U.S. Multi-State Privacy Toolkit

December 2023





DISCLAIMER

Interactive Advertising Bureau, Inc. ("IAB") provides this Toolkit as a practical guide and resource for general information. Please be aware that this Toolkit does not constitute legal advice, and if you have any legal questions, please consult your attorney. While IAB has made efforts to assure the accuracy of the material in this Toolkit, it should not be treated as a basis for formulating business and legal decisions without individualized legal advice.

IAB makes no representations or warranties, express or implied, as to the completeness, correctness, or utility of the information contained in this Toolkit and assumes no liability of any kind whatsoever resulting from the use or reliance upon its contents.

© 2023 Interactive Advertising Bureau, Inc. All rights reserved. No part of this Toolkit may be sold, licensed, or otherwise commercialized without the prior written permission of IAB; provided, however, IAB hereby grants you during the full term of copyright available to the Toolkit the non-exclusive, royalty-free right and license to reproduce, customize, and use the templates, checklists, questionnaires, and guides contained herein solely in connection with your multi-state compliance efforts.



U.S. MULTI-STATE PRIVACY TOOLKIT

The number of state privacy laws continues to expand rapidly. Complying with these laws is an opportunity to develop privacy-forward practices to enhance consumer trust, but it can also be challenging to implement for many businesses – particularly where digital advertising is concerned. Compliance is a necessity, and this Toolkit provides an overview of the important state privacy law compliance priorities for publishers, advertisers, and the technology companies that make this complex marketplace function. This Toolkit is a start to conceptualizing and building a compliance program. Companies will need to undertake a comprehensive look at their specific legal and technology practices with their legal counsel and cross-functional privacy teams.

OVERVIEW

Five states have enacted generally applicable privacy laws that have or will become effective in 2023, including:

- California Consumer Privacy Act (CCPA): Enacted in June 2018 and extensively amended in 2020 by the California Privacy Rights Act (CPRA), which entered fully into effect on January 1, 2023
- Virginia Consumer Data Protection Act (VCDPA): Passed in March 2021, it entered into effect on January 1, 2023
- Colorado Privacy Act (CPA): Passed in July 2021, it entered into effect on July 1, 2023
- Connecticut Data Privacy Act (CTDPA): Passed in May 2022, it entered effect on July 1, 2023
- Utah Consumer Privacy Act (UCPA): Passed in March 2022, it will enter effect on December 31, 2023

Aside from the five comprehensive privacy laws that currently make up the US privacy landscape, organizations should also be aware of "data broker" laws in California, Nevada, Texas, and Vermont, which entered into effect in 2020, 2018, 2023 and 2019 respectively. Unlike the comprehensive state privacy laws, Nevada's law has a narrow definition of personal information and a limited right to opt-out of sales or collection of such information. The centerpiece of California's, Texas' and Vermont's laws is a requirement to register with the attorney general's office in both states. However, in October 2023 California enacted the "Delete Act" (SB 362), which significantly expands California's oversight of data brokers. In particular, the Delete Act requires the California Privacy Protection Agency (CPPA) to establish one-stop mechanism for consumers to use to send deletion requests to registered data brokers and grants the CPPA broad rulemaking authority to implement the new law.

Laws that go into effect beginning in 2024 are:

General Consumer Privacy Laws

- Texas (TDPSA): July 1, 2024
- Oregon (OCDPA): July 1, 2024



- Florida (DBR): July 1, 2024
- Montana (MCDPA): October 1, 2024
- Delaware (DPDPA): January 1, 2025
- Iowa (ICDPA): January 1, 2025
- Tennessee (TIPA): July 1, 2025
- Indiana (IDPL): January 1, 2026

Consumer Health Data Privacy Laws

- Connecticut (CTDPA): October 1, 2023
- Washington (MHMD): March 31, 2024
- Nevada (SB 370): March 31, 2024 (amending NRS Chapter 603A)

Data Broker Laws

- Oregon (HB 2052): January 1, 2024

IDENTIFY BUSINESS SCOPE IMPACTED BY PRIVACY LAWS

Organizations must identify the extent to which their business operations will be impacted by U.S. state privacy laws, particularly in relation to the following topics:

1. Are you performing programmatic (targeted) advertising?

   Identifying instances of programmatic or targeted advertising is an essential starting point. The CCPA provides consumers with a right to opt out of "selling" or "sharing" their personal information, which is closely related to the right to opt-out of "cross-context behavioral advertising" (CCBA). The CTDPA, CPA, UCPA, and VCDPA provide individuals with the right to opt-out of "targeted advertising," in addition to the right to opt-out of "sales." This step will help start a road map of where opt-outs are required. It will also clarify where exemptions or limitations may apply, such as ads based on activities on the business's own platforms.

