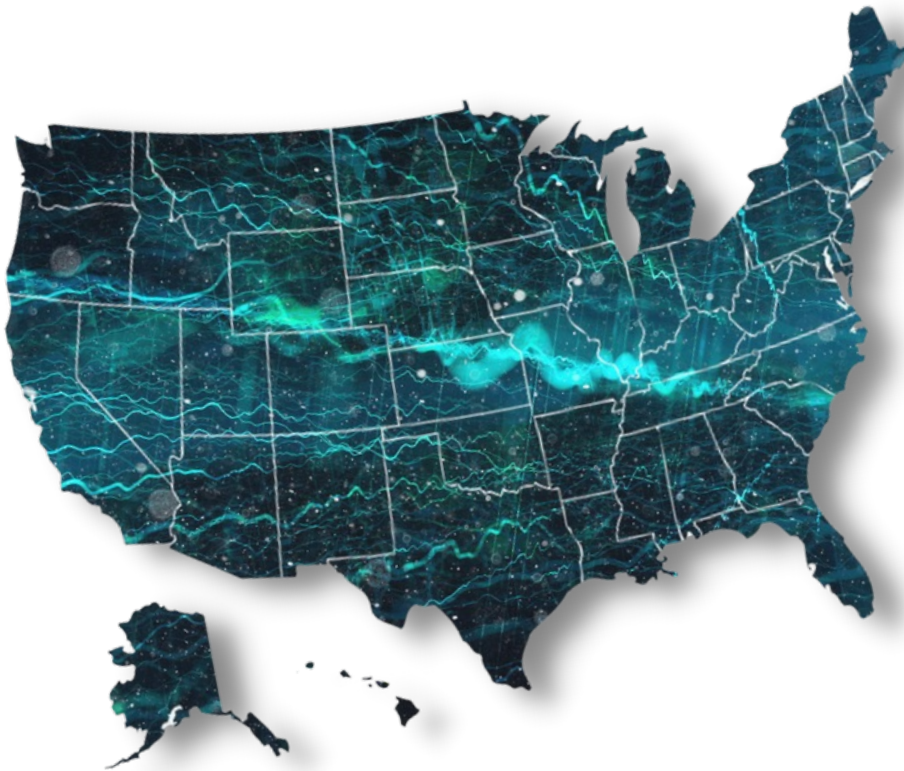




# 2024 PRIVACY PROGRAM

## 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](mailto:info@redcloveradvisors.com)

🌐 [www.redcloveradvisors.com](http://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.



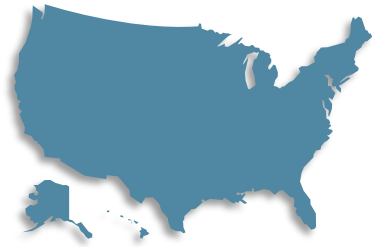
# 2024 Privacy To-Do List

In the U.S., privacy law continues to be a complex patchwork of national, state, and local privacy laws and regulations with **five new laws taking effect in 2024** (WA, OR, CT Amendment, TX, and MT), as well as two going into effect Jan 1, 2025 (IA and DE). Included in this is Washington’s MHMDA, which is a health data specific privacy law. As this list does not comprehensively cover children and health data laws, neither WA nor CT will be covered in depth. Stay tuned to Red Clover channels for additional materials on those topics!

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**”). While they all largely reflect the other US state privacy laws, they do have some notable distinctions.

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

The **2024 Privacy To-Do List** will assist your organization comply with data privacy obligations **with obtainable objectives for 2024 & beyond**.



## U.S. State Privacy Laws Coming into Effect in 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)

### ADDITIONAL

- Connecticut 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 01/01/24)

**\*WA Small businesses have until June 30<sup>th</sup>, 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 Change

2023 kept us on our toes in the world of data privacy and data protection, and it looks like 2024 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:



### Pixel Litigation Rises

Dozens of lawsuits have been filed over the use of pixel tracking tools on websites containing sensitive data. The suits allege that the use of these tools, largely provided by Meta and Google, improperly gathers sensitive data. These trackers have been found across the web, on pages with sensitive financial and health information, to more places like video players; every imaginable website may have a tracker.



### FTC Revs up Enforcements

In 2023 the FTC has aggressively sought to hold businesses accountable to their stated and required privacy practices. Major actions included those against BetterHelp, GoodRx, Epic Games, and many more. The FTC has made clear (1) that companies' privacy notices need to accurately reflect what happens on their sites and (2) that restrictions on the use of health data may not be skirted. This focus on accuracy and transparency will likely continue into 2024.



