMP.

What to watch out for:

Don't assume that CMP compliance with these industry standards is table stakes. Ask your vendor for proof of compliance with these specific standards. An especially important part of compliance with these standards is the ability to pass consumer consent signals to downstream systems–what we call consent orchestration at Ketch. Refer back to question #3 in this document for how to suss out vendor consent integration capabilities. Cross-device compliance is an important consideration for these standards, too. For example, regarding Google Certified CMP – ask your vendor if they're certified for both web and mobile environments.



How Ketch does it:

Ketch has prioritized compliance certifications across important industry standards. The Ketch platform is Google Certified for web and mobile, compliance with IAB frameworks including TCF and IAB, and can help you respect the Global Privacy Control signal across the personal data in your business ecosystem.

Ask our team for a demo to prove compliance across any of these certifications.

→ Ask for a demo

7

What is the process to stand up a new jurisdiction and corresponding frontend privacy experiences (e.g. location-aware cookie banners) in your product? Are there additional product fees or development/ engineering resources required to deploy?

Why this matters:

The privacy regulatory landscape is a patchwork of fragmented laws with varying requirements for how companies must collect, use, and retain customer data. In the United States alone, the lack of federal regulation has devolved into 18 state-level regulations with more on the way. In this uncertain environment, your business needs a consent management platform (CMP) that is flexible and responsive across regions, with the ability to quickly deploy and serve frontend privacy banners and modules that adhere to new regulations. Ideally, you need a CMP that doesn't require additional fees or heavy work to get this done; otherwise, the unpredictable nature of legislation will make it impossible for you to plan for budget and resource requirements.

What to watch out for:

Many first-generation privacy software products were built before regulations and laws ballooned into the fragmented, unpredictable landscape we have today.

Often built to comply with GDPR alone, these products lack the flexible architecture to easily support new laws. Many vendors treat new privacy laws as new "modules" for purchase, with a new license and implementation fee to support each new law. Implementation = developer/ engineering resources, whether it's your in-house team or an unexpected professional services expense.

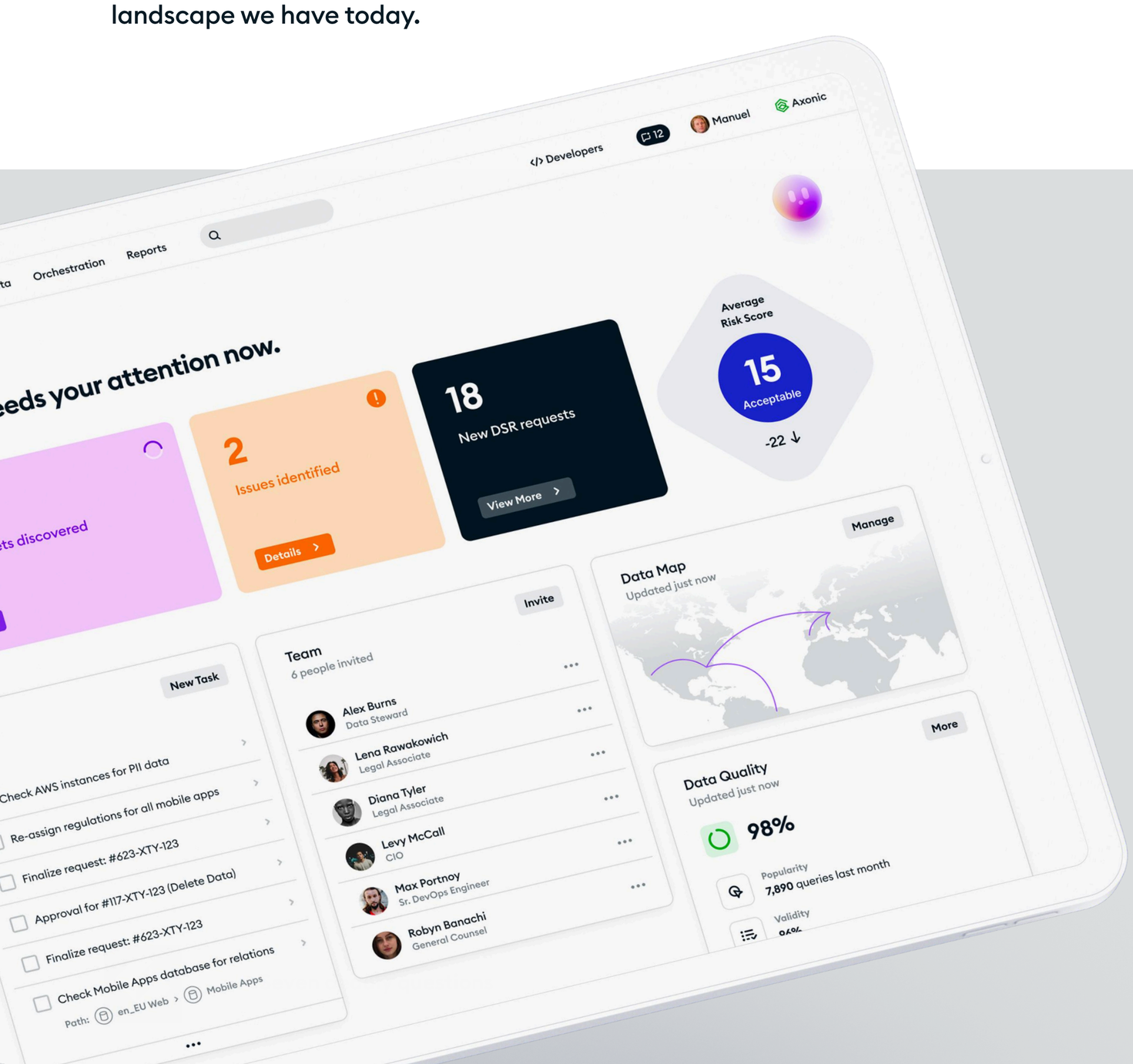
How Ketch does it:

The Ketch platform is purpose-built for today's complex legislative landscape. Our founders saw the fragmented, expanding patchwork of laws and knew our CMP needed to be flexible, responsive, and scalable. Our mantra is **Deploy Once, Comply Everywhere.** No hidden fees, and no add-on complexity for new jurisdictions.

- The Ketch CMP includes configurable policy templates for every single major privacy law (clicks, not code–no developer help required) so you can customize for your business and roll out as needed.
- Whenever a new law is passed, our team provides a new policy template.
- With each new policy deployment, your non-technical stakeholders can customize and deploy new consumer-facing privacy experiences–banners, modals, and preference centers–to match. Banners are automatically location-aware, serving the right experience to the right consumer, based on their jurisdiction and rights.

Deploy Once, Comply Everywhere.

No hidden fees, and no add-on complexity for new jurisdictions.



Do these questions hit home in your privacy tech evaluation? Ketch gives you license to steal 😉 Drop them into your RFP questionnaire or during your next demo call.

Interested in learning more about Ketch? We'd love to talk. Click below to schedule an introductory call with our team.

Learn more →

Visit us at ketch.com