REDCLOVER ADVISORS

2026 PRIVACY PROGRAM

TO-DO LIST

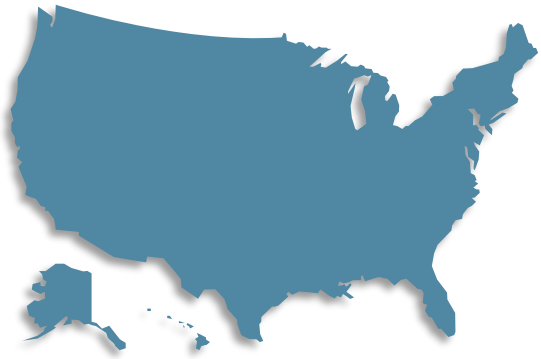
US State Law Guidance

- Simple and easy to follow privacy tasks
- Covers new and existing US data privacy laws
- Defines how each piece of the privacy compliance puzzle is useful to your organization
- Align your marketing strategy with consumer expectations

www.redcloveradvisors.com info@redcloveradvisors.com

Red Clover Advisors

2026 Privacy To-Do List



With 19 state consumer privacy laws on the books, privacy pros have their compliance work cut out for them.

Unique provisions like Minnesota's data inventory obligation, Maryland's ban on processing sensitive personal information, and Rhode Island's third-party disclosure obligations, impact every aspect of a program from data inventories to privacy risk assessments and privacy notices.

ACTION: Organizations should **conduct a privacy program assessment** to find and mitigate compliance gaps related to new obligations in advance of the effective dates.

* Provisions related to automated decision-making and risk assessments have rolling effective dates beginning in 2027.

2026: Important Dates for Compliance

New/Amended Laws

- Jan. 1: Revisions of existing CCPA obligations in new CCPA Regulations*
  Jan. 1: Indiana Consumer Data Protection Act
- Jan. 1: Kentucky Consumer Data Protection Act
- Jan. 1: Rhode Island Data Transparency and Privacy Protection Act

Right to Cure Expirations

- Jan. 1: Oregon, New Hampshire
- Jan. 31: Minnesota
- Jul. 1: Indiana, New Jersey

Data protection assessment obligations

- Jan. 1: Rhode Island
- Jun. 1: Kentucky (for activities created or generated after this date)

Universal opt-out obligations

- Jan. 1: Delaware, Oregon

Note: This checklist mainly covers comprehensive consumer privacy laws.

Red Clover Advisors

A Year of Continued Privacy Change

2025 saw states with comprehensive consumer privacy laws deepening and expanding consumer protections and raising the compliance bar for organizations. Regulators are coming into their own with enforcement sweeps, warning letters, and—increasingly—fines.

TIP: Many of the cure periods in state laws have now expired—meaning you might not get an opportunity to correct violations before an enforcement action.

2025 Enforcement Highlights

COOPERATION IN ENFORCEMENT

Regulators are conducting coordinated sweeps

CA, CO, and CT launched a coordinated sweep to find businesses violating universal opt-out obligations.

Consortium of Privacy Regulators

Regulators from CA, CO, CT, DE, IN, MN, NH, NJ, and OR have joined a consortium aimed at coordinating enforcement of state privacy laws.

- **Action:** In January, the **Texas** AG enforced against Allstate and subsidiaries alleging it developed an SDK that was harvesting consumers' data without providing notice or obtaining consent.

- **Action:** The **New York** AG settled with app developer Saturn Technologies for $650,000 under the state's unfair and deceptive practices law for allegedly failing to verify high school students' email addresses and ages, which allowed anyone to join school communities and access personal information (PI) and calendar information.

- **Action:** In July, **Connecticut**'s AG agreed to its first settlement with TicketNetwork, Inc., for $85K for a failure to cure deficiencies in its privacy notice after an initial letter sent in November 2023.

- **Enforcement Report: Oregon**'s right to cure period is in effect through Jan. 1, 2026. Even so, the DOJ issued a report noting that as of Sept. 30, 2025, it received 265 complaints and continues to send cure letters.

As state laws settle in, privacy regulators are becoming more active. It's important to get public-facing compliance obligations like consent mechanisms and privacy notices right!

Red Clover Advisors

Lessons from California Regulators

Enforcement actions provide valuable insight into what matters to regulators. With five CCPA enforcement actions in 2025, businesses can learn important lessons to help them avoid running afoul of the CPPA and the California AG.

MAR — HONDA: $635K

- Requiring verification to opt out of sale and sharing
- Using dark patterns
- Insufficient data protection agreements

MAY — TODD SNYDER: $345K

- Requiring verification to opt out of sale and sharing
- Ineffective opt-out mechanism
- Collecting more PI than needed for verification

JUL — HEALTHLINE: $1.55M

- Failure to allow consumers to opt out of targeted ads
- Purpose limitation violations
- Insufficient data protection agreements involving SPI
- Ineffective opt-out mechanism

SEP — TRACTOR SUPPLY: $1.35M

- Failure to maintain a privacy notice
- Failure to present a privacy notice to job applicants
- Ineffective opt-out mechanism, including UOOM
- Insufficient data protection agreements

OCT — SLING TV: $530K

- Requiring verification to opt out of sale and sharing
- Confusing and ineffective opt-out mechanism
- Insufficient protections for children on the platform

LESSONS LEARNED

- Regulators are looking at and testing **cookie banners**. Make sure yours show **symmetry of choice and work as they should**.
- **Data minimization and use limitation** aren't just principles, they're requirements. **Review your practices** to ensure you're not over collecting or using PI for secondary purposes without appropriate consent.
- **Data Protection Agreements** must be present any time you're sharing PI with third parties. **Review your vendor contracts** to ensure they include necessary provisions.
- Employees and candidates matter. You need to **maintain an updated privacy notice and one that includes employment use cases**.