### Children’s Data Comes Under the Microscope

Regulators and lawmakers around the country have indicated their interest in a renewed push into regulating children’s data with the stated goal of ensuring privacy. These laws have been politically contentious, and are not uniform in their approaches. This will be something to watch in 2024.



### EU-U.S. Data Privacy Framework (EU-U.S. DPF),

**Becoming Effective July 10, 2023**, this agreement has enabled easier data transfers across the Atlantic from EU to US.



### AI Regulation Gains Steam

As AI continues to become more common place, global regulators have begun to take aim at reigning in excesses and harm. The European Union, usually a trendsetter for all things privacy, is quickly moving to become the first major market with comprehensive AI regulation, in the form of the “AI Act.” American regulators are also closely monitoring AI, with the FTC releasing warnings against misleading marketing as well as discussions on potential harms within their purview. This is an area that is sure to see growth in 2024.



# 2024 Privacy To-Do List: Scope

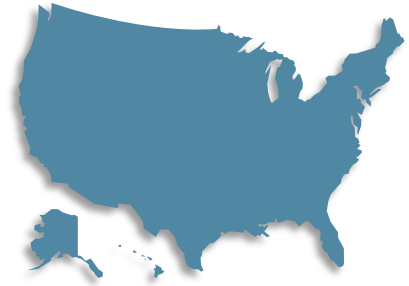
The scope of these new laws largely mirrors earlier laws. All target businesses, and most have similar exemptions. Almost all laws govern personal data as well as sensitive personal data.

## Some Unique Distinctions:

**Notably** WA provides very few exemptions, following CO by **denying non-profits an exemption**. WA is also unique, as a health law **it does not govern personal data but instead “Consumer Health Data” (CHD)**, discussed later. CHD is defined broadly, necessitating its inclusion with the other general data privacy laws covered here. WA’s law covers both residents **as well as anyone whose CHD is collected in WA**.

**TX is unique**, as instead of setting a threshold amount of data collected or revenue earned to be applicable, it **exempts Small Businesses as defined by the US Small Business Administration**.

**Delaware** has one of the lowest potential thresholds for applicability with one of its two potential criteria controlling or processing the personal data of a minimum of **10,000 DE consumers** while simultaneously deriving more than 20 percent of their gross revenue from the sale of personal data (in the prior year).



## U.S. State Privacy Laws Coming into Effect in 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)

## BONUS

- Connecticut 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 01/01/24)

**\*WA Small businesses have until June 30<sup>th</sup>, 2024**

**\*\* OR Non-profit organizations have until July 1, 2025**



**Tip:** A comprehensive privacy governance structure is the most effective defense 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 governance processes and activities 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 and update organization-wide privacy policies and standards to confirm 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

Data Mapping ensures the accuracy, completeness and timeliness of Personal Data inventories and supports actionable business intelligence for risk management and compliance activities.

### TO-DO

- ✓ Establish a detailed Personal Data inventory that catalogs what data your organization collects, the business purposes for using the data, where it is stored, to whom it is shared, and associated security measures.
- ✓ Maintain that inventory by updating it on a schedule to ensure your catalog reflects your organization's current data collection practices. Be sure to consider how your organization's data may have changed, such as a new business activity, a new system, or any other new data elements.



**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 Data and/or special categories of Personal Data (“Sensitive Personal Data”)

Organizations need to be able to identify Sensitive Personal Data, which is defined differently depending on the data privacy law. Data privacy laws treat Sensitive Personal Data differently, requiring **disclosure of its collection, limiting its use, providing consumers with the ability to opt-in or opt-out, and requiring risk assessments.**



#### TO-DO

- ✓ Understand the various data elements collected and identify which are considered sensitive under applicable laws. Establish procedures to limit your organization’s use and disclosure of Sensitive Personal Data.
- ✓ For all US states: update consent processes and obtain and track consent that meets new requirements for valid consent.
  - ✓ Iowa and Utah utilize an opt-out structure for processing Sensitive Personal Data and therefore do not require consent.
  - ✓ Note that WA has special consent requirements (see next page)
- ✓ Confirm your organization’s external Privacy Notice adequately discloses your practices regarding Sensitive Personal Data.
- ✓ Understand where Sensitive Personal Data resides, and ensure the protective controls applied to those systems are appropriate for the sensitivity of the data.
  - ✓ Remember California has a focus on opt-out rights for sensitive data, as well as limits on the secondary use of sensitive data.

