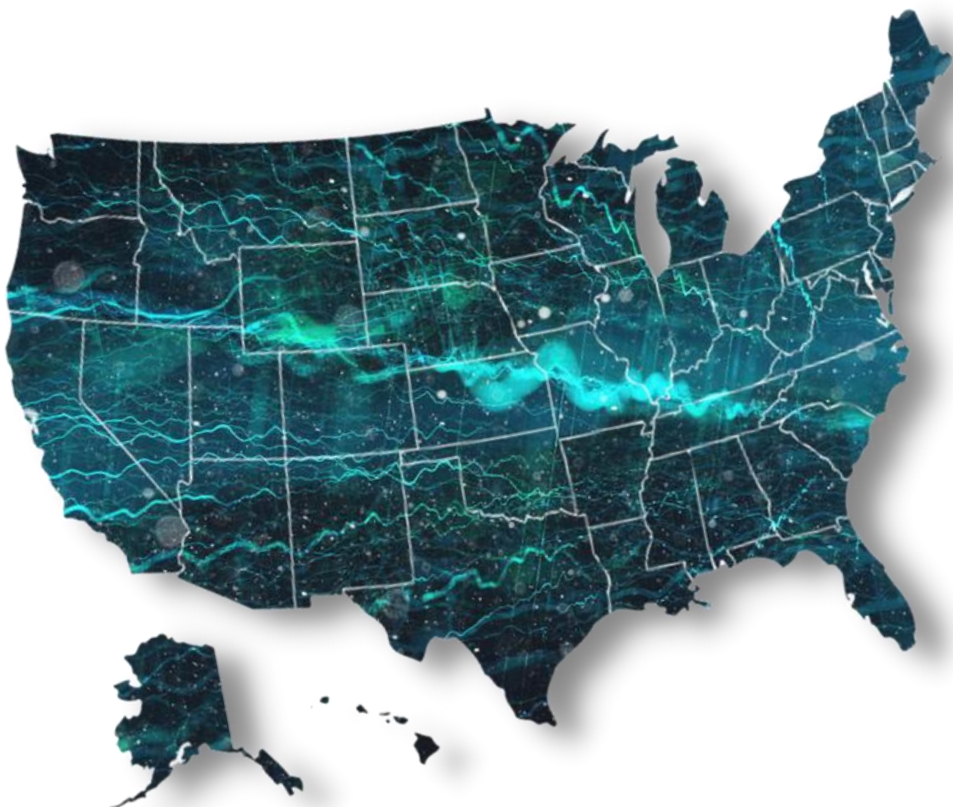


2024 PRIVACY PROGRAM

TO-DO LIST

US State Law Guidance



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

✉ info@redcloveradvisors.com

🌐 www.redcloveradvisors.com

DISCLAIMER: The materials available in this document are for informational purposes only and not for the purpose of providing legal advice. Red Clover Advisors, LLC is not a law firm, and if you need legal advice, please contact a competent attorney to provide appropriate legal advice with respect to your specific concern.



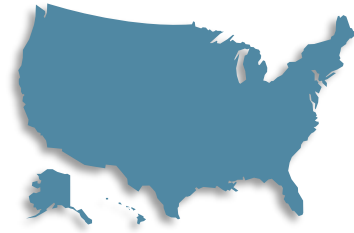
Red Clover Advisors 2024 Privacy To-Do List

In the U.S., privacy law continues to be a complex patchwork of national, state, and local laws and regulations with **five laws taking effect in 2024** (WA, OR, CT Amendment, TX, and MT) and five more going into effect in January 2025 (IA, NH, NJ, NE and DE). Maryland will follow in October 2025, followed by Kentucky and Indiana on January 1, 2026. Included in this group is Washington's MHMDA, which is a health data-specific privacy law.

The **new U.S. data privacy laws** contain several requirements that differ from those of the California Consumer Privacy Act of 2018, as amended by CPRA (**CCPA**). The broad concepts in each of these laws are similar and reflect those previously passed, however, there are some notable distinctions.

ACTION: Organizations **should make efforts to update existing compliance initiatives or establish new ones** to ensure compliance in advance of the effective dates.