Red Clover Advisors

A Year of Continued Privacy Change

2025 saw states with comprehensive consumer privacy laws deepening and expanding consumer protections and raising the compliance bar for organizations.

Amendment Outlook

Colorado

- Added precise geolocation data to its definition of sensitive personal information

---

Connecticut

- Added rules to better protect minors online
- Modifications to definitions of consumer health data, publicly available data, and added neural data to definition of sensitive personal data
- Expanded consumer access rights
- Lowered applicability threshold

Kentucky

- Required data protection assessments for processing that presents a "reasonably foreseeable risk" of unlawful or significant impact on consumers
- Added entity-level exemption for HIPAA-covered entities

Montana

- Added protections for minors
- Lowered applicability threshold
- Ended right to cure period
- Narrowed GLBA exemption

Oregon

- Prohibited the sale of minors' data or processing it for targeted advertising or profiling for significant decisions and increased the age limit to 16 from 15
- Prohibited the sale of precise geolocation data

Utah

- Added the right to correct personal information
- Added requirements for social media platforms related to data portability

---

Virginia

- Added rules for social media platforms to better protect minors

Red Clover Advisors

A Year of Continued Privacy Change

California passed new regulations that revise existing obligations and create new ones around cybersecurity audits, privacy risk assessments, and reporting obligations.

Did you know?
The California Privacy Protection Agency's nickname is now **CalPrivacy**.

2025 California Consumer Privacy Act New Regulations & Amendments

CCPA Regulations

New rules for **automated decision-making technology (ADMT)** used for "significant decisions."

- Pre-use notice obligation
- Consumer right to get information about use of ADMT
- Consumer right to opt out of ADMT (exceptions apply)

New **privacy risk assessments and annual reporting**.

- Must conduct assessment prior to processing that presents "significant risk" to consumers
- Must submit annual reports of risk assessments to the CPPA, including attestation to truthfulness under risk of perjury

New requirements for large businesses* to conduct annual **cybersecurity audits and submit certification**.

- Must outline authentication and access controls, personal information inventories, vendor management practices, and more
- Must submit annual audit certification to the CPPA, including attestation to truthfulness under risk of perjury

Clarification on **dark patterns**.

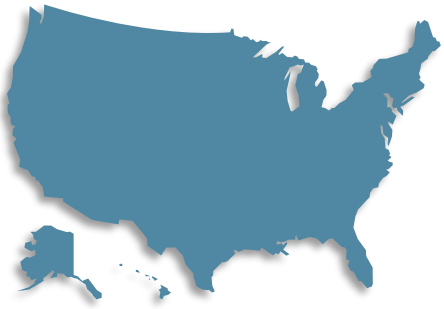
- A consumer closing or navigating away from a pop-up window on a website that requests consent does not provide consent
- Privacy options must use symmetry of choice in design elements

---

Opt Me Out Act (OOPS Act)

Requires browser developers to create and display an opt-out preference setting so consumers can opt out of the sale and sharing of browsing data across sites visited on that browser.

* Scoping threshold includes processing the PI of 250,000 Californians or SPI of 50,000. Rolling effective date based on revenue.



2026 Privacy To-Do List: Unique Requirements

Scope

All state consumer privacy laws are extraterritorial, covering organizations that process the personal information of residents of each respective state. Key differences lie in exemptions and in coverage thresholds for business size and PI processed. For example, some cover non-profits while others exempt them, and there are exemptions related to federal statutes, like HIPAA and GLBA. All laws cover "personal information," broadly defined as information relating to an identified or identifiable individual, with minor variations in wording.

Check out our website for more details on obligations!

Examples of Distinctions in Laws

MARYLAND: MD bans the processing of sensitive PI unless it is "strictly necessary to provide or maintain a specific product or service requested by the consumer." So instead of seeking consent, the law limits the opportunities for collecting, using, and sharing sensitive PI.

MINNESOTA: MN requires organizations to maintain a data inventory and an internal privacy policy.

NEW JERSEY: NJ introduces financial account access information as a form of SPI. Biometric data is defined more broadly than other states to include data generated by technological processing or analysis.

NEW HAMPSHIRE: NH's law accepts compliance with a more protective law when there's a conflict between NH and a law that provides a greater measure of privacy.

OREGON: OR grants consumers the right to request a list of specific third parties to which the controller has shared either the consumer's PI or any PI.

RHODE ISLAND: RI requires businesses to list the entities to which they have or will sell "personally identifiable information," which it fails to define.

Red Clover Advisors

2026 TO-DO LIST

TIP: A robust privacy governance framework is essential for effectively safeguarding against non-compliance.