**WA MHMDA focuses “Consumer Health Data” (CHD), not Sensitive Personal Data.**



#### Important New Elements of Sensitive Personal Data:

- National Origin (OR)
- Status as transgender or nonbinary (OR and DE)
- Status as a victim of a crime (OR and CT)
- Immigration Status (all new laws)
- “Sexuality” (TX) instead of “Sex Life”
- This is not a complete list as many additional elements exist and are covered in both new and existing Data Privacy Laws



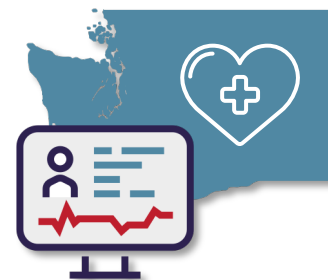


# Red Clover Advisors 2024 TO-DO LIST

3

## Identify and manage Sensitive Personal Data cont'd Washington "Consumer Health Data"

As stated previously, Washington MHMDA is a health data focused privacy law, covering "Consumer Health Data" (CHD).



### What is CHD?

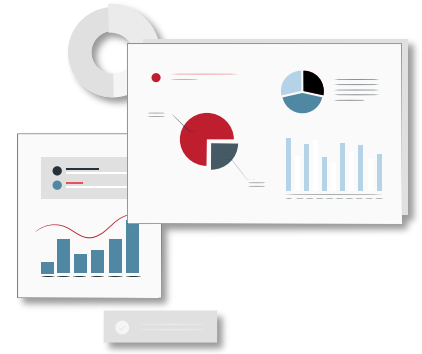
- ✓ As defined, CHD is personal data that is linked or reasonably linkable to a consumer and identifies a consumer's past, present, or future physical or mental health; Including (but not limited to):
  - ✓ Individual health conditions, treatment, diseases, or diagnoses;
  - ✓ Gender Affirming Care;
  - ✓ 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"**
  - ✓ This means there are restrictions on having any tracking pixels on websites that contain health data.
- ✓ **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 at places involving health data.



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

**4** **Conduct Privacy Impact Assessments (“PIA”s) or Data Protection Impact Assessments (“DPIA”s)**

Conduct PIAs or DPIAs any time your organization begins new projects, when a new project is likely to involve “high risk” of harm to individual data subjects, or when there are major changes to existing programs or activities where Personal Data is involved.



**7 TO-DOs**

- ✓ Determine what jurisdictions apply to your business
- ✓ Determine who needs to be involved in your PIA.
- ✓ Develop a governance plan for your PIA
- ✓ Create the necessary processes and policies to support PIAs
- ✓ Conduct a thorough data inventory
- ✓ Identify any potential risks associated with your processing activities
- ✓ Plan to review your PIA regularly moving forward





**4** Highlights of U.S. Data Privacy Law 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**.
- The risk assessment should 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. (Regulations forthcoming).

**Utah, Washington, and Iowa**

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

**Oregon, Texas, Montana, and Delaware**

- These laws closely mirror Virginia, Colorado, and Connecticut.
- 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.**

# Red Clover Advisors 2024 TO-DO LIST

## 5 Review and Revise Consent Processes

### TO-DO

- ✓ For compliance with **Oregon, Texas, Iowa, Montana, Delaware, and Connecticut's new amendment**, ensure that consent is obtained before:
  - 1) processing Sensitive Personal Data,
  - 2) processing Personal Data concerning a known child (under 13); or processing personal data about consumers for targeted advertising or sale in **Montana** for ages 13-16, in **Oregon** and **Connecticut** for ages 13-15, and ages 13-18 in **Delaware**.
    - In essence: cannot process personal data of a child under 13, and some states create restrictions on processing for ages past 13.
  - 3) if the consumer has previously opted-out (either directly or via a Universal Opt-Out Mechanism) of the selling of Personal Data, processing Personal Data for Targeted Advertising, or processing Personal Data for profiling, or
  - 4) processing Personal Data for any purposes that are not reasonably necessary to or compatible with originally specified processing purposes.
- ✓ Review consent processes to confirm that consent:
  - 1) is obtained through a consumer's clear, affirmative action,
  - 2) is freely given,
  - 3) is specific,
  - 4) is informed, and
  - 5) reflects the consumer's unambiguous agreement.
- ✓ 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.