Note: As this list does not comprehensively cover children's privacy or some of the amendments to data privacy law's covering health-data. However, some details are addressed here. Stay tuned to Red Clover channels for additional materials on these topics!



US State Privacy Laws Signed As of May 1, 2024

- Washington My Health My Data Act (**WA MHMDA**) (effective 03/31/24*)
- Oregon Consumer Privacy Act (**OCPA**) (effective 07/01/24**)
- Texas Data Privacy and Security Act (**TDPSA**) (effective 07/01/24)
- Montana Consumer Data Privacy Act (**MCDPA**) effective 10/01/24)
- Connecticut (**CTDPA**) Amendment: Concerning Online Privacy, Data and Safety Protections (10/01/24)
- Iowa Consumer Data Protection Act (**ICDPA**) (effective 01/01/2025)
- Delaware Personal Data Privacy Act (**DPDPA**) (effective 01/01/25)
- New Hampshire (**NH**) (effective 01/01/2025)
- New Jersey (**NJ**) (effective 01/15/2025)
- Nebraska (**NDPA**) (effective 01/01/2025)
- Maryland (**MODPA**) (effective 10/01/2025)
- Indiana (**INCDPA**) (effective 01/01/2026)
- Kentucky (**KCDPA**) (effective 01/01/2026)

***WA small businesses have until June 30th, 2024**

**** OR non-profit organizations have until July 1, 2025**

Throughout this document, all references to CCPA mean **CCPA, as amended by CPRA**.

A Year of Continued Privacy Change

2023 kept us on our toes in the world of privacy and data protection, and the start of 2024 has shown it will not be any different. The evolving regulatory landscape has transformed privacy from a simple “check-the-box” compliance task into a full-scale operational concern.

Demonstrating your organization’s commitment to data privacy can be a competitive advantage that creates transparency, trust and brand equity.

Highlights of Notable Events:

Enforcement Outlook



In 2024, the CA Attorney General (AG) settled the second major enforcement under the CCPA with DoorDash, emphasizing the need for transparent privacy notices. A major takeaway is that accurate data mapping is a key practical compliance need.

Additionally, the CPPA, California’s new privacy regulatory agency, is enhancing its capabilities by hiring auditors and investigators, as stated by Executive Director Ashkan Soltani at the annual IAPP Global Privacy Summit 2024. This expansion indicates a shift towards more proactive privacy enforcement. Further collaboration between the CPPA, the California AG, and other state AGs is expected to uncover non-compliant behavior.

In February, the Connecticut Attorney General [released a report](#) detailing that it has issued over a dozen violation notices to companies, some unresolved. The AG indicated its current and future enforcement priorities, with a focus on privacy notices (improper disclosures and rights management), the handling of sensitive personal and teens' data, and the behavior of data brokers. Expect these areas to be common targets of regulatory activity.

CPPA Issues First-Ever Enforcement Advisory

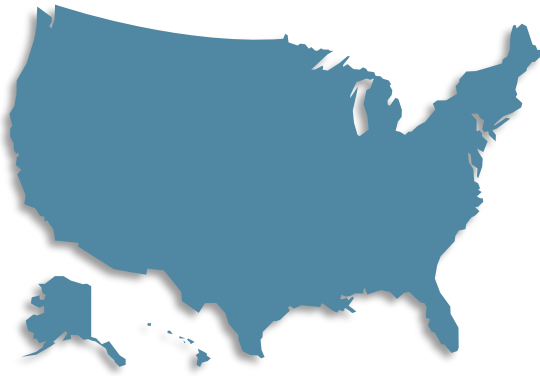


The CPPA issued its first ever enforcement advisory on data minimization in privacy rights response. This advisory, while not officially interpreting the CCPA, serves as a reminder to organizations to adhere to the CCPA’s core principle of data minimization. The advisory specifically reminds organizations to avoid requesting “excessive and unnecessary personal information in response to [privacy rights] requests.”

New Laws Continue to Pass Around the Country



Lawmakers around the country continue to pass comprehensive consumer privacy laws. At the time of writing (early May) Nebraska, Kentucky, and Maryland have been signed or are awaiting the governor’s signature. Expect more laws to pass as the year goes on.