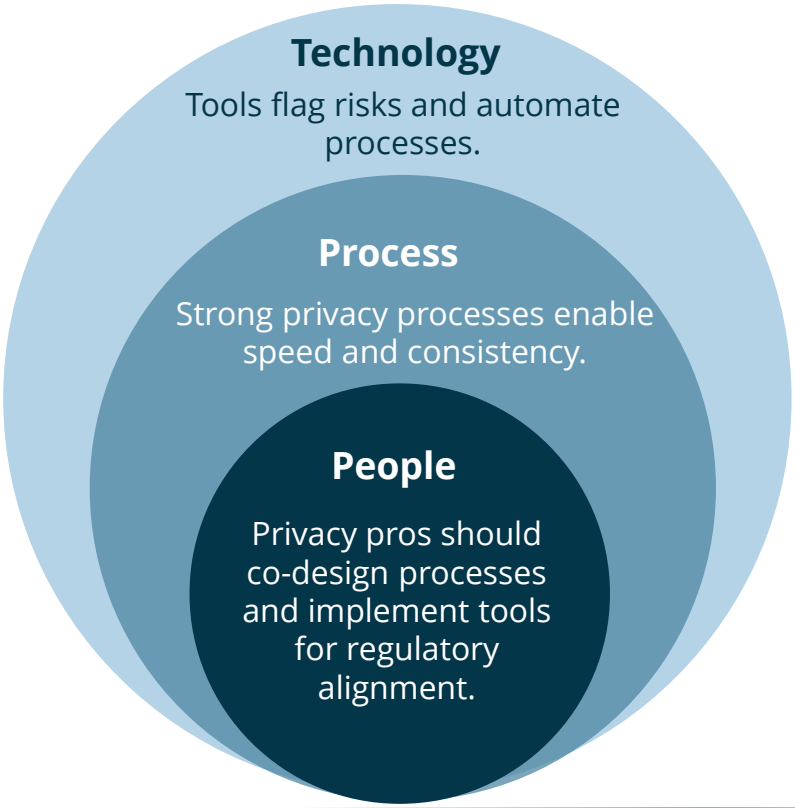
1 Establish Privacy Governance

Existing and emerging data privacy laws continue to bring to the forefront complex and challenging compliance requirements. As a result, organizations should enhance privacy governance activities by implementing reasonable and appropriate processes that support accountability, authority, risk management, and assurance.

TO DO

- ✓ Confirm your organization has adequate resources and has designated at least one person to oversee privacy.
- ✓ Establish or update organization-wide privacy policies and standards to ensure compliance with new and updated privacy laws.
- ✓ Routinely review and revise these policies and procedures to address changes in the risk landscape and the regulatory environment.
- ✓ Ensure all employees are trained on data privacy.

People, Process, Tech – Three Factors That Define Program Maturity



Effective privacy programs rely on the synergy of people, process, and technology. Each contributes unique value:

- People bring judgment and cross-functional fluency
- Process delivers structure and scalability
- Technology elevates workflows and reduces operational friction

When the three are operationally aligned, privacy becomes scalable, sustainable, and strategic.

TIP: A clear and accurate privacy notice is your opportunity to tell consumers about your data privacy practices and build trust.

2 Identify and Manage Sensitive Personal Information

Data privacy laws across the globe recognize that some personal information comes with a higher risk of harm to individuals. Sensitive Personal Information (SPI) is defined differently from one law to the next, but all state laws require elevated risk mitigation, like **conducting privacy risk assessments, disclosing your collection of it, obtaining consent or providing opt-outs for processing it, and giving consumers the ability to limit your use of it.**

TO DO

- ✓ Understand the data elements your organization collects and identify those considered SPI under applicable laws.
- ✓ Establish or update policies and procedures to limit your organization's collection, use, and disclosure of SPI.
- ✓ Create or update data protection assessment processes to ensure all processing of SPI is assessed for risk.
- ✓ Update consent and opt-out processes to obtain and track consumers' choices about their SPI.
  - ❖ Note: MD bans processing not "strictly necessary," while some states require consent and others provide opt-out rights for SPI.
- ✓ Review your organization's privacy notice to ensure it accurately discloses your practices regarding SPI.

Common SPI Data Elements*

- Race/ethnicity
- Religious/philosophical beliefs
- Sex life or sexual orientation
- Citizenship/immigration status
- Health information
- Biometric and genetic information
- Precise location
- Children's PI

Less Common Elements of SPI

- Consumer health data (CT, MD, NV, WA**)
- Financial information (CA, CT, NJ)
- National origin (MD, OR)
- Trade union membership (CA)
- Neural data (CA, CO, CT)
- Status as transgender or nonbinary (DE, MD, NJ, OR)
- Status as a victim of a crime (CT, OR)

** This list may change as privacy laws evolve.*
*** WA and NV have consumer health data-specific laws in place.*

2 Identify and Manage Sensitive Personal Information (cont'd)

Consumer Health Data

Washington, Nevada, Connecticut, and Maryland all have rules around the handling of health information. While HIPAA focuses on health information handled by healthcare providers, health exchanges, and business associates, these state laws cover health information processed by non-HIPAA-covered entities.

What Is Consumer Health Data?

Broadly, consumer health data (CHD) is personal information that is linked or reasonably linkable to a consumer and identifies a consumer's past, present, or future physical or mental health; including (but not limited to):

- ✓ Health conditions, diseases, or diagnoses
- ✓ Reproductive, sexual, or gender-affirming healthcare
- ✓ Bodily functions, vital signs, symptoms, or measurements of anything in this list
- ✓ Social, psychological, behavioral, and medical interventions and treatments
- ✓ Surgeries or other health-related procedures
- ✓ Use or purchase of prescribed medication
- ✓ Biometric and genetic data
- ✓ Data, including geolocation information that identifies a consumer seeking healthcare services or supplies

TIP: CHD is a broad category of data. Organizations need to carefully consider all the possible ways they may processes CHD.