2. Are you selling or sharing data?

   The definition of "sale" is broad, but is similar across the US state privacy laws. The CCPA defines "sell" and related terms as renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to a third party for monetary or other valuable consideration. The California Attorney General's office recently clarified the expansive scope of the term "sale" in its August 2022 enforcement action against Sephora, stating that "if companies make consumer personal information available to third parties and receive a benefit from the arrangement—such as in the form of ads targeting specific consumers—they are

deemed to be "selling" consumer personal information under the law."[3]

[1] While organizations focus on state-level privacy legislation, many of the state laws include exemptions for personal information already covered by sectoral laws in the US, including:

- Gramm-Leach-Bliley Act (GLBA): Requires financial institutions to protect consumers' financial information
- Health Insurance Portability and Accountability Act (HIPAA): Requires covered entities to prevent protected health information from being disclosed
- Fair Credit Reporting Act (FCRA): Requires consumer reporting agencies to follow certain accuracy and security requirements, in addition to use restrictions
- Family Educational Rights and Privacy Act (FERPA): Requires covered educational institutions to maintain confidentiality and provide access rights for student records

---

[2]IAB, State Privacy Law Survey Results, available at: https://www.iab.com/insights/iab-state-privacy-law-survey-results/.

[3]Complaint. People of the State of California v. Sephora USA, Inc., San Francisco Superior Court Case No. CGC-22-601380, ¶ 3.

Your organization must be aware of the activities that might qualify as a "sale." For example, the term "valuable consideration" encompasses a range of non-monetary benefits that your organization might receive in exchange for sharing consumer personal information with a third party, such as a cross-promotion where two companies agree to share each other's customer data for mutual marketing benefits, providing personal information to a third party in return for insights and analytics, or exchanging personal information for personalized recommendations, services, or products. Regulators are broadly interpreting the scope of "valuable consideration" such that sale broadly applies in the digital advertising context.

Under the CCPA, "share," "shared," or "sharing" pertains to the communication of consumer personal information to a third party for "cross-context behavioral advertising." The other state privacy laws contain a similar concept of processing personal information for "targeted advertising" purposes. "Sharing" or processing of personal information for "targeted advertising" encompass a wide variety of scenarios, regardless of any direct monetary benefit or valuable consideration, such as providing user data for targeted ads across platforms or creating segments based on bid request data across digital properties for use by advertisers.

The concepts of "sales," "shares," and "targeted advertising" apply to users that are indirectly identified ("**pseudonymous users**") or directly identified ("**known users**"). "Pseudonymous" information (i.e., information that is not attributable to a specific consumer without additional information, provided appropriate technical and



administrative measures are in place to prevent such attribution) is still personal information and is generally subject to the right to opt out sale, sharing, and targeted advertising; provided, however, pseudonymous information is exempt from opt-out rights in Iowa, Florida, and Tennessee. Hashed or encrypted email addresses are often used as pseudonymous identifiers.

Additionally, California, Connecticut, Delaware, Florida, Montana, and Oregon require consent to sell personal information or process personal information for "targeted advertising" to consumers where the business has actual knowledge or willfully disregards that the consumer is at least 13 and under 16 years old. Delaware's and Florida's laws expand the upper end of this age range to 18 years old.

In the realm of ad targeting, consumers' right to opt-out of "sales" and "shares" likely applies to the following practices:

- Third-party data and audience segments, as these likely also involve "cross-context behavioral advertising."
- Advertiser audience segments, including retargeting or custom audience lists, often classified as "cross-context behavioral advertising."
- Publisher audience segments sold programmatically, such as seller-defined audiences, as the ad delivery process typically necessitates revealing the consumer's IP address.
- Contextual targeting on programmatically sold inventory, where the ad delivery process typically involves disclosing the consumer's IP address to the winning bidder.

In the domain of ad delivery and reporting, consumers possess the right to opt-out of specific activities, which likely have implications categorized as a "sale" under the law:

- Frequency capping, as it involves passing a unique user ID to track impressions.
- Measurement, as unique user IDs are often transferred to calculate the reach and frequency of ad displays.
- Conversion tracking, as it often entails the exchange of unique user IDs for matching against impressions.
- Optimization, which can fall under the classification of both "sale" and "targeted advertising," as optimization models frequently rely on aggregating user information across advertiser campaigns.
- Any other combination of consumer personal data collected from various sources for any ad-related activity.

"De-identified" information is not considered personal information and, therefore, is not regulated by US state privacy laws. De-identified information is generally defined as information that cannot be reasonably used to infer information about, or otherwise be linked to, a particular individual (or device linked to such individual, in some states) provided that the organization that possesses such information meets certain requirements. Specifically, the organization must: (1) take reasonable steps to ensure that the information cannot be associated with an

individual (or a household, in the case of California); (2) publicly commit to process the information in de-identified form and not attempt to reidentify the information; and (3) contractually obligate any recipient of the de-identified information to comply with the obligations above.



3. Are users being profiled?

   Under the CDPA, CPA, CCPA, and VCDPA, "profiling" means any form of automated processing performed on personal data to evaluate, analyze, or predict personal aspects related to an identified or identifiable natural person's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.

   Profiling is often carried out by companies across the ad tech ecosystem (e.g., publishers, advertisers, SSPs/DSPs, DMPs). As with "sales," "shares," and "targeted advertising," "profiling" activities relate to "pseudonymous" and "known" users.

   Organizations may also need to analyze third-party data transfers to determine if these may lead to further profiling by third parties.