Accept

### 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

### Washington Distinctions

- WA requires consent prior to collection or sharing when the data is to be used for purposes other than providing the consumer a requested service. Consent to share is distinct from the consent to collect, both must be obtained separately and both require that a privacy notice be accompanied with the consent.
- **Consent for the sale of CHD has heightened requirements: This "authorization" requires a consumer's signature, has 9 distinct requirements, and is only valid for a year.**



[www.redcloveradvisors.com](http://www.redcloveradvisors.com) | [info@redcloveradvisors.com](mailto:info@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 TO-DO LIST

6

## Obtain consent for the **sale, sharing or processing** of Personal Data about minors

### TO-DO

- ✓ Minor/Child is someone under 13
- ✓ Identify where Personal Data and Sensitive Personal Data about minors is collected, shared or sold.
- ✓ Obtain appropriate consent prior to the collection, sharing, or selling of Personal Data about minors.
- ✓ Appropriate consent for someone under 13 is parental consent
- ✓ Ensure Privacy Notice to minors is age-appropriate and written in a clear, plain way that is easily understood.
- ✓ Confirm strong security measures are in place for Sensitive Personal Data about minors.



## Highlights of New U.S. Data Privacy Law Requirements

- 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.
  - OR does not explicitly state as such but in practice has the same rule
- Best practice: children should receive an age-appropriate Privacy Notice.
- Heightened security measures for Sensitive Personal Data about minors.
- Consent is required for the processing for targeted advertising or sale in **Montana** for ages 13-16, in **Oregon** and **Connecticut** for ages 13-15, and ages 13-18 in **Delaware**.
- CT New Law Highlights:
  - Do not collect precise geolocation data from a minor without consent
  - Social Media accounts for those under 16 require parental consent
  - Cannot allow tracking of minors' online activity (like a website log installed by parents) without a conspicuous signal to minor that they are being monitored
  - And more!

# Red Clover Advisors 2024 TO-DO LIST

## 7 Disclose if Personal Data is sold to or shared with third parties for targeted advertising

Certain jurisdictions require organizations to provide individuals the right to opt-out of targeted advertising.

### 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 12 for more details



## Comparison of U.S. Data Privacy Law Requirements

### CCPA

- 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).

### New Laws

- Like the laws coming 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. (OCPA, TDPSA, DPDPA, and MCDPA)

**8 Update and Revise 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**

- ✓ Update external Privacy Notices to ensure compliance with applicable data privacy laws.
- ✓ Satisfy Texas’s unique rules: the privacy notice must include the following when either sensitive or biometric data is collected (or both):
  - ✓ "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.



Be sure to actively maintain your Privacy Notice, checking it throughout the year to ensure it aligns with the latest laws

As more laws enter into force, consider splitting your privacy notice requirements into three parts: **GDPR**, **CCPA**, and the other Comprehensive **US State Laws**. 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.

## 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 include **disguising ads** to look like independent content, making it difficult for consumers to cancel subscriptions or charges, burying key terms or junk fees, and **tricking consumers** into sharing data.

The new laws are part of a broader focus on dark patterns, with state regulator's increasingly seeking to stamp these patterns out.

### TO-DO

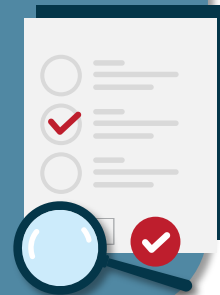
- ✓ Review your user interfaces to identify and **eliminate any Dark Patterns.**
- ✓ Consider engaging an independent party outside of your organization and/or conducting user testing facilitated by a market research firm to identify any potential Dark Patterns, particularly in any consent processes.
- ✓ Because the FTC and other enforcement bodies are focused on stamping out dissimilar treatment across populations, the review and/or user testing optimally will include input from individuals representing different populations (such as age, gender, race, level of education, etc.) so that different perspectives and experiences can be considered.
- ✓ Use the results of the review or user testing to reassure leadership that your organization does not engage in this behavior. Particularly if your efforts included diverse populations, this can be part of your Diversity & Inclusion activities.
- ✓ Add training on Dark Patterns to your teams that develop web interfaces and consent processes.



Many laws, including most of the new laws, treat **consent** that has been obtained via a **Dark Pattern as invalid.**

Use the results of a Dark Patterns review or user testing exercise to **reassure your leadership** that your organization does not engage in this behavior.

