DATAGRAIL®

Privacy Management Solution Buyer's Guide

CHOOSE THE *RIGHT* PRIVACY MANAGEMENT SOLUTION FOR YOUR ORGANIZATION

You've determined that you're subject to CCPA, CPRA and/or GDPR, and now you need to figure out if there is a data privacy solution that can help handle your privacy program. You're not alone. Millions of companies are asking the same question. Designing a privacy program that instils the necessary transparency to build trust with your customers isn't always easy, but with the right partner, it can be done well.

This guide is designed to help you choose a privacy solution that is best for your company. After speaking with dozens of privacy professionals, we found **accuracy, ease of ongoing maintenance, and automation** rose to the top as the most beneficial, which is why you'll see these attributes highlighted in the requirements below.

A privacy solution is the backbone of your privacy program, and the right one should enable you to automate elements of your program, and help you fulfil requirements to become (and remain) compliant with CCPA, CPRA, GDPR, LGPD, and upcoming regulations. And, as we just saw with the passing of CPRA (otherwise known as CCPA 2.0), the laws change frequently, so a solution that will scale and evolve as regulations do is critical.

The **top five requirements** you should consider when evaluating a data privacy solution for your business include (remember the acronym DMAAP, like 'Data Map'):

1. **Detect** - Enumerates unknown systems containing personal data in your organization
2. **Map** - Discovers and maps personal data within your organization's systems
3. **Automate** - Automates privacy workflows and processes
4. **Authenticate** - Verifies an identity without requiring additional personal information
5. **Partner** - Offers a dedicated privacy program partner to ensure ongoing success

Depending on your organization's size and privacy program, you may prioritize the requirements differently. We've included a few questions to detect which requirements your organization should prioritize.

If you'd like to jump straight to the questions we recommend you ask your organizations and potential vendors, click here to jump to the appendix.

1. Detect

ENUMERATES UNKNOWN SYSTEMS CONTAINING PERSONAL DATA IN YOUR ORGANIZATION

Organizations store personal information everywhere — on locally owned databases, in cloud-based servers, in SaaS solutions (e.g. Salesforce, Snowflake, Slack, Shopify, Zendesk, Zoom etc.), and throughout their supply chain. A privacy program is only as good as the source of the data, so the first step for building your privacy program is to locate where all the personal data lives in your organization.

Most modern companies don't know where all the personal data is stored on an individual. In fact, many companies don't even know all the systems it uses that contain personal data. According to Okta, the average organization uses upwards of 190 different enterprise applications to conduct business, many of which contain personal data.

When evaluating a privacy solution, it's critical to understand how it identifies and takes inventory of all the places data is stored at an organization. Some solutions rely on you — the customer — to detect all the sources of data. Other solutions can detect new places where personal information is stored and data platforms that are *unknown* to you (also known as shadow IT). If you're 100% confident you know where all data resides in your organization, you can opt for a solution that leans on you to take inventory of where data resides. For those who aren't confident in their data locations, you should opt for a solution that can detect what systems you don't know about.

Requirements for a Data Privacy Solution: DMAAP

1. Detect

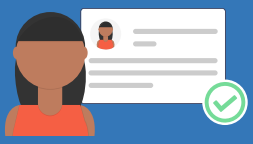
Enumerates unknown systems containing personal data in your organization

2. Map

Discovers and maps personal data within your organization's systems

3. Automate

Automates privacy workflows and processes



4. Authenticate

Verifies an identity without requiring additional personal information

5. Partner

Offers a dedicated privacy program partner to ensure ongoing success

The ideal data privacy solution will augment your existing inventory of known data sources with any additional data platforms it finds after integrating with systems in your IT environment. It should perform a system discovery and inventory to find any unknown sources of data, like SaaS applications brought on by different departments.