Who Is Covered?

Laws in Connecticut, Nevada, and Washington apply to any controller—including non-profits—that operate in the states with some exceptions for federal laws. Maryland's rules apply to organizations in scope for its consumer privacy law.

TO DO:

- ✓ Revise your privacy notice to include information on your processing of CHD. *Note: Washington requires a separate notice linked from your full privacy notice.*
- ✓ Ensure you have protections around geo-targeted advertising near healthcare providers in these states.
- ✓ Review your consent mechanisms to ensure alignment with applicable laws—all four states require prior consent to sell CHD, and some require it prior to collection.
- ✓ Review tracking pixels on websites that could be classified as healthcare services.
- ✓ Update your privacy impact assessment process to include the processing of CHD.
- ✓ Review third-party contracts to ensure appropriate protections are in place if CHD is involved.

3 Conduct Privacy Impact Assessments

Most US state consumer privacy laws* require privacy impact assessments (PIAs), also called data protection assessments, for processing that represents a "heightened risk of harm" to consumers. These processing activities commonly include targeted advertising, sale of personal information, certain types of profiling, and processing sensitive personal information or personal information collected from children.

TO DO

- ✓ Revisit processing activities that require a PIA to ensure they are up-to-date with changes in jurisdictions in which your organization operates.
- ✓ Review PIA templates and instructions for use to ensure they encompass regulatory changes—especially those in California and Maryland.
- ✓ Create or revise a governance plan for your PIA program, including documented policies, record-keeping, and regular updates.
- ✓ Integrate PIAs into your procurement, development, and production processes.
- ✓ Review, revise, and deliver training on PIA obligations to all business units that interact with personal information.

TIP: Leverage existing processes created for GDPR or other international laws to create a tiered privacy risk assessment process that meets all jurisdictional obligations.

Check out Red Clover's Privacy Risk Assessment Business Guide!

* All except Utah and Iowa as of 11/2025

Red Clover Advisors

2026 TO-DO LIST

3 Conduct Privacy Impact Assessments (cont.)

"Heightened risk of harm" includes*:

- Targeted advertising
- Profiling that presents a risk of:
  - Unfair or deceptive treatment, or unlawful or disparate impact
  - Financial, physical, or reputational injury
  - Intrusion upon a consumer's solitude or seclusion, or the private affairs or concerns of the consumer, if such an intrusion would be offensive to a reasonable person
  - Other substantial injury to consumers
- Selling personal information
- Processing sensitive personal information, including children's PI

* This list may change as privacy laws evolve.

STATE-SPECIFIC VARIANCES**

** Does not include differences in all states.

Connecticut

- An amendment to the CTDPA added an additional "impact assessment" obligation for profiling for the purposes of decisions that produce legal or similarity significant effects.

Delaware

- Delaware's PIA rules apply only to controllers who control/process the PI of at least 100,000 Delaware consumers.

New Jersey

- PIAs must be conducted prior to commencing the processing activity.

California Regulations on PIAs

The CCPA regulations clarify what must be included in a CCPA-compliant risk assessment.

- A detailed description of the purpose and means of processing the PI throughout the data lifecycle
- Categories of personal information to be processed, including SPI
- Use of automated decision making, including logic and outputs, where applicable
- Approximate number of consumers
- Categories of service providers, contractors, or third parties
- A risk-benefit analysis, which evaluates negative impacts to privacy against benefits to business, consumers, and public interest
- Safeguards planned to mitigate negative impacts
- Designated personnel who reviewed and approved the risk assessment (except legal counsel who provide legal advice) and the individual that authorizes the processing

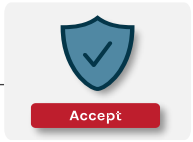
Red Clover Advisors

2026 TO-DO LIST

TIP: Collecting personal information from children under age 13 online requires parental consent under COPPA.

4 Review and Revise Consent Processes

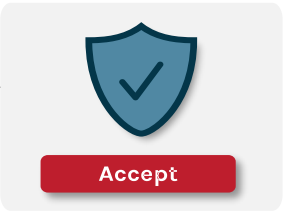
Many state privacy laws require consent for processing certain types of data.



State	Age of minor	PI of Minors					All other residents
		Sale	Targeted Ads (TA)	Profiling	Sharing for TA	Precise Geolocation	
CA	13 - 15	X	X	X	X	X	
CO	13 - 17	X	X	X		X	SPI
		Processing PI longer than reasonably necessary, secondary purposes, features that would extend or increase use					
CT	13 - 17	X	X	X			SPI, collecting or selling consumer health data
		7/1/2026: Ban on selling minors' PI or targeting ads					
DE	13 - 17	X	X	X	X		SPI
IN	N/A						SPI
IA	N/A						
KY	N/A						SPI
MD	13 - 17	BANNED	BANNED	Only when in best interests of minor			Collecting or selling consumer health data, *ban on certain processing of SPI*
MN	13 - 16	X	X	X			SPI
MT	13 - 15	X	X	X		X	SPI
		Processing PI longer than reasonably necessary, secondary purposes, using features that would extend or increase use					SPI
NB	N/A	X					SPI
NH	13 - 15	X	X				SPI
NJ	13 - 17	X	X	X			SPI
OR	13 - 15	X	X	X			SPI
		1/1/2026: Ban on sale, targeted ads, profiling					
RI	N/A						SPI
TN	N/A						SPI
TX	N/A						SPI
UT	N/A						
VA	N/A						SPI

States including Arkansas and New York don't have comprehensive privacy laws, but they do have laws protecting minors' online personal information and many states have student privacy laws.