2024 Privacy To-Do List: Unique New Elements

Scope

The scope of these new laws largely mirrors existing state consumer privacy laws. All state consumer privacy laws are extraterritorial, covering the personal information of residents of the respective state. While all target businesses, some include non-profits as well. The exemptions related to HIPAA, GLBA and other federal statutes are similar, though some exempt an entity and others the covered data. And the material scope of each law is personal information, broadly defined as information relating to an identified or identifiable individual — though nuances differ in this definition from one law to another.

Example of Distinctions in New Laws

OREGON: The OCPA grants consumers the right to request a list of **specific third parties** to which the controller has disclosed either the consumer’s personal data or any personal data. This practical provision will require businesses to keep accurate and up-to-date **personal data inventory maps**.

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.

MARYLAND: Instead of requiring consent to process Sensitive PI, Maryland bans its collection, processing, or sharing of unless it is “strictly necessary to provide or maintain a specific product or service requested by the consumer.” So instead of seeking consent, the idea is to instead limit the opportunities where sensitive PI can be used at all.





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.



2 Establish and Maintain a Data Inventory

Mapping how personal information flows through your organization— from collection to deletion or de-identification — supports business intelligence, risk management, and compliance with privacy laws. This is critically important as laws such as Oregon rest on the assumption that businesses know to whom and where their data goes.

TO DO

- ✓ Establish a detailed personal information inventory that catalogs what data your organization collects, the business purposes for collection, where it is stored, to whom it is shared, and associated security measures.
- ✓ Maintain the inventory with regular audits and updates to ensure it reflects your organization's current practices. Consider how your organization's business practices may have changed, including new systems, technologies, use cases, and types of personal information collected.





Tip: A robust and honest Privacy Notice is your shield and armor; it is what consumers see and think about your data privacy practices.

3 Identify and Manage Sensitive Personal Information

Data privacy laws treat Sensitive Personal Information (SPI) differently than other personal information, requiring **disclosure of its collection, limiting its use, providing opt-in or opt-out rights to consumers, and requiring risk assessments**. SPI is defined differently depending on the law, so organizations need to know what constitutes SPI in their jurisdictions and be able to identify it in their systems.

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 use and disclosure of SPI.
- ✓ Update consent and opt-out processes to obtain and track consumers' choices about their SPI in alignment with applicable privacy laws.
 - ❖ Note: States have different rules for processing SPI--some require consent and others provide opt-out rights.
- ✓ Review your organization's Privacy Notice to ensure it adequately discloses your practices regarding SPI.
- ✓ Understand where SPI resides and ensure appropriate security measures are in place related to the sensitivity of the data.



Common SPI Data Elements*

- Race/Ethnicity
- Religion
- Sex life or sexual orientation
- Citizenship
- Immigration status
- Health records
- Biometric information
- Genetic information
- Precise location

Less Common Elements of SPI

- Philosophical Beliefs (CA)
- National Origin (MD & OR)
- Status as transgender or nonbinary (OR, NJ, DE, and MD)
- Status as a victim of a crime (OR & CT)
- Expanded definition of biometric information (NJ)
- Financial information (NJ)
- Consumer Health Data (MD & CT)

*This list may not be comprehensive and is subject to change as privacy laws evolve.

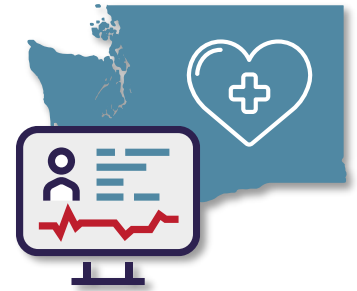
2024 TO-DO LIST

3

Identify and manage Sensitive Personal Data (cont'd)

Washington's "Consumer Health Data"

Washington MHMDA is a health data-focused privacy law covering "Consumer Health Data" (CHD) instead of personal information.



What is CHD?