Detecting all the data platforms containing personal data is critical to complying with many elements of the new privacy regulations, including:

- Records of Processing Activity (RoPA) (GDPR's Article 30)
- Data protection impact assessment (DPIA)
- Data subject access request (DSAR) completion

Without an accurate account of every system containing personal data, companies risk being fined. We're seeing that hundreds of the fines being issued (totalling millions of dollars) are due to non-compliance with basic privacy principles and insufficient fulfillment of rights requests.

> "The ideal data privacy solution will augment your existing inventory of known data sources with any additional data platforms it finds."

2. Map

DISCOVERS AND MAPS PERSONAL DATA WITHIN YOUR ORGANIZATION'S SYSTEMS

Once you've found all the applications, databases, systems, etc. that contain personal data, the next task is to **connect and discover** data within those systems so you can map and classify that data in such a way that it's **usable** for your privacy program. Before we get to the "usable" part, let's dive deeper into what it means to "connect and discover".

A privacy solution should connect with your data sources so it can be updated in real-time to create a data map — a living blueprint of all the data in your organization. The data mapping functionality should automatically capture changes as new data is created & stored or a new data platform is added to your environment.

There are three core components to great data discovery: breadth, depth, and continuous accuracy.

Breadth of data discoverability

The ideal privacy solution should have the ability to integrate directly with all the different types of data platforms at your organization:

- Internally owned and managed data platforms (on-prem or hosted on AWS or Snowflake)
- Third-party SaaS solutions
- Structured and unstructured datasets

Questions to answer about your organization

1 How many internal resources can you dedicate to privacy?

a. Do you have anyone working on privacy? If so, how many people?

b. How many internal IT resources can you dedicate to privacy?

If you have limited resources, you're likely on the hunt for a solution that can "check the boxes" on privacy compliance. You'll need a privacy solution that provides ongoing support and can be a dedicated resource to help you build your privacy program as it progresses. You'll need something that can lighten the load for your internal privacy team (if you have one!).

Larger organizations are more likely to have dedicated privacy teams and are searching for a one-stop-shop privacy solution — automating workflows, uncovering new sources of personal data, and building custom integrations that connect to internally owned data platforms. As a large organization, you need a technology solution that's willing to partner with you AND your other solutions in your tech stack, to ensure you're designing a holistic privacy program that can lead to the transparency you need at your organization to build trust with customers.

2 Where is personal data stored in your organization?

This is typically the hardest question for companies to answer, simply because most companies have grown organically over the past several years, and no single person has a handle on all the new technologies brought on that could contain personal data.

At smaller organizations, it might be easier to complete an audit; however, at large organizations (even with a big IT team) it's often impossible. If this sounds like you, prioritize a solution that can easily find unknown sources of personal data. This is critical to creating a solid foundation for your privacy program.

3 Have you had your first data subject access requests (DSARs)?

Regardless of how many DSARs your organization is experiencing, consider seeking out a solution that can help automate the fulfilment and processing of DSARs. Without a technology solution that helps with automation, you'll find yourself manually processing DSARs requests that can take a lot of time and are error-prone.

Business-to-consumer (B2C) and data broker companies are likely to receive a higher volume of data subject requests. In fact, DataGrail research shows that the average B2C company should expect to receive 170 DSARs for every million records they have — with Do-Not-Sell requests being the most popular type of request. If you anticipate a higher volume of DSARs, seek out a data privacy solution that also does real-time data mapping to ensure more accuracy and reduce the likelihood of fines.