4 Review and Revise Consent Processes (cont'd)



Many state privacy laws require consent for processing certain types of data.

TO DO

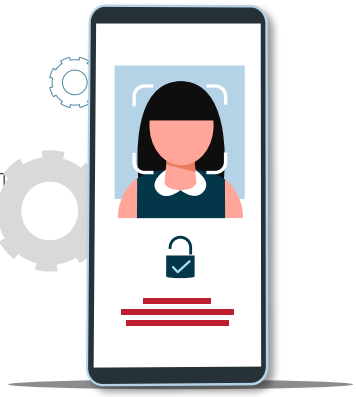
- ✓ Review and revise existing consent processes to confirm that consent is:
  - Obtained through a consumer's clear, affirmative action;
  - Freely given;
  - Specific;
  - Informed; and
  - Unambiguous.

Note: Laws in **Washington, Nevada,** and **Connecticut** require consent for processing consumer health data.

- ✓ Refresh previously granted consent, if needed, to meet the requirements of the new laws.
- ✓ Review data collection points to ensure consent is collected where necessary. And remember, some privacy laws cover information collected online *and offline*.

Information that must be made available to support informed consent:

- The controller's identity
- Why consent is being requested, in plain language
- The processing purpose(s) for which consent is sought
- The categories of personal information that will be processed to achieve the purpose(s)
- If you sell sensitive personal information, the names of all third parties that will receive it
- The consumer's right to withdraw consent at any time, and how to do so



5 Handling the PI of Minors

Children's privacy has been a major focus of both state and federal agencies for years. The FTC strengthened the Children's Online Privacy Protection Act (COPPA) as of June 2025, and states have included protections in comprehensive laws as well as passing specific privacy laws to protect minors online.

TO DO:

- ✓ Identify where you collect, share, or sell personal information and sensitive personal information about minors.
- ✓ Ensure you are only collecting the personal information necessary for the purpose.
- ✓ Obtain appropriate consent prior to the collection, sharing, or selling of personal information about minors. This may be from parents or from the minor.
- ✓ Ensure the privacy notice you present to minors is age-appropriate and easily understood.
- ✓ Confirm strong security measures are in place for the personal information you hold about children.
- ✓ Comply with parental consent requirements in the Children's Online Privacy Protection Act (COPPA) as this is generally deemed compliant with consent requirements in state privacy laws.

TIP: A child is defined as a person under age 13 by COPPA at the federal level. While many states have extended privacy protections to older minors, COPPA still applies to children under 13 throughout the US.

Variations in State Laws

- Some states have passed child-specific privacy laws, including CA, CO, CT, FL, MD, NY, UT, VA. **Nebraska and Vermont passed new age-appropriate design codes in 2025.**
- States have set different age ranges in their definition of "minor." Some states include increased protections for minors through age 17, while others stick with the obligations under COPPA.
- Some states consider PI collected *from* children to be sensitive personal information and others include any personal information *about* children.

6 Review Profiling, Personal Information Disclosures, and Targeted Advertising

Many jurisdictions require organizations to provide individuals the right to opt out of the sale of personal information, targeted advertising, and certain sharing and profiling. And some of those require organizations to recognize opt-outs via universal opt-out mechanisms like the Global Privacy Control.

TO DO

- ✓ Review automated decision making to determine whether it results in any *significant decisions* being made.
- ✓ Review contracts with third parties to identify any disclosures that may be considered a sale.
- ✓ Implement mechanisms for individuals to opt out of the sale of personal information or sharing for targeted advertising.
- ✓ Notify consumers of their rights and options and avoid using dark patterns.
- ✓ Tell consumers if their experience may change by opting out and ensure you do not discriminate against consumers who have opted out.
- ✓ **See number 13 of this To-Do List for more details.**

REMEMBER:

Not all sale and sharing of personal information occurs via cookies! Make sure your opt-out program includes all forms of sale and sharing.

CCPA-Specific Obligations

Businesses must:

- Provide consumers the option to opt out of the **sharing** of personal information for targeted advertising in addition to selling.
- Include a link with the language "Do Not Sell or Share My Personal Information" on their website's homepage or the Attorney General-approved icon paired with "Your Privacy Choices" if they sell personal information.
- State in their privacy notices whether they do or do not sell or share personal information. (Reminder: most ad-tech likely means you do!)

Actively maintain your privacy notice, checking it throughout the year to ensure it aligns with your practices and new laws.

7 Update Privacy Notices

Your privacy notice must be easy to read, available in languages in which your organization does business, and accessible to people with disabilities according to generally recognized industry standards.

TO DO

- ✓ Review new laws coming into effect to identify any compliance gaps in your privacy notices.
- ✓ Review your privacy notices at least annually based on an up-to-date data inventory to ensure your notice aligns with your practices.
- ✓ Ensure your privacy notice is accessible and understandable to your audience.
- ✓ Enhance and optimize privacy notices and terms of use to provide clarity to your customers.