- ✓ As defined, CHD is personal data 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):
 - ✓ Individual health conditions, treatment, diseases, or diagnoses;
 - ✓ Gender Affirming Care;
 - ✓ Bodily functions, vital signs, symptoms, or measurements of anything in this list
 - ✓ Social, psychological, behavioral, and medical interventions;
 - ✓ Health-related surgeries or procedures;
 - ✓ Use or purchase of prescribed medication;
 - ✓ Reproductive Health Info;
 - ✓ Biometric and Genetic data;
 - ✓ Data that identifies a consumer seeking **health care services**;
 - ✓ Location information that could reasonably indicate a consumer's attempt to acquire or receive **health services or supplies**.
- ✓ **"Health Care Services" is defined as "any service provided to a person to assess, measure, improve, or learn about a person's mental or physical health"**
 - ✓ As the law provides restrictions on the use of CHD, this broad definition means that there are restrictions on having any tracking pixels on websites that could be classified as Health Care Services.
- ✓ **Geofencing Ban:**
 - ✓ There is a restriction on implementing a geofence "around an entity that provides in-person health care services where such geofence is used to" track a person, collect health data from said consumer, or send notifications/messages/advertisements related to their health data or health care services.
 - ✓ This may inhibit geo-targeted advertisements in places involving health data.



Tip: CHD is a broad category that consumers and regulators are extremely weary of misuse. Be sure to consider all the possible ways your organization uses CHD.



4

Conduct Privacy Impact Assessments

Many U.S. state privacy laws require privacy impact assessments (PIAs), also called data protection assessments (DPAs), for processing that represents a “heightened risk of harm” to consumers, often including sale and sharing of personal information for targeted advertising, certain types of profiling, and processing sensitive personal information.



TO DO

- ✓ Identify the processing your organization conducts that requires a PIA based on your jurisdictions.
- ✓ Develop a governance plan for your PIA program, including record-keeping and regular updates.
- ✓ Create a standard PIA template and instructions for use as this will be used throughout the organization.
- ✓ Communicate your PIA obligations to all business units that interact with personal information and provide training on the process.
- ❖ *Note: The EU General Data Protection Act and other data protection laws outside the U.S. have similar obligations to conduct data protection impact assessments (DPIAs). DPIAs must include specific elements as outlined in those laws.*

“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; or
 - Other substantial injury to consumers
- Selling Personal Information
- Processing Sensitive Personal Information

*This list is not comprehensive and is subject to change as privacy laws evolve.





2024 TO-DO LIST

5

Highlights of US State PIA Requirements

CCPA

- **Perform and submit risk assessments to the California Privacy Protection Agency (CPPA)** where processing activities present a **significant risk to consumers' privacy or security**.
- **Note that Regulations clarifying the requirements of risk assessments are forthcoming from the CPPA.** However, we believe that the risk assessment rules will seek to have organizations weigh the benefits resulting from the processing to the business, the consumer, other stakeholders, and the public, against the potential risks to the rights of the consumer.

Utah, Washington, and Iowa

- **Utah, Washington's MHMDA, and Iowa do not require PIAs/DPIAs**

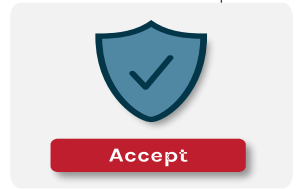
CO, CT, DE, IN, KY, MD, MT, NE, NH, NH, OR, TN, TX, and VA

- Some variation of: Data protection assessments are required when **conducting processing activities that present a heightened risk of harm**. Controllers might be required to make PIAs/DPIAs available to the Attorney General.
- **"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 Data.
 - Processing Sensitive Personal Data.
- **Delaware only requires PIAs/DPIAs for controllers who control/process data of not less than 100,000 Delaware consumers.**



6 Review and Revise Consent Processes

U.S. state laws are increasing consent requirements around specific types of processing.