4. Are you processing any sensitive personal information (SPI)?

   SPI typically relates to information that is typically kept highly confidential or could lead to concrete harm if misused. US privacy laws place stricter rules for collection and usage of SPI, meaning that organizations that process SPI must take careful steps to ensure they are handling it within the boundaries of the law. In many cases, this means obtaining opt-in consent before collecting SPI. Categories of SPI under each state privacy law are listed in the table below, but determining whether specific pieces of information are sensitive is often uncertain.



	Sensitive personal information												
	Racial or Ethnic Origin	Religious Beliefs	Union Membership	Health Data	Sexual Orientation	Citizenship Status	Genetic or Biometric information	Children's Data	Geolocation	Crime Victim Status	Government ID	Financial Information	Private Comm-unications
CPRA	✓	✓	✓	✓	✓	✗	✓	✗	✓	✓	✓	✓	✓
VCDPA	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✗	✗	✗
CPA	✓	✓	✗	✓	✓	✓	✓	✓	✗	✓	✗	✗	✗
CTDPA	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✗	✗	✗
UCPA	✓	✓	✗	✓	✓	✓	✓	✗	✓	✓	✗	✗	✗

DEFINE COMPLIANCE STRATEGY

With the increasing number of state privacy laws, it is important for organizations to think through their compliance strategy. Many organizations opt to take one of two approaches:

1. National Approach
2. Geo-targeted Approach

When deciding whether to proceed with either option, the organization should consider risk, the types of processing it performs, the overall user experience, the methods used to determine a user's relevant jurisdiction, and the practical ability to provide certain rights to some individuals but not others (e.g., consumer or industry expectation, technical feasibility).

National Approach

Organizations that need to comply with laws across multiple jurisdictions may consider the "national approach," which finds a highest common denominator across the applicable laws, for the following reasons:

- It allows the organization to adopt a standardized approach across all jurisdictions. This approach offers a simpler path to multi-jurisdictional management. There will be fewer policies, interfaces, and disclosures to maintain.
- The organization may be better prepared to comply with additional laws as they go into effect. Users will have one streamlined and centralized experience to exercise rights.

- From a signaling perspective, many tracking technologies overlap with support to selling, profiling, and targeting. This approach allows for a unified user interaction to match.

There may be other considerations to this approach, including:

1. By covering all requirements with one framework, organizations will most likely need to take a more restrictive approach, even in jurisdictions that do not require it.
2. Processing performed by tracking technologies will need to be mapped to achieve the highest common legal denominator offered across jurisdictions.

Geo-targeted Approach

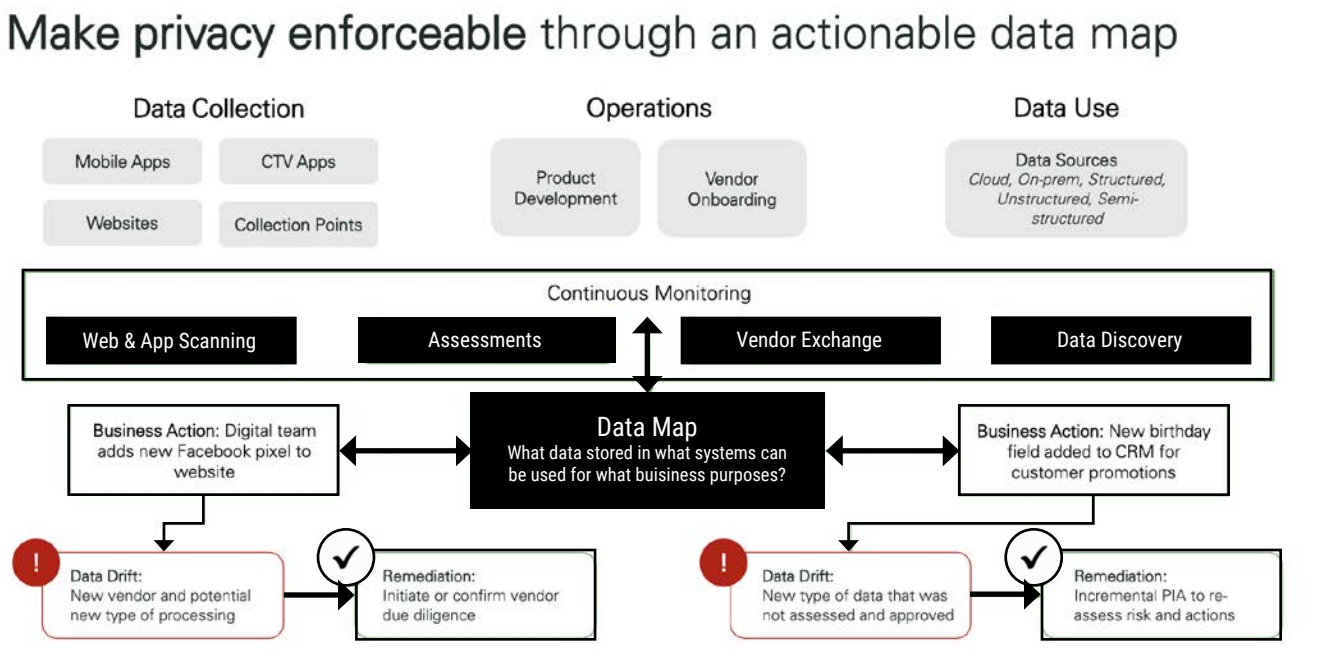
Organizations that need to comply with the laws in only a few jurisdictions might want to consider this approach for the following reasons:

1. The organization can target compliance to each user's specific jurisdiction.
2. The organization can draft narrow policies, notices, and disclosures can be that meet the requirements of a single law, rather than all laws.