State-Specific Obligations

- ➢ California has many prescriptive notice requirements, including notice of financial incentives; privacy rights metrics for certain large companies; sale and sharing activities broken out by specific categories of information identified in the law; enumerated business purposes; a specific button and/or language to allow consumers to opt out of sale or sharing from the home page; and annual review of privacy notices.
- ➢ California's Shine the Light law also requires specific notice around direct marketing.
- ➢ Texas requires businesses that sell biometric or sensitive data to post "NOTICE: We may sell your biometric personal data" or "NOTICE: We may sell your sensitive personal data," respectively, in the same location and manner as the privacy notice.
- ➢ Rhode Island requires organizations to list the entities to which they have sold or may sell personally identifiable information.

TIP: Dealing with Differences

As different laws come into force, organizations need to manage state-specific notice obligations.

Adding separate sections for obligations related to specific regions, like the EU and US states is one way to help simplify the process of updating your notices for new laws. But that can get messy!

Look for ways to manage separate obligations while streamlining your notice so it's both compliant and user-friendly.

8 Eliminate Dark Patterns

Dark patterns are user interfaces designed to manipulate users by subverting or impairing user autonomy, decision making, or choice.

Dark patterns often confuse users through visual tactics such as differing font sizes (making "opt out" smaller than "opt in"), color schemes, and asymmetrical layouts; creating designs where privacy-preserving choices are harder to see or access than less private alternatives. Additionally, deceptive wording can mislead users about their choices. Consumers usually recognize dark patterns as trickery and respond negatively to them, harming customer retention and trust in your organization.

TO DO

- ✓ Identify and review all interfaces where you provide consumers with privacy choices.
- ✓ Test your user interfaces for dark patterns; consider engaging an independent party to conduct user testing—particularly for any consent processes.
- ✓ Include individuals representing different demographics in your testing so that different perspectives and experiences are considered.
- ✓ Document the results of your testing and report out to leadership on the effectiveness of your privacy program in building fair practices that also bolster the organization's diversity, equity, and inclusion efforts.
- ✓ Create and deliver training on dark patterns for teams that develop web interfaces and consent processes.

Use the following principles when designing user interfaces:

- Choices should be presented in an **even-handed manner** (e.g., "Accept" or "Reject" in the same font, buttons the same size).
- **Silence or failure to take action** should not be considered consent.
- Avoid **pre-selected** options.
- **Exercising either choice** (consenting or not consenting) should take equal effort from the individual.
- Consider your audience's **ability to understand and navigate** when designing choice options.

Regulators have said they *do not* consider consent obtained using dark patterns valid consent!

9 Create or Revise Data Minimization, Retention, and Deletion Policies

REMEMBER:
Data you don't have is data you can't lose in a breach!

Data minimization means collecting only the information you need to achieve a stated purpose and retaining it only as long as necessary for that purpose. Many state privacy laws include data minimization obligations, but it's also just good business. Minimizing the data you hold to only that which is up-to-date, accurate, and valuable to your organization limits your risk in data breaches, lowers data storage costs, reduces the need for resources to protect and maintain the data, and ensures you are making business decisions based on good information.

TO DO

- ✓ Conduct a data inventory to get a comprehensive understanding of what personal information you are collecting and what you currently have in your systems.
- ✓ Assess collection points and ensure you are only collecting personal information needed for the purpose identified at each collection point.
- ✓ Create and implement policies and procedures to ensure new systems and processes limit the collection, use, retention, and sharing of personal information to that which is "reasonably necessary" to achieve the specified purposes of processing.
- ✓ Review deletion processes to ensure deletion is happening according to policy and identify opportunities for automation.
- ✓ Ensure data minimization is considered in privacy risk assessments.
- ✓ Look for opportunities to de-identify or anonymize personal information.

Anonymization, de-identification, and pseudonymization are valuable tools to mitigate privacy risk. All state consumer privacy laws exclude de-identified data from the scope of personal information, and many don't require businesses to provide privacy rights where data has been pseudonymized.

10 Update Your Data Inventory

Data inventories are the foundation for a successful and effective data privacy program. A data inventory establishes a comprehensive understanding of the personal information an organization holds enabling it to effectively implement privacy strategies and compliance measures.

A data inventory is the keystone that supports all other privacy functions. It is essential for compliance with US state privacy laws.

TO DO

- ✓ Review and update your data inventory to capture all your organization's current data collection and processing practices.
- ✓ Establish a cadence to regularly review data practices with business units to maintain an accurate and comprehensive data inventory.
- ✓ Prior to engaging in any new projects, review your data inventory to see how the new project will impact your existing data processing.
- ✓ Integrate data inventory updates into procedures for implementing new processes or technologies.

Relevant State Obligations

- **Oregon** and **Minnesota** give consumers the right to request the named entities with which an organization has shared personal information—the organization may either provide the entities with which it shared the specific consumer's personal information or any personal information.
- **Minnesota** requires organizations to implement and maintain a data inventory.
- **Rhode Island** requires organizations to list in their privacy notice the entities to which they have sold or may sell personally identifiable information*.

*The RI law does not define personally identifiable information.