Processing type	Consent required
Sensitive personal information	CO, CT, DE, IN, IO, KY, MT, NE, NH, NJ, OR, TN, TX, VA
Secondary use	CO, CT, DE, IN, IO, KY, MD, MT, NE, NH, NJ, OR, TN, TX, VA
Children (U13) – parental consent	All States (COPPA)
Minors (13-15) for sale or targeted ads	OR (incl. profiling*), MT, NH, CT
Minors (13-16) for sale/share, targeted ads, profiling*	CA (S/S only), NJ
Minors (13-17) for sale or targeted ads	DE

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 Data that will be processed to achieve the purpose(s)
- ✓ If you sell Sensitive Personal Data, 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

TO DO

- ✓ Refresh previously granted consent, if needed, to meet the requirements of the new laws.
- ✓ Establish a process to get new consent from any consumer who hasn't interacted with you in the past 24 months.
- ✓ Review consent processes to confirm that consent:
 - is obtained through a consumer's clear, affirmative action,
 - is freely given,
 - is specific,
 - is informed, and
 - reflects the consumer's unambiguous agreement.



WA MHMDA

Required: Consent for any use of CHD other than to provide requested services to the individual.

*Limited to profiling that furthers legal or similarly significant effects.

7 Handling the PI of Minors

TO DO:

- ✓ Identify where Personal Information and Sensitive Personal Information about minors is collected, shared or sold.
- ✓ Obtain appropriate consent prior to the collection, sharing, or selling of Personal Information about minors.
- ✓ Appropriate consent for someone under 13 is parental consent.
- ✓ Ensure Privacy Notice to minors is age-appropriate and easily understood.
- ✓ Confirm strong security measures are in place for Sensitive Personal Information about minors.
- ✓ As a rule, complying with the verifiable parental consent requirements of the Children's Online Privacy Protection Act (COPPA) is generally deemed compliant with the consent requirement for children.



TIP: **CHILD v. MINOR**

- A Child is federally defined under COPPA as a person under age 13.
- Minors (13-18) may have different rules than adults (18+) under state data privacy laws.

A Note on the CT Amendment

- CT Requires:
 - Consent for collecting precise geolocation from a minor.
 - Parental consent for social media accounts of minors under 16.
 - Obligation to include a conspicuous signal to a minor when tracking their online activity (e.g., a website log installed by parents).
 - And more!

2024 TO-DO LIST

8

Profiling, Selling or Sharing Personal Information and Targeted Advertising

Certain jurisdictions require organizations to provide individuals the right to opt-out of the sale of personal information, targeted advertising and certain sharing and profiling.

TO DO

- ✓ Identify if your organization sells Personal Data to third parties or processes Personal Data for targeted advertising.
- ✓ Implement mechanisms to allow individuals to opt-out of the sale or sharing of Personal Data for targeted advertising.
- ✓ Ensure consumers are able to make this choice in a clear and comprehensible manner.
- ✓ Avoid discriminating against consumer's for utilizing their opt-out rights.
- ✓ See Step 14 for more details



TIP: Dealing with Differences

States are inconsistent on requiring opt-out for sale, profiling, and targeted advertising. Determine the importance of each for your business and decide if you want to grant the same opt-out rights to all or break it up by state.

Comparison of U.S. Data Privacy Law Requirements

CCPA	Other Laws
<ul style="list-style-type: none"> • Provide individuals the option to opt-out of the sale or sharing of Personal Data for targeted advertising. • There must be a "Do Not Sell or Share My Personal Information" link (or icon) on the organization's website (or state in your Privacy Notice that Personal Data is not being sold). • Must recognize a universal opt-out mechanism such as the GPC 	<ul style="list-style-type: none"> • Like the laws that came into effect in 2023, the new laws require a Controller to disclose if they sell Personal Data to third parties or processes Personal Data for targeted advertising and provide individuals the option to opt-out. • Enable consumers to opt-out, including via a universal opt-out mechanism such as the GPC (CO, CT, DE, MD, MT, NE, NH, NJ, OR, and TX).



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

9 Update Privacy Notices

The **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.
- ✓ Update external Privacy Notices to comply with applicable data privacy laws.
- ✓ Satisfy Texas's unique rules: the Privacy Notice must include the following when sensitive or biometric data is collected, respectively:
 - ✓ "NOTICE: We may sell your sensitive personal data."
 - ✓ "NOTICE: We may sell your biometric personal data."
- ✓ Enhance and optimize Privacy Notices and Terms of Use to provide clarity to your customers.
 - ✓ Oregon, like Colorado, has some specific requirements including specifying the "express purpose" for the collection and processing, be given. This likely requires more specificity than other states ask.