There may be other considerations to this approach, including:

1. If an organization uses technology to identify a user's jurisdiction, the results may be inaccurate, especially when users are near borders or on mobile devices.
2. Consumers often travel state to state which can cause issues when determining residency or domicile.
3. If treating user rights requests as state-specific, re-prompts may occur as users move from one relevant jurisdiction to another.

IMPLEMENT COMPLIANCE STRATEGY



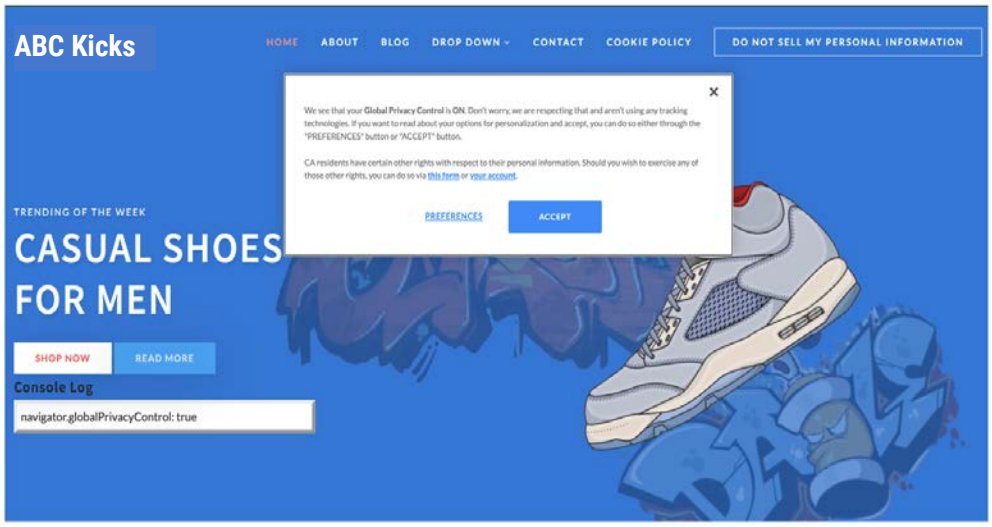
1. Front-End:

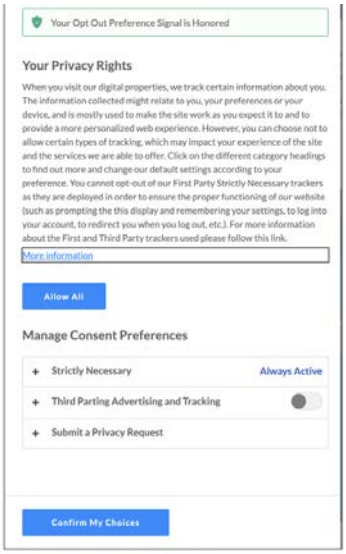
a. ***Consent & Preference Management***

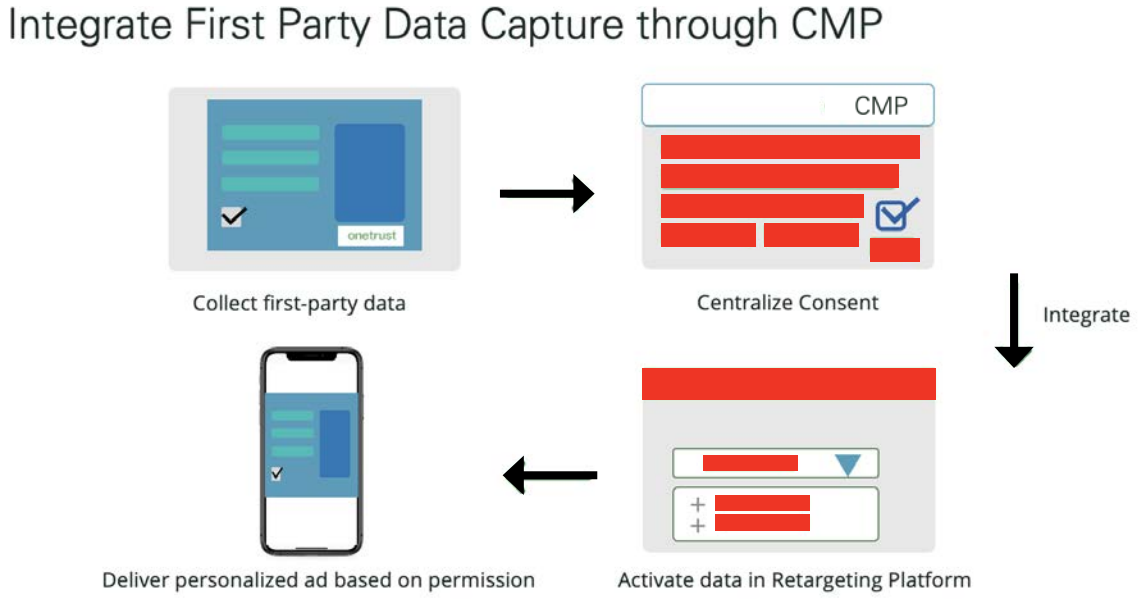
Consent & Preference management is the first step to managing user-choices and rights. This applies to both "pseudonymous" and "known" users and scales across consent to policies, consent to sale/share/profiling, consent to marketing communications and more.