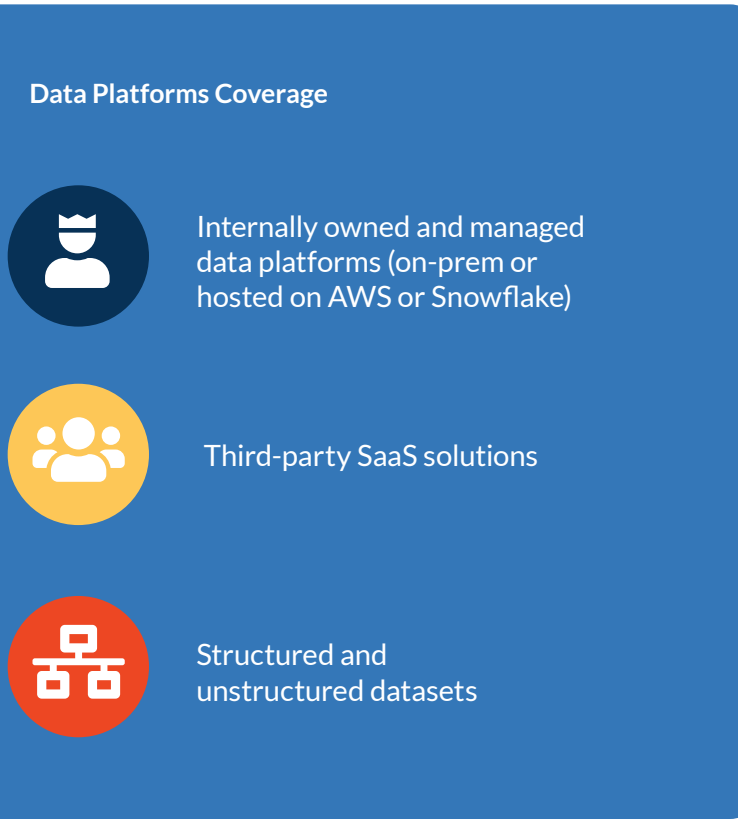
2. Map (Cont.)

DISCOVERS AND MAPS PERSONAL DATA WITHIN YOUR ORGANIZATION'S SYSTEMS

If you have personal information stored in SaaS apps, data lakes, and unstructured datasets, find a privacy solution robust enough to connect into all of your data platforms.

Take note: tackling an unstructured dataset requires distinct technology and some customization on behalf of the privacy solution. Find a privacy solution with an "unstructured integration" that is reusable and requires minimal customization to ensure a speedy onboarding and implementation. It's best to avoid solutions that put unnecessary engineering work on your team or require multiple hours of professional services.

If you find that most of your data resides in third-party solutions (e.g. Salesforce, Mailchimp, Marketo, or Okta), prioritize a solution that does an excellent job using APIs and pre-built connectors to make onboarding and maintenance a breeze. Direct integrations ensure a quality foundation for your privacy program.



Depth of data coverage

For some, a solution that goes the extra mile to classify and correlate data is valuable. For larger organizations that handle a lot of data that might not be instantly attached to a person's record, you may need a solution that does correlation — but this might not be necessary for all organizations.

The accuracy of data discovery is foundational to any privacy program. Seek out a solution that has strong data discovery capabilities to make it instantly usable for your privacy program.

> "Prioritize a solution that does an excellent job using APIs and pre-built connectors to make onboarding and maintenance a breeze."

Continuous accuracy

Data is dynamic, not static. Fields in data platforms are always changing, and so are the systems your organization uses to store personal data. This is where the concept of "usable" comes in. You should not be asked to fill out spreadsheets or surveys — this should all be automated, ensuring real-time accuracy so you can be continuously compliant. With real-time updates being made to your data map, you're establishing a high quality data foundation and creating efficiencies at your organization.

The data map should be an integral part of the privacy management solution — not be in a separate platform or product that requires additional engineering work to be compatible with DSAR fulfillment and preference updates. Many legacy privacy vendors offer these capabilities as isolated, distinct solutions, which means they don't integrate well, and therefore aren't a one-stop-shop privacy solution.

3. Automate

AUTOMATE PRIVACY WORKFLOWS AND PROCESSES

A modern-day privacy solution should deliver automation with appropriate controls. First generations of data privacy solutions designed workflows and processes to help build the underpinnings of a privacy program.