WA MHMDA

Required: separate notice dedicated to CHD and a separate link to said notice.

As more laws enter into force, consider splitting your privacy notice requirements into three parts: **GDPR**, **CCPA**, and the other Comprehensive **US State Laws**. To date, the US Laws, outside of CA, are broadly similar. This allows for easier updates and is more approachable to consumers. Be sure to note differences between laws where needed, or simply choose to apply the most stringent regulatory requirements to all users.

2024 TO-DO LIST

10

Eliminate Dark Patterns

Dark Patterns are defined as a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making, or choice.

Common Dark Patterns often confuse users through visual tactics such as differing font sizes (making "opt-out" smaller than "opt-in"), color schemes, and asymmetrical option layouts, where privacy-preserving choices are harder to access than less private alternatives. Additionally, deceptive wording can mislead users regarding their choices.



Many laws, including most new U.S. state privacy laws, treat **consent** that has been obtained via a **Dark Pattern as invalid.**

Experience shows that customers recognize Dark Patterns as trickery and consistently respond negatively to them, harming customer retention and trust in your organization.

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.

TO DO

- ✓ Review and test your user interfaces to identify and **eliminate any Dark Patterns.**
- ✓ Consider engaging an independent party to conducting user testing to identify any potential Dark Patterns, particularly in any consent processes.
- ✓ Include individuals representing different populations (age, gender, race, education, etc.) 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 & Inclusion efforts.
- ✓ Create and deliver training on Dark Patterns for teams that develop web interfaces and consent processes.



2024 TO-DO LIST

11

Create or Revise Data Minimization, Retention and Deletion Policies

Ensure your organization complies with data minimization and retention requirements.

TO DO

- ✓ Implement procedures to limit the collection, use, retention, and sharing of Personal Information to that which is "reasonably necessary" to achieve the specified purposes of processing.
- ✓ Part of this is practicing de-identification and anonymization where relevant:
 - ✓ Most states exclude de-identified data — data not linkable to identifiable individuals or their devices.
 - ✓ Many states exempt most or all privacy rights requests from applying to pseudonymous data.



REMEMBER:
Put the customer first when creating user experiences!



12

Keep a Current Data Inventory

Data inventories are an important foundation for a successful 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.

TO DO

- ✓ Assess or update your data inventory to capture all your organizations current data collection and processing practices.
- ✓ Set a schedule to regularly update and review your data inventory.
- ✓ Prior to engaging in any new projects, review your data inventory and mock how this data will interface and affect your existing data.

Oregon: Right to Access Rule

OR provides consumers a right to know the specific third parties that the controller disclosed either (controller's option): (a) the consumer's personal information or (b) any personal information. This makes an up-to-date data inventory essential!



2024 TO-DO LIST

13

Review and Update Contracts with Third Parties

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



TO DO

- ✓ Create or update your third-party inventory, including categorization by relationship type.
- ✓ Review vendor contracts to ensure they include appropriate privacy and data protection language.
 - ✓ Specific obligations differ somewhat based on jurisdiction; in general contracts must require that vendors assist controllers in responding to privacy rights requests and to correct or delete personal information upon request from the controller.
 - ✓ Many privacy laws also require that contracts include obligations for vendors to cooperate with compliance audits conducted by or on behalf of controllers.
- ✓ Regularly conduct privacy and security assessments to confirm third parties are compliant with applicable data privacy laws.
- ✓ Implement procedures to identify, manage, and mitigate information security and privacy risks.

U.S. Data Privacy Law Requirements

Obligations in U.S. state consumer privacy laws require that businesses know to whom they disclose personal information (with varying levels of specificity), for what purpose and in what manner (sell, share for targeted ads, share with a processor).

Contracts determine the type of relationship, so when writing or reviewing contracts ensure your contracts with vendors (processors, service providers) include the processing limitations required by applicable jurisdictions.

Oregon's new law underscores the need for this with its obligation to provide consumers with the specific entities to which a business has shared personal information.

2024 TO-DO LIST

14 Manage Privacy Rights Requests

Organizations must provide certain privacy rights to individuals, like access, deletion, correction, and opt-out rights and disclose those rights in their Privacy Notice.