To operationalize, organizations should:

- Examine their websites and mobile applications for cookies and other tracking technologies to understand how users are tracked on their websites and apps.
- Deliver a dynamic consent management platform (CMP) across websites and mobile apps that enables individuals to opt in or opt out of the use of personal data for programmatic advertising, automatically delivering the appropriate experience based on which US state privacy law applies.
- Automatically respect browser-based opt-outs like the Global Privacy Control (GPC) by orchestrating data to marketing and IT systems.
- Collect consent, preferences, and first-party data and activate data across the MarTech stack based on individual choice.
- Deliver a Preference Center to enable users to centrally manage all of their consent choices (on opt in/opt out basis, as applicable) across granular personalized choices delivered.







b. ***Re-assess Consumer Rights***

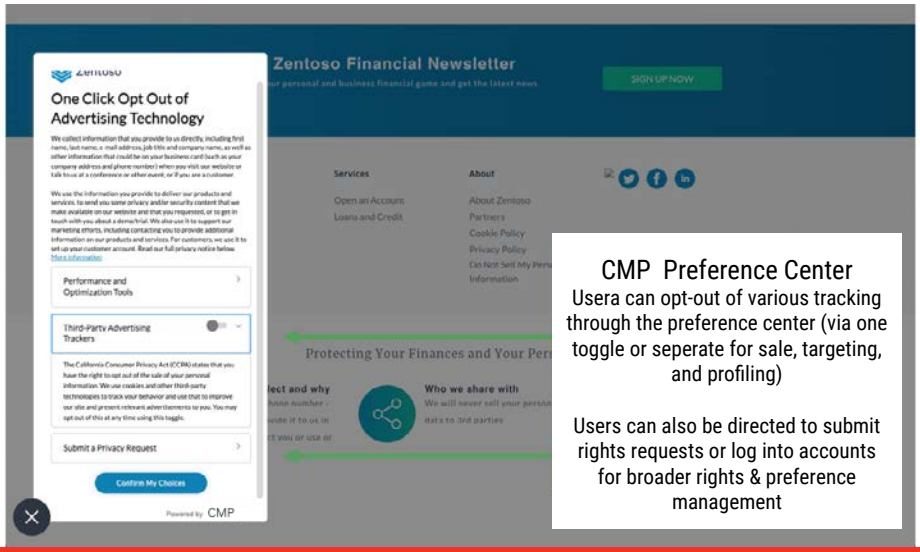
The table below summarizes consumer rights that may apply to your organization:

	Consumer Rights											
	Right to access	Right to correction/ rectification	Right to deletion	Right to opt-out				Right to non-discrimination	Sensitive data rights		Right to appeal	Right to data portability
				Sale	Sharing for CCBA	Targeted advertising	Profiling		Right to limit processing*	Right to opt-in to processing		
CPRA	✓	✓	✓	✓	✓	✗	✓	✓	✓	✗	✗	✓
VCDPA	✓	✓	✓	✓	✗	✓	✓	✓	✗	✓	✓	✓
CPA	✓	✓	✓	✓	✗	✓	✓	✓	✗	✓	✓	✓
CTDPA	✓	✓	✓	✓	✗	✓	✓	✓	✗	✓	✓	✓
UCPA	✓	✗	✓	✓	✗	✓	✗	✓	✓	✗	✗	✓

* Under the CPRA, individuals have an express right to limit the use and disclosure of their sensitive personal information in some contexts. Under the UCPA, there is a similar obligation not to process sensitive data without first presenting the consumer with clear notice and an opportunity to opt out of the processing. However, under the UCPA, different obligations based on the federal Children's Online Privacy Protection Act (COPPA) apply when processing sensitive data concerning a known child.

In general, consumer rights can be best operationalized by managing them by persona type.

Persona Type	Consumers can request	Organizations Must
Pseudonymous	• Opt out of sale • Opt out of sharing for CCBA/targeted advertising • Opt out of profiling	• Allow opt-out of device-based tracking. • Company website must be able to read and respond to device/browser privacy signals (GPC)
Known/Identified	• Data Access • Data Deletion • Opt-out Of Sale, Share, Profiling • Data Correction • Limit Use Of Sensitive Personal Information (CCPA only)	• Fulfill deletion requestions throughout all company systems. • Provide all requested data packaged and delivered to consumer securely in a readable format. • Update systems of record with rectified data • Update systems of record to limit processing of SPI



Leverage preference center for transparency, opt-outs and broader consumer requests

c. ***Privacy Notice & Disclosure***

All current US state privacy laws contain transparency provisions, and complying with all these requirements requires precision.