Experience shows that customer's consistently object to dark patterns, harming customer retention.





**9 Eliminate Dark Patterns (cont'd)**

Keep in mind the following principles when designing new user interfaces:

- Choices should be presented in an **even-handed manner** (“Yes” or No” or “Accept” or “Reject” in the same size font)
- Avoid **emotional language** (avoiding language like **“DANGER DO NOT CLICK OPT-OUT”**)
- Do not interpret **silence or failure to take action** as consent
- Do not use **pre-selected** options
- Ensure that **exercising choice** (*consenting or not consenting*) involves the same number of clicks/steps
- Consider the target audience's **ability to understand and navigate** when designing choice options

**10 Create or revise data minimization/retention policy**

Ensure your organization complies with data minimization and retention requirements.

**TO-DO**

- ✓ Implement procedures to limit the collection, use, retention, and sharing of Personal Data to that which is "reasonably necessary" to achieve the specified purposes of processing.



**REMEMBER:**  
Put the customer first when creating user experiences!



# Red Clover Advisors 2024 TO-DO LIST

10

## Review and amend contracts with third parties/ vendors/service providers/processors

Organizations must create binding contracts with vendors that set out the subject matter and duration of the processing, the nature and purpose of the processing, the type of Personal Data and categories of data subjects, and the obligations and rights of each party to the contract.



### TO-DO

- ✓ Review vendor contracts to ensure they include appropriate data privacy and protection language.
  - ✓ Processor obligations include assisting Controllers to respond to Individual Rights Requests and to make corrections to and/or delete Personal Data that they process on behalf of Controller.
  - ✓ The state laws also require that contracts include an audit provision, requiring Processors to cooperate with efforts by Controller to confirm compliance.
- ✓ Conduct information security and privacy assessments to confirm third parties are compliant with applicable data privacy laws.
- ✓ Implement procedures to identify, manage, and mitigate information security and privacy risks.
- ✓ Understand how a vendor uses personal information. Depending on the level of usage, it may qualify as a sale under the CCPA.
- ✓ Confirm vendors can respond to Individual Rights Requests.

## Highlights of New U.S. Data Privacy Law Requirements

- Execute written data processing agreements that govern how vendors and other third parties process data on behalf of your business.
- These agreements should generally address dynamics such as the purpose and duration of processing, the specific data the third party is processing on behalf of your organization, and any specific limitations on processing by the third-party.



---

 Red Clover Advisors  
**2024 TO-DO LIST**

**11** **Manage Individual Rights Requests**

Organizations must afford individual's specific rights and disclose those rights in its Privacy Notice.



**TO-DO**

- ✓ Implement internal procedures to accept and respond to Individual Rights Requests (including Employee Rights Requests where applicable).
  - ✓ Ensure there is a process to include new vendors that process data (especially if they need to be added to automated processes)
- ✓ If new vendors or features are added during the year, work with the data inventory and your team to ensure individual rights reflect the changes made to your service.
- ✓ Confirm you have established an appeals process that is conspicuous and easy to use.
- ✓ Provide clear and conspicuous disclosures in your organization's external Privacy Notice to inform individuals of their rights and how to exercise those rights, including how to submit an appeal.
  - ✓ Add information to your external Privacy Notice and/or template response letters for appeals that informs individuals that they may contact the state Attorney General if they have concerns about the result of an appeal.
- ✓ Record, track, and maintain records of Individual Rights Requests.
- ✓ Train all employees who handle Individual Rights Requests on the organization's policies and procedures.


**Individual Rights Differences – Distinctions in the New Laws**

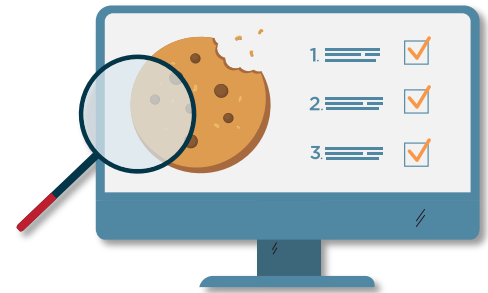
- Trade Secrets are excluded from Individual Rights requests in Delaware and Oregon.
- **Delaware and Oregon allow the deletion of any personal data the controller has about the consumer**, as opposed to only consumer provided information such as the rule in Utah.
- Oregon uniquely allows an individual to **request the specific third parties with whom their data has been shared**, as opposed to only the categories of third parties.