Red Clover Advisors

2026 TO-DO LIST

11 Review and Update Contracts with Third Parties

Organizations must enter into binding contracts with vendors (also called data processors, service providers, or contractors) with which they share personal information. The contract must define the nature, purpose, and duration of the processing; the type of personal information; categories of individuals; and the obligations and rights of each party to the contract.

TO DO

- ✓ Review contracts to ensure you understand the nature of your relationships with third parties.
- ✓ Update any vendor contracts to include appropriate information, obligations, and protections.
- ✓ Create or update your third-party inventory and categorize by relationship type.
- ✓ Establish a cadence for privacy and security assessments based on risk to ensure third parties comply with contractual obligations.
- ✓ Implement procedures to identify, manage, and mitigate security and privacy risks.

STANDARD ELEMENTS TO INCLUDE IN VENDOR CONTRACTS

- ✓ **Categories of information** involved
- ✓ The **duration and location** of the processing
- ✓ Obligation to process **only as instructed**
- ✓ Obligation to **comply with applicable data protection laws**
- ✓ **Security** obligations
- ✓ Data **breach obligations** including liability and notification
- ✓ Obligation to **notify you if they can no longer meet contractual obligations**
- ✓ Obligations around **further sharing**, such as using sub-processors
- ✓ Obligation to **assist you in compliance**, especially in privacy rights response
- ✓ Your **right to monitor** compliance with the contract
- ✓ Instructions to **return or destroy** personal information at the end of the agreement

Why is this important?

Regulators may request access to contracts to ensure compliance. The CPPA has issued fines for violations including sharing PI without an appropriate contract in place!

12 Manage Privacy Rights Requests

Regulators are cracking down on businesses that violate consumer privacy rights (see page 5). These enforcement actions teach important lessons on how to do rights *right*!

TO DO

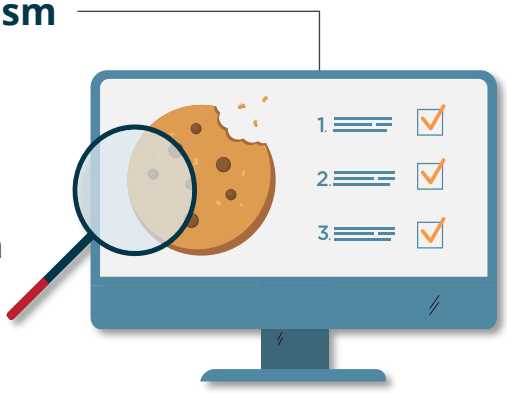
- ✓ Ensure you have privacy rights submission methods anywhere you collect personal information (e.g., websites, apps, brick and mortar locations).
- ✓ Test methods for individuals to submit privacy rights requests.
- ✓ Create or update internal procedures to respond to privacy rights requests (including from employees where applicable) that meet jurisdictional obligations.
  - ✓ Ensure your process is flexible and can handle the addition of new vendors—especially when they will need to be added to automated processes.
- ✓ Establish or test your appeals process and ensure it is conspicuous and easy to use.
- ✓ Review your privacy notice(s) to ensure rights, methods for exercising rights, and information on the appeals process are included.
  - ✓ Some laws require that organizations include in their privacy notice(s) information on how individuals can file a complaint with a regulator.
- ✓ Create a system to track and maintain records of privacy rights requests.
- ✓ Train all employees who handle privacy rights requests to ensure they follow the organization's policies and procedures.

Avoid Regulatory Action with these Steps

It's become clear that regulators are using businesses' privacy rights processes to test their effectiveness and send inquiries. To steer clear of violations, businesses need to ensure that:

- Cookie banners have symmetry of choice and *actually work to block cookies!*
- They're only collecting the minimum amount of information necessary for the request.
- Verification is not required for opt-out requests.
- Universal opt-out signals are honored and authorized agents can make rights requests on behalf of consumers.

13 Establish and Maintain a Cookie Opt-Out Mechanism



As more privacy laws go into effect, more consumers gain the rights to opt out of the sale of their personal information, targeted advertising or sharing of their personal information for targeted advertising, and certain profiling. Many states also mandate the recognition of a universal opt-out mechanism (UOOM), also called Global Privacy Control (GPC).

TEST YOUR OPT-OUT BANNERS!

Regulators are focused on consumer rights mechanisms, and they are checking to make sure they work. So should you!

TO DO

- ✓ Implement or review your existing cookie banner(s) and confirm that it provides accurate notice and appropriate choices, whether opt-in or opt-out.
- ✓ Review cookie consent/opt-out interfaces for dark patterns.
- ✓ Ensure that the cookies listed in your preference center are accurate to the cookies on the site.
- ✓ Work with your web team to honor universal opt-out mechanisms.
- ✓ Ensure your website's homepage includes an opt-out link with appropriate opt-out language and icon, where applicable, or state in your privacy notice that you don't sell or share personal information.
- ✓ Establish a cookie governance program that includes regular audits, review process for new tracking tech, and testing of opt-out mechanisms.

Universal Opt-Out Mechanism (UOOM)

Most state privacy laws require businesses to honor UOOMs, and California recently passed the OOPS Law, which provides a one-stop shop for consumers to opt out across websites.

What do you need to do?

- **Turn on UOOM settings to recognize browser signals**
- **Regularly test the functionality to ensure it's working**

14 Provide Privacy Training and Awareness

Under CCPA and other privacy laws, covered entities must provide appropriate privacy training to employees. Regardless of whether training is a regulatory requirement, a successful privacy program depends on employees understanding their organization's privacy obligations and their own responsibility to uphold those obligations.

