Your Action Plan For Data Success

US Data Privacy Checklist

With a patchwork of US state privacy laws, there's a lot of uncertainty about what needs to be done and when. Follow this action plan so you're not caught unprepared.

☐ 1. Determine Which Laws Apply to Your Organization

Which laws do you need or want to comply with? All of your consumers might live in Virginia, for instance. In that case, you'll undoubtedly want to study the VCDPA, but maybe you don't care too much about California's CPRA.

Some businesses choose to follow the most comprehensive data privacy laws, like the EU's GDPR or the CPRA, regardless of whether or not they have to. This often means they automatically meet many of the requirements of less strict data privacy laws and only have to make minor adjustments to become fully compliant.

☐ 2. Establish Project Timeline and Priorities

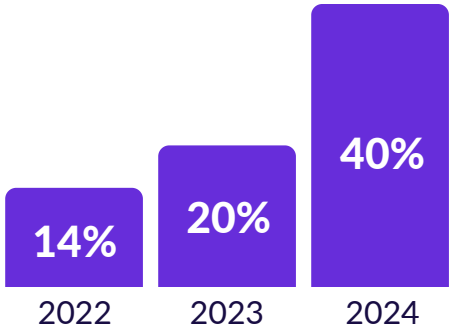
Compliance is a multifaceted and ongoing process. Odds are, your business isn't going to be able to become 100% compliant straightaway. That means you need to determine what compliance targets you need to hit first and when. Your organization might collect and process a lot of children's data, for example. This data class is often subject to multiple regulations and additional privacy requirements, so determining what you have to do to handle that data compliantly will be a priority.

Or, maybe you process special category data like genetic information or users' geolocations, which has special requirements and higher penalties for associated infractions, so you may want to become compliant with any processing activities that handle that data first. Plan out what you'll do first and when you need to accomplish it, and then proceed to build out a timeline for the foreseeable future. Even if you draw attention from data protection authorities for being only partially compliant, demonstrating that you have a plan will go a long way to mitigating your risk.

☐ 3. Update Your Data Map, Data Inventory, and/or RoPA

Anytime your organization changes how it processes personal information or embarks on a larger compliance initiative, updating or creating a data inventory is your first step.

In essence, this document should record where you collect personal information, where that data is stored, who you share it with, and virtually every detail on your processing activities you can think of. Data inventories/data maps also overlapped heavily (though not completely) with the GDPR's Record of Processing Activity requirement, or RoPA. For one, a data map should be more comprehensive and granular than a RoPa, going so far as to identify and tag individual stores of personal data across your organization.



The importance of data mapping is on the rise—40% of privacy professionals cited data mapping as a top-five strategic priority in 2024, compared to 20% in 2023 and 14% in 2022 (Source: 2024 IAPP Privacy Governance Report).

Crucially, this document must pay special attention to processing activities involving sensitive personal data. If you've identified the laws you must comply with previously in this checklist, then you'll know what specific definitions of sensitive personal data you must track and what extra steps you need to take to secure it. What qualifies as sensitive information broadly correlates with what you might consider sensitive: a data subject's gender identity, healthcare information, precise location, biometric data, and so on.

☐ 4. Identify Consent Management Mechanism

Regardless of which data privacy laws you must comply with, you'll have to manage user consent under a variety of circumstances.

For instance, it could be that you need to collect freely given, unambiguous, specific, and informed consent before you can process personal data, as is the case under the GDPR. In that case, you'll need a banner that gives website users the option of opting into or out of the use of cookies and other data trackers. Those trackers can't load until the user makes their choice, too. And you'll need a banner that displays in the language of your visitors' choice and stays up to date with changes in regulatory policy.

Obviously, operationalizing all of that is quite difficult—and that's just for the GDPR. If you want to maximize your web analytics data, you'll want to display the right banner to different individuals protected by different laws. For instance, an opt-in consent mode might be appropriate for EU website visitors, but Californian visitors are covered by a law that takes an opt-out approach to consent—meaning you can load data trackers so long as you give users an option to later opt out of tracking. How do you display the appropriate banner for any individual visiting your website across the globe?

And that's just for deploying cookie banners. There are other methods and requirements for indicating consent—some jurisdictions require you to recognize universal opt-out preference signals, like the Global Privacy Control, for instance.

☐ 5. Update Website and/or Mobile Application Privacy Policies

An important aspect of data privacy compliance is disclosing the right information to the public. As part of becoming prepared for the state data privacy laws, review your privacy policy and confirm that you're actually doing everything you claim to within your policy. Since your data processing activities will change over time, it's a good idea to review your policy once every 12 months at a minimum.

There is a spectrum of detail that the different state privacy laws require, but here's a brief overview of what's required in the CCPA/CPRA, which is among the most comprehensive:

- Categories of personal information processed.
- Purpose for processing How to exercise consumer rights.
- Categories of third parties with whom you sell or share data.
- Categories of sources of personal information.
- Description of the sale or sharing of personal information and/or targeted advertising and how to opt out.
- Retention periods for each category of personal information.
- Categories of sensitive personal information, including the purpose of collection and consumers' right to opt out.

☐ 6. Update Website and/or Mobile Application Hyperlinks

Depending on the data privacy law, you'll need to provide links or buttons that enable consumers to opt out of the sale, share, and use of their personal information and/or sensitive personal information. Importantly, these links need to be functional. When a consumer clicks on them, all of the data collection and dissemination technologies on your website need to be blocked for that consumer.

☐ 7. Establish and/or Review Consumer Request Program

As more consumers gain the ability to request DSARs and more businesses become subject to data privacy laws, businesses can expect to receive an increasing number of DSARs. Now is the time to review your existing DSAR program or develop one if you don't have a process in place.