**12** **Establish and Maintain a Cookie Banner & Do Not Sell Links, and Prepare for Universal Opt-Out**

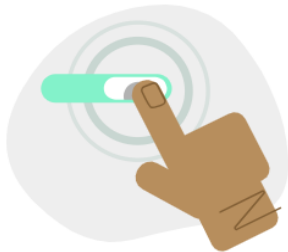
Mirroring requirements in CA, CT, CO, VA, and UT, these new laws require that Controllers allow consumers to exercise their rights to opt-out of targeted advertising. OR, TX, MT, and DE also mandate the recognition of a “universal opt-out mechanism”, commonly called a GPC.

**TO-DO**

- ✓ Review any existing cookie banner your website(s) may have to confirm that it provides the requisite notices and enables users to opt out (or opt in, if required by applicable data privacy laws).
- ✓ Ensure that the cookies listed in your preference center are accurate to the cookies on the site.
- ✓ Prepare for acceptance of universal opt-outs.
- ✓ 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 Personal Data is not being sold.
- ✓ Train your team on the latest in cookie consent and management practices.



**GPC Basics**



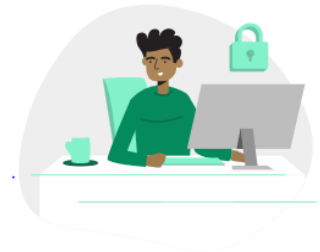
**Turn On GPC**

Enable Global Privacy Control to communicate your privacy preference.



**Send the Signal**

Your browser will send the GPC signal to websites you visit.



**Exercise Your Rights**

Participating websites can respect your privacy rights accordingly.

# Red Clover Advisors 2024 TO-DO LIST

## 13 Privacy Training and Awareness

Organizations should establish privacy training and awareness programs that include year-round activities for employees.

### TO-DO

- ✓ Implement privacy training such as workshops for those employees with responsibilities for managing Personal Data.
- ✓ Ensure training and awareness programs include security awareness, Individual Rights Requests (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 and compliance.



## Highlights of U.S. Data Privacy Law Requirements: CCPA v. Everyone Else

### CCPA

- Requires that covered businesses train the individuals responsible for internal compliance with the regulation as well as those responsible for handling consumer requests regarding privacy practices. These individuals should be aware of applicable CCPA regulations and be able to direct consumers on how to use their statutory rights.
- Organizations must also have and comply with 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.

### Other State Laws

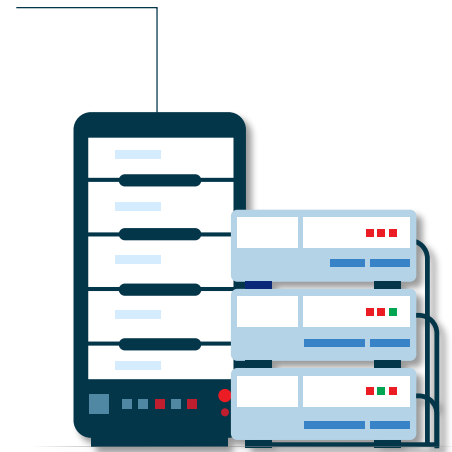
- Organizations should implement and maintain a training program for all employees who handle Personal Data and Individual Rights Requests, including for employees.
- Training should be year-round and not just on an annual basis. Training should also be documented. Organizations should have a means to identify which staff has received training.

**14** **Validate data security practices and procedures are implemented and maintained**

Organizations should have implemented and documented robust security processes, procedures and policies to protect Personal Data from unauthorized access.

**TO-DO**

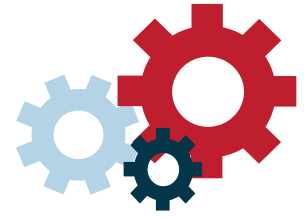
- ✓ Create, implement, and/or update technical and operational security measures to protect Personal Data.
- ✓ Dedicate a resource to proactively monitor security and practice incident response scenarios to prepare for possible data breaches. Review these policies and incident response plans at least annually.
- ✓ Confirm that safeguards are commensurate with the type of Personal Data and the means used to transmit it.