Privacy notice requirements vary from state-to-state, but many businesses operating in multiple jurisdictions choose to include information to satisfy the most stringent requirements. To take either a national or a state-by-state approach, the organization must first understand what is required in each state.



US state privacy laws require businesses to provide notice and generally restrict processing to purposes that are disclosed to consumers, or reasonably compatible with those purposes, at the time of collection, and prohibit "secondary uses" without consent. The CCPA, in particular, requires businesses to provide a detailed "notice at collection," which must include information about the categories of personal information collected and sold or shared, as well as retention periods.

However, across all five state privacy laws that have or will become effective in 2023, there are four constants that should be included in an organization's privacy notice: categories of personal information, purposes for its use, categories of third parties with which personal information is disclosed, and how consumers may exercise their rights under these laws.

It is important to take your audience into account when providing this information and ensure the language used is understandable and free from technical or business jargon.

Operationalize:

- Centralize all policies (internal – employee, external – consumer)
- Leverage third party tools to enable ease of development & ongoing management using workflows.
- Define templates to enable scaling of policies across jurisdictions, regulations, and business entities in scope.
- Maintain policy acknowledgment and consent records.

d. *Technology Standards to Consider*

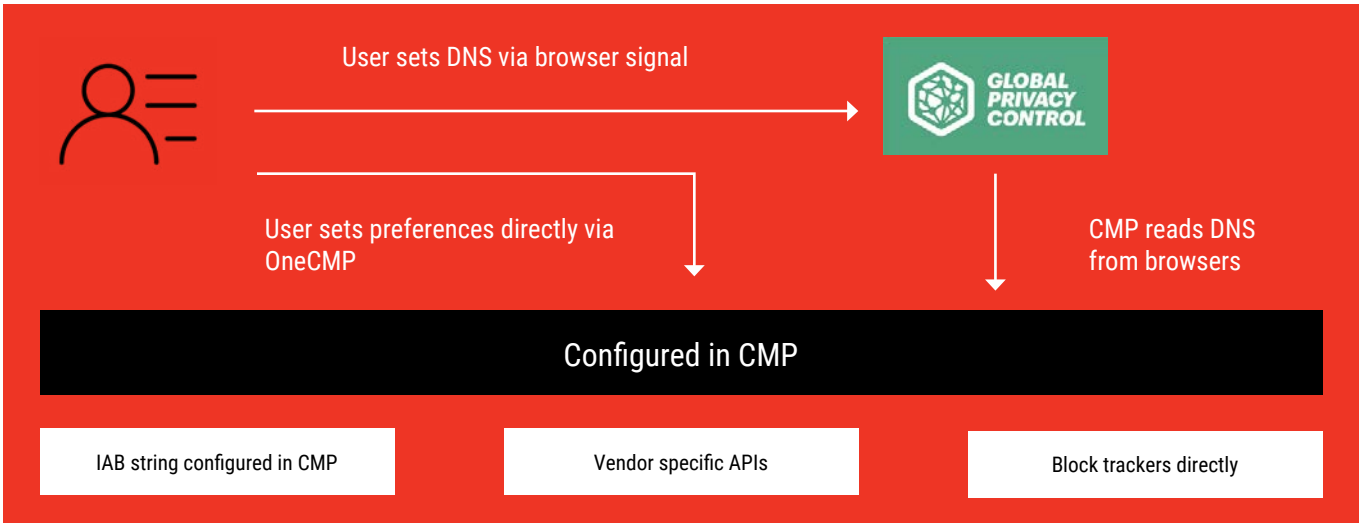
i. Global Privacy Control (GPC)

The GPC is a user-enabled method for communicating opt-out preference signals on the browser. Consumers can utilize the GPC to send a single universal signal to all webpages and applications that they interact with, rather than having to make multiple requests individually on each site. Honoring signals from the GPC or similar technologies is now mandated in certain states.

- The CCPA requires businesses to honor browser- or device-based universal opt-out signals without the user taking any further action to opt out of "sales" and "sharing." The California Attorney General issued an FAQ in July 2021 that specifically mentions the GPC as one such signal that meets the universal opt-out standard.
- The CPA and CTDPA will also allow consumers to communicate their "sale" and "targeted advertising" opt-out preferences through a "user-selected universal opt-out mechanism" or other opt-out preference signal. The Colorado Attorney General's Office will publish a list of mechanisms that businesses will be required to recognize.

- Privacy laws enacted in Delaware, Montana, Oregon, and Texas will also give consumers the right to send their preferences by opt-out signals.

Companies should leverage a CMP tool that helps deliver a compliance consent banner and supports auto-acknowledgement of GPC signal across regulations.



ii. Global Privacy Platform (GPP)

IAB Tech Lab, the digital advertising technical standards-setting body, announced the launch of its Global Privacy Platform (GPP) in 2022. The GPP is designed to streamline transmitting privacy, consent, and consumer choice signals from websites and applications to adtech vendors. The GPP enables advertisers, publishers, and technology vendors to adapt to regulatory requirements across markets.