TO DO

- ✓ Implement or test methods for individuals to submit privacy rights requests.
- ✓ Ensure you have privacy rights submission methods anywhere you collect personal information (e.g., websites, apps, brick and mortar locations).
- ✓ Create or update internal procedures to respond to privacy rights requests (including from employees where applicable).
 - ✓ Ensure your process is flexible and can handle the addition of new vendors – especially where they 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) and/or rights responses information on how individuals can file a complaint with a regulator.
- ✓ Record, track, and maintain records of privacy rights requests.
- ✓ Train all employees who handle Individual Rights Requests on the organization's policies and procedures.

Privacy Rights – Distinctions in Newer Laws

- **Delaware, New Hampshire, Kentucky, Nebraska, Indiana, New Jersey, Maryland and Oregon allow the deletion of any personal information the controller has about the consumer**, as opposed to only information collected directly from the consumer.
- **Oregon** uniquely offers consumers a right to know the specific third parties that the controller disclosed either: (a) the consumer's personal data or (b) any personal data; The choice is up to the controller's discretion.

2024 TO-DO LIST

15


Establish and Maintain a Cookie Opt-Out Mechanism

As new state privacy laws are passed, more consumers gain the rights to opt-out of sale of their personal information, targeted advertising or sharing of their personal information for targeted advertising, and certain profiling. CA, CO, CT, DE, MD, MT, NH, NJ, OR, and TX also mandate the recognition of a universal opt-out mechanism (UOOM), also called a Global Privacy Control (GPC).

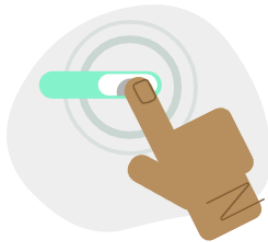


REMEMBER:
Not all sale and sharing of personal information occurs via cookies! Make sure your opt-out program includes all forms of sale and sharing.

TO DO

- ✓ Implement or review your existing cookie banner on website(s) and confirm that it provides appropriate notice and enables users to effect choice, whether opt-in or opt-out.
- ✓ Ensure that the cookies listed in your preference center are accurate to the cookies on the site.
- ✓ Prepare for acceptance of universal opt-out mechanisms.
- ✓ Include a “Do Not Sell or Share My Personal Information” link or this  privacy icon (available from the CA AG’s website) on your website’s homepage. Alternatively, state in your Privacy Notice that you don’t sell personal information.
- ✓ Train your team on the latest in cookie consent and management practices.

GPC Basics



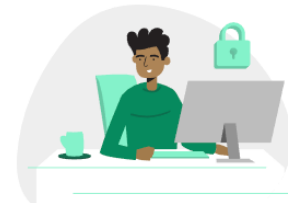
Turn On GPC

Enable Global Privacy Control to communicate your privacy preferences.



Let Businesses Know

Your browser will then send the GPC signal to websites you visit, indicating your privacy choices.



Exercise Your Rights

Participating websites that adopt this mechanism can then respect your privacy rights accordingly.



2024 TO-DO LIST

16 Privacy Training and Awareness

Under CCPA, organizations have an obligation to provide appropriate privacy training to employees that handle privacy inquiries. Even when not required elsewhere, organizations should ensure that employees understand their organization's privacy obligations and their responsibilities, especially as related to privacy rights.



CCPA

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.

- Requires that covered businesses train the individuals responsible for compliance and/or handling privacy requests. These employees should be aware of applicable CCPA regulations and be able to direct consumers on how to use their statutory rights.
- Requires organizations to 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.

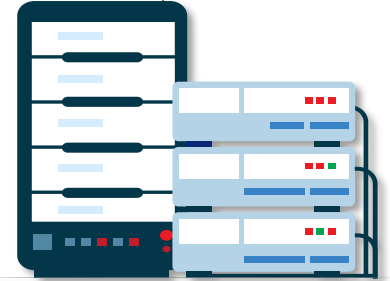
BEST PRACTICES FOR TRAINING AND AWARENESS

- 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.

17

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, vendor management policies.

CCPA v. Everyone Else: Security Practices

CCPA

- If your organization's processing of Personal Data is a significant risk to consumers' privacy or security, it must perform an annual cybersecurity audit. (Regulations forthcoming).