**CCPA v. Everyone Else: Security Practices**

CCPA	Other State Laws
<ul style="list-style-type: none"><li>• 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).</li></ul>	<ul style="list-style-type: none"><li>• Continually assess and implement reasonable administrative, technical, and physical data security practices and procedures to protect Personal Data.</li><li>• Perform regular cybersecurity audits for processing that presents a significant risk to consumer privacy or security.</li></ul>



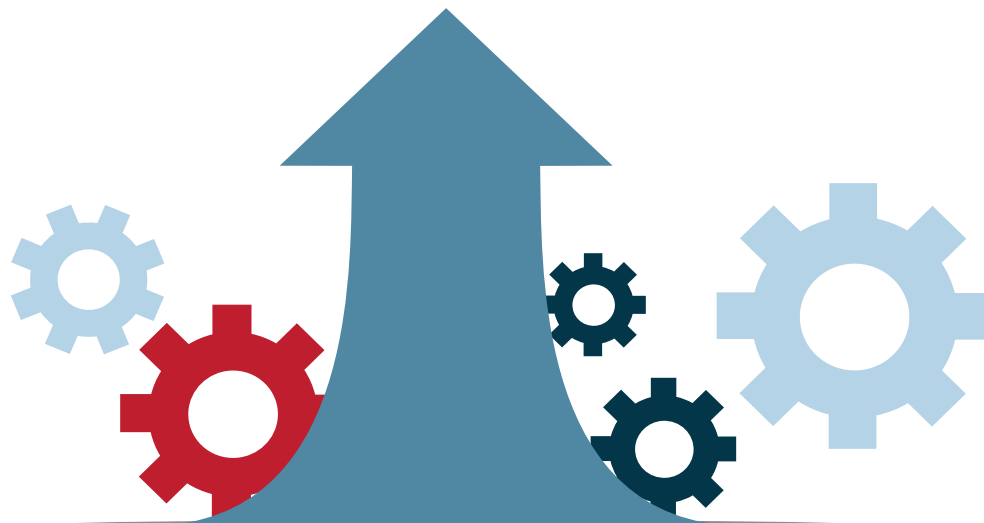


## **15** Sustainable Compliance

Organizations must undertake efforts to comply with existing and emerging data privacy laws and compliance obligations to further mature their data privacy governance programs. Increased privacy regulations require a durable and sustainable data privacy governance model.

### **TO-DO**

- ✓ Embed privacy controls throughout the Personal Data lifecycle.
- ✓ Align Privacy with your organization's strategy.
- ✓ Establish and maintain a privacy framework that aligns with privacy principles and incorporates privacy by design to ensure on-going compliance.
- ✓ Implement a risk-based approach, focusing on the high-risk critical business processes and systems first.
- ✓ Have a dedicated resource (internal or external) focused on privacy.
- ✓ Identify channels to stay up to date on new and updated privacy laws
- ✓ Ensure all parts of your privacy program are updated on a regular basis, including your data inventory, individual rights strategy, cookie audit, privacy impact assessments, and all vendor contracts.





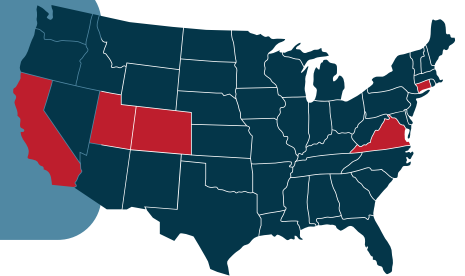
Red Clover Advisors

# 2024 TO-DO LIST

## Looking Ahead

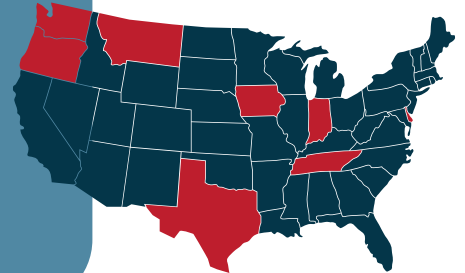
The regulatory landscape is not one to ignore and will continue to drive privacy strategy programs. 2023 was a big privacy year with the following five states having privacy laws come into effect:

- 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, eight other states (and CT passing their amendment to the CTDPA) passed laws in 2023 with the following effective dates:

- Washington (WA MHMDA) as of March 31, 2024
- Oregon (OCA) 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
- Tennessee (TIPA) as of July 1, 2025
- Indiana (INCDPA) as of January 1, 2026



Increased U.S. state and federal government data privacy regulations are expected to continue in 2024 and beyond.

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](http://www.redcloveradvisors.com)



[www.redcloveradvisors.com](http://www.redcloveradvisors.com) | [info@redcloveradvisors.com](mailto:info@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.