But with new regulations, manual processes and dozens of spreadsheets are no longer sustainable. Even processing a few DSARs a month can create problems and disrupt daily business operations. Regardless of request volume, organizations are responsible for enumerating every business system containing personal data, how it's used, and why. When conducted manually, RoPAs are extremely time-consuming and perpetually out-of-date since systems change all the time. Without a technology system to help automate processes and workflows, you'll be buried beneath tedious and error-prone work.

The value of automation is two-fold:

1. **Efficiency** - save time and money, and guarantee timely responses
2. **Correctness and accuracy** - automation eliminates the risk of human error. Data shows that on average, 26 employees touch a single DSAR. Every touch is an opportunity to make a mistake. Even if every employee gets it right 99% of the time, you're still leaving yourself open to a mistake nearly 25% of the time.

Good privacy solutions automate repeatable processes and allow for organizations to add the appropriate controls and escalations. They are also designed to scale and easily add new functionality as new regulations emerge or existing regulations change.

Look for a privacy solution that can automate these regulatory requirements:

Data Subject Access Requests (DSAR)

The right solution automates a DSAR in minutes. There should be the ability to create controls and escalations so organizations can customize the process as needed. This includes all types of requests:

- The right to know (access requests)
- The right to be forgotten (deletion requests)
- The right to opt-out (Do-Not-Sell [DNS] requests)
- The right to data portability (portability requests)

It is important to note that the CCPA "opt-out" requests (i.e. DNS requests) give consumers the right to stop a business from selling their data to a third-party. It is not the same as GDPR or ePrivacy-required consent management, or cookie management, which fall under different regulations.

Be sure to find a solution that also automates the process of reaching out and communicating with service providers (processors and sub-processors) to ensure you've accurately fulfilled a DSAR.

Preference & Consent Updates

A privacy solution should make it easy to automate preferences and consent changes. Also, It should synchronize any preference updates across all business systems, ensuring an individual's preferences changes are reflected everywhere that they are supposed to occur.

Record of Processing Activities (RoPA)

A privacy solution that has a data map in place should also detect how a system is being used, which can be used to update any relevant changes to your RoPA (Article 30).

> "Two-thirds of organizations had 25 or more employees involved in managing GDPR"

Cost of Compliance Report May 2019

4. Authenticate

VERIFIES AN IDENTITY WITHOUT REQUIRING ADDITIONAL PERSONAL INFORMATION

Fraud comes up as a top concern when organizations realize that they will be handing over a PDF full of personal information to an individual exercising that right.

Your organization does not want to pass along personal information to the wrong person or to someone who is impersonating a customer.

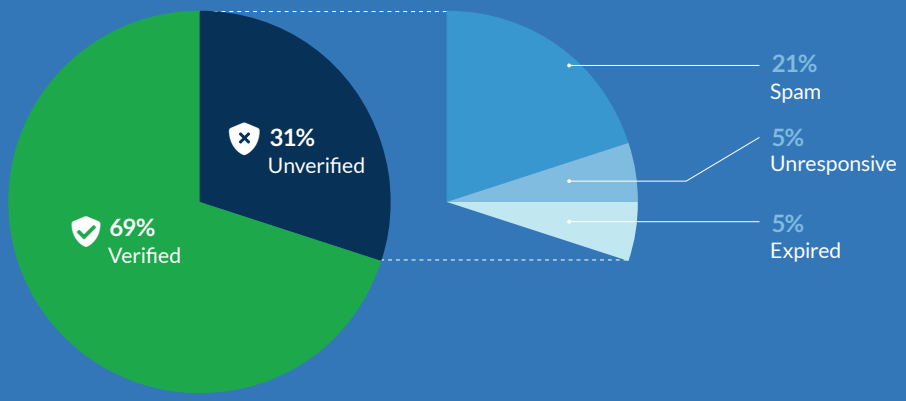
Currently, many privacy solutions ask people to provide additional data to verify their identity — like uploading a selfie or scanning their passport or driver's license. This method goes against the very spirit of these privacy regulations. Requiring a person to submit more personal information to protect their privacy was not the intention! Verification methods such as these have gained notoriety. Journalist Alastair Barr documented her negative experience in Bloomberg, and others have taken to Twitter to complain about their experiences (Forrester analyst Fatemeh Khatibloo and Coinbase PM Will Drevo).