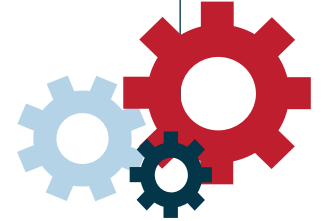
Other State Laws

- Continually assess and implement reasonable administrative, technical, and physical data security practices and procedures to protect Personal Data.
- Perform regular cybersecurity audits for processing that presents a significant risk to consumer privacy or security.



Sustainable Compliance

Organizations must undertake robust privacy governance programs to maintain compliance with existing and prepare for changes to the legislative landscape to come. Documented, repeatable privacy policies will create a durable and sustainable privacy program to withstand internal changes to business practices as well as changes in legal obligations and consumer expectations.



TO DO

- ✓ Embed privacy controls throughout the personal information lifecycle.
- ✓ Align privacy with your organizational goals, strategy and risk profile.
- ✓ Establish and maintain a privacy program that aligns with fundamental principles and incorporates privacy by design.
- ✓ Implement a risk-based approach, focusing on the high-risk critical business processes and systems first.
- ✓ Appoint a dedicated resource (internal or external) to be responsible for privacy.
- ✓ Stay up to date on current events in privacy, especially new and updated privacy laws.
- ✓ Establish a privacy program maintenance plan including regular updates to policies, standards, procedures and reviewing data inventories, privacy rights strategy, cookie audits, privacy impact assessments, and all vendor contracts.

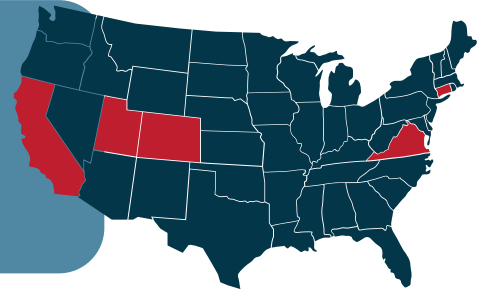


2024 TO-DO LIST

Looking Ahead

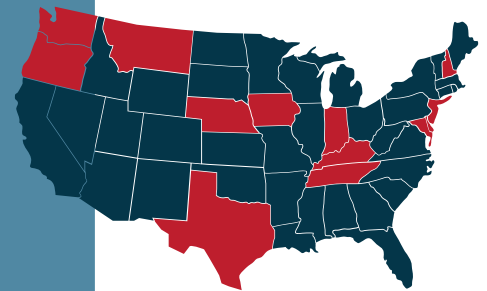
The regulatory landscape is not one to ignore and will continue to drive privacy strategy programs. In 2023 five state consumer privacy laws came into effect.

- California (CCPA) as of January 1, 2023
- Virginia (VCDPA) as of January 1, 2023
- Colorado (CPA) as of July 1, 2023
- Connecticut (CTDPA) as of July 1, 2023
- Utah (UCPA) as of December 31, 2023



Thus far, many additional states (plus amendments to the CTDPA) have laws coming into effect in 2024, 2025, and 2026.

- Washington (WA MHMDA) as of March 31, 2024
- Oregon (OCPA) as of July 1, 2024
- Texas (TDPSA) as of July 1, 2024
- Montana (MCDPA) as of October 1, 2024
- Iowa (ICDPA) as of January 1, 2025
- Delaware (DPDPA) as of January 1, 2025
- New Hampshire as of January 1, 2025
- New Jersey as of January 15, 2025
- Tennessee (TIPA) as of July 1, 2025
- Maryland (MODPA) as of October 1, 2025
- Indiana (INCDPA) as of January 1, 2026
- Kentucky (KCDPA) as of January 1, 2026



U.S. state and federal data privacy regulations will expand in the coming years.

To get ahead of these existing and emerging data privacy laws, prioritize your compliance program with an aim to completing these critical privacy steps before the end of the year.

WONDERING HOW YOU CAN GET IT ALL DONE?

WE CAN HELP

Our team of privacy experts can help navigate you through best practices, strategies and tactics. Contact us for a consultation.

www.redcloveradvisors.com