TO DO

- ✓ Identify or create privacy training that integrates well with your existing employee training program.
- ✓ Work with HR to incorporate privacy training into regular training cadence, employee handbook, company intranet, and any other format where employees get information.
- ✓ Ensure training includes information on data security, privacy rights (for employees who may handle requests), understanding dark patterns (for employees who design user interfaces), privacy awareness, and privacy regulations.
- ✓ Track and monitor training attendance.

CA Training Requirements

- Covered businesses must train individuals responsible for handling privacy requests on privacy rights and directing consumers on how to exercise those rights.
- Covered businesses must implement a training policy if they know, or reasonably should know, that they buy, receive for commercial purposes, sell, or share for commercial purposes the personal data of 10 million or more consumers in a calendar year.

BEST PRACTICES FOR TRAINING AND AWARENESS

- Ensure privacy training is tailored to an employee's role in the organization and how they interact with personal information.
- Training should be regular and consistent, not just an annual box-checking activity.
- Create regular awareness materials and communicate them in ways consistent with other organizational communications.
- Document and track training so you can measure its effectiveness.

15 Validate Data Security for Personal Information

To maintain privacy, organizations must have appropriate physical, technical, and administrative security protections in place. Security for privacy entails ensuring that personal information is protected according to the risk it represents to individuals and the organization.

TO DO

- ✓ Review your data classification policy and practices to ensure individual data elements are appropriately classified—pay special attention to data considered sensitive personal information by various laws.
- ✓ Work with the security team to audit the protections around each class of personal information to ensure appropriate protections are in place.
- ✓ Create or review your security auditing and testing program to ensure proactive monitoring and red-flags systems are in place and functioning.
- ✓ Create an incident response team and ensure the team regularly conducts round-table training exercises and response scenarios at least annually.
- ✓ Work with the security team to review and revise policies that bridge teams, e.g., data retention and destruction policies, data transfer policies, incident response plans, vendor management policies.

PRIVACY AND SECURITY: TEAM UP FOR SUCCESS

Privacy and security teams have different mandates but align on many of their goals and have significant overlap when it comes to operations. When these teams work together, they are more efficient and effective. Work with your security team to:

- Create holistic data inventories
- Classify data by privacy and security risk
- Identify and collaborate on common metrics
- De-identify and anonymize PI
- Conduct internal risk assessments
- Vet third parties prior to engagement
- Train employees on data protection

16 Establish a Sustainable Program

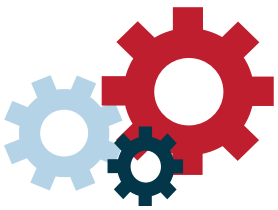
Creating a privacy program that your organization can sustain is essential for long-term compliance and maintaining consumer trust. This requires a strategic approach that accounts for both the obligations and the constraints your organization faces. You will need robust privacy governance that can adapt to changes in the business and the privacy landscape, documented privacy policies and procedures that are integrated into workflows, support from leadership, and a well-trained staff.

TO DO

- ✓ Appoint a dedicated internal resource to be responsible for privacy.
- ✓ Identify external resources to partner with (e.g., attorneys, consultants, software vendors).
- ✓ Maintain a data inventory to understand what personal information you collect and retain, where you store it, and with whom you share it.
- ✓ Embed privacy controls throughout the personal information lifecycle.
- ✓ Align privacy with your organizational goals, strategy, and risk profile.
- ✓ Implement a risk-based approach, focusing on high-risk critical business processes and systems first.
- ✓ Align your program with fundamental principles and incorporate privacy by design.
- ✓ Stay up to date on current events in privacy, especially new and updated privacy laws.
- ✓ Establish a privacy program maintenance plan, including regular updating policies, standards, procedures, and data inventories; testing privacy rights mechanisms; conducting cookie audits and privacy impact assessments; and reviewing vendor contracts.

REMEMBER:

A sustainable program will look different from one organization to the next. It's important to weigh resources and business priorities against privacy risks and obligations when determining the composition of your program. Do you want in-house staffing or contracted consulting? Do automated tools or manual processes make more sense?



Red Clover Advisors

2026 TO-DO LIST

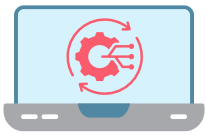
Wondering How to Get it All Done?

Implementing this checklist is a great way to kick off a privacy program that will get you compliant and build trust with consumers. Need more guidance? We're ready to assist.

Red Clover Advisors is Your Full-Service Privacy Provider

DESIGN

Strategic guidance aligning privacy with business objectives and risk profiles to create an adaptable privacy program that scales as regulations and priorities change.



IMPLEMENT

Hands-on execution of privacy program components through policy creation, process design, and technology setup/automation to operationalize compliance.

SUSTAIN

Front-line support maintaining privacy compliance through continuous monitoring and adaptation as laws, technology, and business needs evolve.

FPO

Privacy experts delivering tailored support from monthly briefings to full program design, ongoing privacy compliance, and daily ownership of privacy requirements such as cookie consent, privacy notices, privacy rights requests, and more.

STILL WONDERING HOW YOU CAN GET IT ALL DONE?

Our team of privacy experts can help you navigate through best practices, strategies, and tactics.

Contact us for a consultation.