- Companies can use a CMP that integrates with the framework in order to capture and consent signals throughout the digital ad supply chain.
- The creation of GPP consolidates the management of different consent signals from multiple global privacy jurisdictions and supports the Global Privacy Control (GPC) signal.
- IAB's existing US Privacy framework will not be updated to align with new state-level privacy laws and will be deprecated as GPP is adopted.
- IAB recommends organizations to adopt GPP, as this will be the only platform to accommodate U.S. state privacy law signaling.

Signaling Process

A GPP String's primary purpose is to encapsulate and encode all the information disclosed to a user and the expression of their choices, for all applicable regions. Using a CMP, the information is captured into an encoded and compact HTTP-transferable string. This string enables communication of the consumer's choices from sites and apps to ad tech providers. Ad tech providers decode a GPP String to determine whether they have the

necessary requirements to process a user's personal data for their purposes.

- End user lands on a publisher's website and interacts with a CMP banner (vendor registered with IAB) that is surfaced to the user based on their geography for compliance, e.g., TCF v2.2 banner for GDPR compliance, CCPA 'Do Not Sell or Share My Personal Information' Banner
- CMP encodes the choices and generates the GPP string that propagates through the pipes of communication and informs the advertisers (vendors signed up for MSPA and on the GVL) of the end user's choices.
- This string informs of users consent choices and hence influences how various data points, e.g., audience metrics, attribution, and more, are processed and in turn supports the bid for the ad-space and ad delivery.
- Sample GPP string:

Example of TCF privacy string today:
CPXxRfAPXxRfAAfKABENB-CgAAAAAAAAAAYgAAAAAAAA

Example of USPrivacy string today:
1YNN

Example of GPP string that integrates TCF and USPrivacy strings:
DBABjw~1YNN~CPXxRfAPXxRfAAfKABENB-CgAAAAAAAAAAYgAAAAAAAA

Version 1 of the GPP String contains the following information:

1. User disclosures and choices: Disclosures to and control by the user, with a given granularity dependent on jurisdictional and policy requirements (by-purpose, by-vendor, by-legal-basis, or "omnibus" all or nothing)
2. General metadata: context of the choices including timestamps, versions, CMP info, locales, publisher info, regional or jurisdictional applicability
3. Restrictions: possible additional legal, publisher, or framework restrictions

iii. App Tracking Transparency (ATT)

In addition to state privacy compliance requirement, in 2021, Apple launched iOS 14.5 and introduced its AppTrackingTransparency (ATT) requirements. Apple requires apps to use an ATT prompt to request permission from end users before "tracking" them or gaining access to their Identifier for Advertisers (IDFA). Considered the third-party cookie of mobile apps, IDFA is a familiar term for publishers, marketers, and app developers because it facilitates personalization of third-party ads, analytics, measurement, and attribution.



Operationalize:

- Scan apps for SDKs and use of the IDFA
- Understand how apps are sharing data with other third parties.
- Configure a UI and pre-prompt to collect consent when needed.
- Build a centrally located, historical consent database to comply with regulations.

1. Back-End:

a. ***Discover Data (Structured & Un-Structured) & Build Data Map***

A foundational step in any privacy program is a data discovery and mapping exercise. With differing definitions of sensitive personal information, opt-out requirements, and disclosure requirements from state to state, organizations must perform this exercise to have a clear and comprehensive understanding of their data flows. While data mapping is not required under the US state privacy laws, having a comprehensive data map can assist organizations when fulfilling consumer and employee rights, meeting data minimization requirements, managing third party risk, and responding to security incidents.

Operationalize:

a. Leverage data discovery tools to:

   i. Intelligently discover, classify, and inventory data (personal and sensitive personal information) across your IT landscape.

   i. Effectively protect and govern sensitive information through automated policy orchestration and remediation actions.

   iii. Enable privacy, data, and business teams to automate compliance activities and use data responsibly.

b. Develop a data map that gives you insights into the assets and the processing activities that are in-scope.

c. Identify assets that contain de-identified data sets and clear data categorizations.

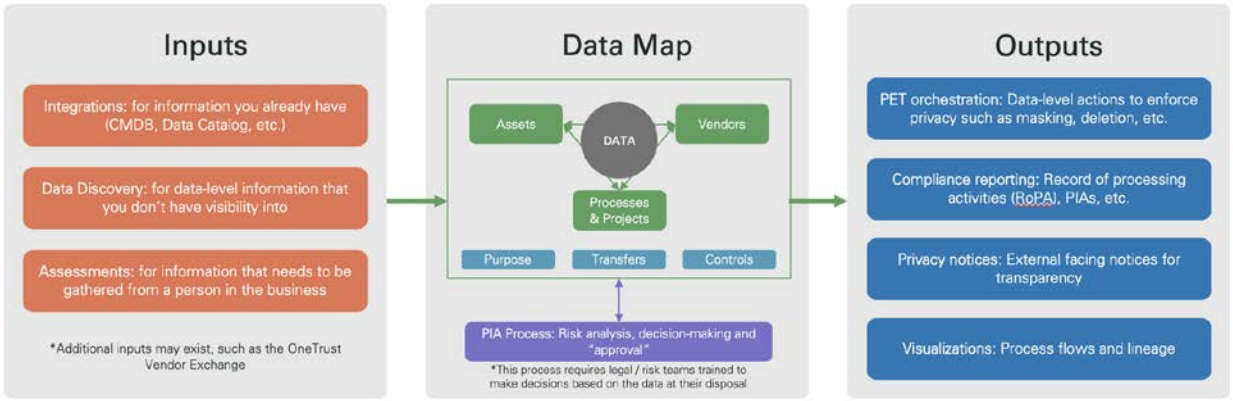
d. Identify data risks and enforce mechanisms and controls to mitigate them.