Notably, several state privacy laws, including the CPRA, permit employees and other commercial partners to make DSARs. Employees are likely a significant source of data and especially sensitive data, making it particularly important to have a solid DSAR process in place to handle employee data.

Many data privacy laws also require you to work with your vendors who handle your consumers' personal information as well. If you built out a comprehensive data map, then identifying these vendors will be easier. Make sure you know who is responsible for what when fulfilling a consumer's DSAR request, and make sure that they know what their responsibilities are and why it's essential to meet them.

☐ 8. Review and Update Data Retention Schedules

Most data privacy laws feature a few common principles regarding data collection: Data minimization, purpose limitation, data retention, and the like. Essentially, these principles state that you should only collect as much data as you need for a specific, pre-defined purpose. Once that purpose has been met, you should delete that data.

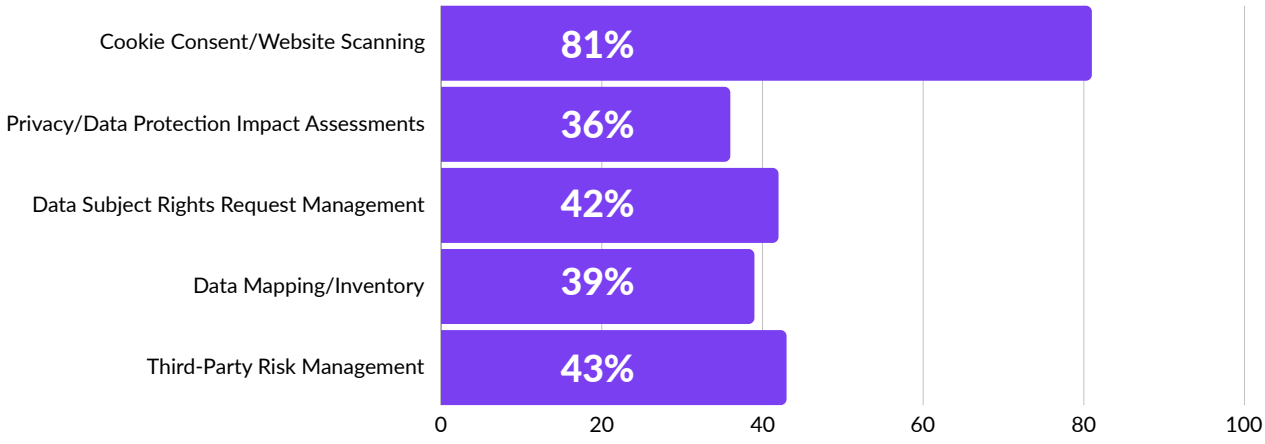
To get ready for compliance with U.S. privacy laws, review the purposes for which you collect data and the criteria you'll use to determine whether that purpose has been met. Ensure this information is reflected in your RoPA or data inventory and kept up to date. Maintaining data retention schedules this way can be challenging, but it absolutely minimizes effort and risk going forward. If your business holds onto consumer data indefinitely, then it is indefinitely responsible for that data. As just one example, handling a DSAR request can be a light lift or a weeks-long effort depending on whether you regularly delete or de-identify consumer data.

☐ 9. Prepare and/or Update Your Impact Assessments Process

Data protection impact assessments, or DPIAs, are required by several state laws to help businesses identify and address privacy risks associated with data processing activities. The events that trigger a DPIA differ from state to state, but generally, a DPIA is required anytime some new data processing activity puts consumer data at risk. As an example, DPIAs should definitely be conducted before undertaking any targeted advertising initiatives.

☐ 10. Prepare and/or Update Data Processing Agreements With Third Parties

Determine with whom you share personal information and who shares personal information with you; under state data privacy laws, your contracts with these individuals need to have the appropriate data processing addenda. Generally, these regulations have individual requirements but leave the exact form of the addendum up to you. That can make it tricky to negotiate with your different counterparties—they might have their own data processing addendum they prefer to use, in which case you'll need to find a compromise. When possible, create one addendum that covers all possible obligations so you can tailor it to individual vendors. To make this process even easier, discuss the data processing addendum as part of your vendor onboarding process.



Percentage of respondents using semi- or fully automated methods, as opposed to manual methods, to achieve various data privacy compliance tasks. *(Source: 2024 IAPP Privacy Governance Report)*

COMPLIANCE IS EASIER SAID THAN DONE

This checklist may have been a quick read, but some of the actions discussed within it can be long and arduous tasks.

Honoring consumer opt-outs, mapping your data, managing DSAR requests, and more are technically complex and potentially fraught with risk when mishandled.

If you come across an action item that seems particularly challenging when working through this list, ask yourself whether it needs to be done in-house or whether compliance could be more quickly, accurately, and cost-effectively accomplished by evaluating a third-party solution.

The Osano platform provides businesses with a solution that reduces the complexity associated with compliance. With it, you can:

- Manage user consent preferences.
- Streamline and automate DSAR processes.
- Discover and map personal data across your organization.
- Manage privacy policies.
- Evaluate vendor privacy practices with Osano's proprietary Vendor Score.
- Accomplish many more data privacy compliance tasks.

About Osano

Osano is a complete data privacy platform trusted by thousands of organizations around the world. Its platform simplifies compliance for complex data privacy laws such as GDPR, CCPS, LGPD, and more. Features include consent management, subject rights management, data discovery, and vendor risk monitoring. Osano is the most popular cookie compliance solution in the world, used on over 900,000 website to capture consent for more than 2.5 billion monthly visitors.