To avoid upsetting your customers, find a privacy solution that uses existing personal information associated with a person's record, such as purchase history or user behavior (e.g. games played, purchases, or products viewed) to securely validate the individual's identity. Providing a crucial privacy-centric experience for individuals looking to safeguard their privacy is essential to preserving your brand and building a relationship of trust with your customers.

A privacy solution that doesn't require additional personal information is a massive benefit to your organization: it minimizes risk by reducing the amount of PII you're holding, making you less of a target for data breach. In many cases, businesses aren't equipped or don't want the responsibility of securely managing the storing, handling, and disposing of sensitive information and documents. A solution that leverages the existing data you have on file means that you're not taking on any additional risk.

> "Find a privacy solution that uses existing personal information associated with a person's record, such as purchase history or user behaviors to securely validate the individual's identity."

VERIFIED VS. UNVERIFIED CCPA REQUESTS BREAKDOWN H1 2020



Important to note in this graphic we're only looking at access (DSAR) and deletion requests, as DNS requests do not require the same level of verification.

Source:
Mid-Year CCPA Trends Report 2020

5. Partner

OFFERS A DEDICATED PRIVACY PARTNER TO ENSURE ONGOING SUCCESS

Privacy is a journey, not a destination. You need a partner who's going to help you every step of the way as you navigate a new regulatory space that's emerging.

That's why it's critical to choose a privacy solution that continues to work with you (without extra fees!) and builds your privacy program beyond the initial implementation.

Regarding implementation, a good privacy solution should be fairly straightforward and shouldn't require much engineering time on your part. Implementing a privacy solution doesn't need to be cumbersome or hard, but it does require a partner on the other side to ensure it goes well. When evaluating privacy management solutions, be sure to clearly understand the implementation process:

1. **How long will it take to set up my data inventory and data discovery?**
2. **How many of my resources will it require?**
3. **How long does it take to onboard an individual business system?**
4. **How does the pricing scale as your organization grows?**

Consider it a red flag if you're expected to devote many engineers to implement a privacy solution, as this suggests limited automation and lots of professional services fees down the road. Some vendors offer professional services as an add-on, while others include customer support as part of the baseline costs. Make sure you know the difference upfront so you're not stuck paying ongoing hidden fees.

Your privacy solution should promise easy ongoing maintenance. Here are a few questions to ask in advance to determine how easy (or hard) it will be to maintain a solution:

- **How many hours per week does a privacy manager spend on your product?**
- **How long does it take to refresh the data map and inventory of business systems?**
- **How long does it take to process a data subject request (DSAR)?**
- **How many people are involved in one DSAR?**
- **What customer support is included in the base fees?**

Privacy is organic and forever-changing. In turn, you need a solution that can scale and a partner who is with you the entire way to guide you through future changes you might need to make.

> "My biggest pain point is complying with the regulations in a timely manner and investing the time and resources that are required for its implementation."
>
> Cost of Compliance Report May 2019

Conclusion

Choosing a privacy solution for your company should take into account your company size, number of anticipated DSARs (if you don't know how many DSRs to expect, check out this report to help you benchmark), and how big your privacy team is.

For larger, more complex organizations, prioritize a solution that can help you build a strong data foundation for your privacy program. Push the vendor to be transparent on the ongoing drain on your internal resources.

For smaller organizations, seek out a solution that's going to partner with you the whole way through. You're going to need someone to work with you as new regulations emerge and evolve. Make sure you find a solution that can automate, easing the burden on you.