e. Exercise data minimization via actions like de-duplication, deletion, and more.

f. Leverage privacy impact assessments to get deeper insights into how data is processed and your risk exposure for the same.

g. Develop a data transfer map to understand potential cross-border data transfers.

A data map is a connected set of inventories that helps you bring the business context to your data processing, connecting what you do with data to why you do it. Why, or your 'purpose for processing', is now a critical attribute for data protection & governance, especially for personal data.



b. ***Privacy Impact Assessment (PIAs)***

Companies should consolidate information from internal and external stakeholders to gain both a technical and contextual understanding for how data is collected, the purpose for which it's being used, where the data is located, and what protections are in place.

a. Leverage pre-built assessment templates that include dynamic logic and automated risk-rules based on US privacy requirements to evaluate compliance posture.

b. Deliver business-friendly assessments that are in plain language, an intuitive UI, and integrate into product and project management tools like JIRA and embedded in existing processes to gain insights in processing activities.

c. Leverage data discovery results to pre-populate privacy risk assessments, increasing accuracy and reducing time and effort from the business to analyze data and risk status.

d. Review de-identification practices, how the data is being processed and managed across assets and processing activities.

e. Manage the entire risk workflow by automatically flagging risk, assigning tasks, tracking, and automating control implementation, and maintaining detailed recordkeeping and audit trails.

f. Conduct DPIA for identified / de-identified data sets and analyze risk posture for any data sharing or access.

g. Ensure privacy team is involved in the PIAs / DPIAs reviews and can collaborate on implementing controls to reduce or de-risk

c. *Incident Management*

Each of the 50 states has its own breach notification requirements, which makes understanding your responsibilities for reporting a security incident particularly complex. Incident response begins with understanding what types of personal information are at issue and whether they are subject to any statutory notification obligations. This includes an understanding of the timeline for notifications, who should be notified, and how. Furthermore, the CCPA provides a private right of action in certain cases where a breach occurs under California's data breach law. Regardless of the individual state requirements might apply in specific scenarios, several steps are important to include in incident response plans:

- Be prepared, establish an intake process, and understand the next steps when you are alerted to an incident.
- Investigate what happened and if personal or sensitive personal information is involved.
- Determine whether the incident requires notifying individuals, regulators, or third parties.
- Assess the incident to understand the extent and severity of the incident.
- Define a remediation strategy, limit damage, and collect and preserve evidence.
- Notify individuals, regulators, and third parties, where applicable.

Another vital part of an incident management strategy is being prepared for an increase in privacy rights requests in the fallout of any incident.

d. *Third-Party Risk Management*

"How likely is it that a vendor will have a data breach and lose personal information?"



Third-party risk management (TPRM) is a crucial component of any compliance program to help organizations identify and reduce operational risk. TPRM is equally vital in the context of the US state privacy laws, which require partner diligence and contracts to govern disclosures of personal information between advertising partners.

The IAB Multi-State Privacy Agreement (MSPA) (see www.iabprivacy.com) is an industry contractual framework intended to aid advertisers, publishers, agencies, and ad-tech intermediaries in complying with state privacy laws. This framework offers a structured approach to managing third-party risks while respecting consumer privacy rights.



- Functions as a "springing contract."
- Supplements commercial contracts among signatories with required privacy terms.
- Where there is no commercial contract between two entities, the MSPA provides the required baseline set of privacy terms.
- MSPA enables advertisers and publishers to engage ad-tech companies as limited joint service providers for specific purposes, such as measurement or frequency capping analytics.
- Advertisers can operate exclusively in either "Opt-Out Option Mode" to facilitate multi-state compliance with opt-outs under each of the state privacy laws, "Service Provider Mode" to avoid "sales" or "shares" of personal information, provided they adhere to data use limitations, such as restrictions on cross-context behavioral advertising.

Operationalize:

- Identify vendors and document what and how you use their services.
- Identify current data sharing practices and potential risks.
- Evaluate data sharing and processing of identified & de-identified data sets with vendors, partners and service providers.
- Define and implement controls to mitigate potential risks, including entering required contracts.
- Maintain an audit trail for all actions performed through the vendor lifecycle for compliance and due diligence reporting.

e. ***Automate Data Retention***

Many of the US state privacy laws now include data retention principles similar to other privacy laws around the globe.

Operationalize:

- Uncover hidden data, flag risk, and identify data policy violations through automated data discovery and classification technology.
- Automate data retention by applying pre-built retention schedules to your data sets, flagging when a retention policy is violated, and executing remedial actions like data deletion, masking, or redaction.