Most organizations want one privacy solution that can manage their entire privacy program, and the good news is that there are some solutions that rise to the occasion. We've found that privacy solutions that prioritize accuracy, create efficiencies, and automate tend to help organizations by doing two things:

1 Increase trust in your brand by ensuring transparency

2 Reduce the risk of being fined

The relationship businesses have with consumer data has shifted over the past 20 years. With each new technology added and the adoption of the digital transformation, consumers are often unknowingly sharing significant data about themselves: physical location, purchasing habits, fingerprints, and facial features. As a business, you know more about your customer's habits than you did in 2000.

It would be easy to approach this era of privacy with fear and concern about how this will impact profit margins, but companies who take a proactive and customer-forward privacy approach will maintain and ideally increase customer trust and brand loyalty. By building a privacy program with transparency at the heart, you'll naturally foster a more trusting relationship with your customer base. Further, proactively embracing privacy regulations is the antidote to fear and risk.

About DataGrail

DataGrail helps companies comply effortlessly with existing and emerging privacy laws, such as GDPR, CPRA and CCPA. It was designed from the ground up to automate data discovery and streamline privacy programs to create less work for customers, while also ensuring a higher level of accuracy and reduced risk. DataGrail built its solution to directly integrate with an organization's internal databases and developed 250+ pre-built connectors with companies — such as Salesforce, Shopify, Adobe, AWS, Oracle, Okta, and many others. These connections provide organizations with an accurate, real-time view of the internal systems and third-party applications used and all the personal data that maps onto each of those systems. DataGrail also allows customers to manage their privacy request workflows and email preferences across applications.

To learn more about DataGrail, please visit www.datagrail.io or follow DataGrail on Twitter and LinkedIn

Request a demo

Appendix

Questions to ask a potential vendor

Detect

Enumerates unknown systems containing personal data in your organization

1. **How does your solution find and take inventory of all the data platforms that may contain personal data?**
2. **Can the solution surface shadow IT that may contain personal data?**
3. **How does the product detect new internal systems or applications that contain personal data?**

Map

Discovers and maps personal data within your organization's systems

1. **What types of data platforms and sources does the solution connect with?**
2. **Can the solution handle unstructured data?**
3. **How does the solution integrate with a data platform to perform data mapping?**
4. **How frequently is the data map updated?**
5. **How does the solution detect changes in data platforms (e.g. field changes, new applications, new administrators, etc.)?**

Automate

Automates workflows and processes

1. **On average, how many people on my team will be involved with completing a single DSAR?**
2. **Do I need to fill out spreadsheets or workflows to complete a DSAR?**
3. **Is there a human in-the-loop from the solution for any automation? If so, how does that work in practice?**
4. **Is there an automated compliance log generated as DSARs are made?**
5. **How does the solution complete Do-Not-Sell requests?**
6. **How does the solution integrate with processors and sub-processors to fulfill access and deletion requests?**
7. **How does the solution support creating a RoPA?**
8. **How does the solution incorporate new regulatory requirements or as existing regulations change?**

Questions to ask a potential vendor

Authenticate

Verifies an identity without require additional personal information

1. **How does the solution meet the CCPA's three-step identity verification requirements?**
2. **How does the solution handle authorized agents?**
3. **Are third-party verification vendors required for identity verification?**
4. **What additional personal information is required to verify a DSAR?**

Partner

Offers a dedicated privacy partner to ensure ongoing success

1. **Can you provide 3+ enterprise references with your product?**
2. **How long will it take to set up my data inventory and data discovery?**
3. **How many of my resources will it require? How involved will my engineering or IT team need to be?**
4. **How long is the typical onboarding process?**
5. **How many hours per week does a privacy manager spend on your product?**
6. **How long does it take to refresh the data map and inventory of business systems?**
7. **How many people are involved in one DSAR?**
8. **What customer support is included in the base fees? Are there professional services?**
9. **How does the pricing scale as your organization grows?**