501CISO
501C CYBERSECURITY LEADERSHIP
Powered by ClearTone Consulting, LLC

501CISO DATA PRIVACY CHECKLIST

The 501CISO Data Privacy Checklist is a data privacy guideline available only from 501CISO. The checklist provides a comprehensive set of controls that supports your compliance with all current US state-level privacy laws and the General Data Protection Regulation (GDPR) from the European Union.
For organizations selling to or servicing customer data from US states with privacy laws or the EU, it's imperative to comply with their respective laws. Failing to adhere to these laws can result in fines and a loss of trust in your business. This checklist simplifies compliance to help you mitigate risks along the way.

Personal Data Defined

It's important to understand what data privacy laws cover and what they refer to as "Personally Identifiable Data (PII)." Does your organization collect, utilize, disclose, or sell any of these types of data:

- Names
- Email addresses
- IP addresses
- Location data
- Ages
- Credit card numbers
- Addresses
- Religious affiliations or inclinations
- Political affiliations or inclinations
- Incomes, net worths, or other financial information
- Biometric data
- Internet activity including search activity, browsing activity, and other actions
- Sensitive personal information

If you are collecting any of these data categories or similar types of data, the next checklist will help you determine if privacy laws apply to your organization.

Does your organization need to adhere to privacy laws

The various consumer privacy laws don't apply to every organization that collects personal information, they often focus on specific types of businesses. Consider which of these are true for your business:

- Your business collects personal data from individuals residing in California, Colorado, Connecticut, Utah and/or Virginia residents (with additional state and federal laws expected to be passed)
- Your business is a for-profit organization, not a government agency or a non-profit organization
- Your business meets at least one of the following criteria:
  - You have a gross annual revenue of $25 million or more
  - Buy, sell, share or process the personal data of 100,000 or more consumers in CA, CO, CT, UT, or VA
  - You collect or possess the personal information of at least 50,000 devices, consumers, or households

- More than 50% of your annual revenue comes from selling consumer data

If you checked all of the three boxes above, you are required to adhere to US consumer data privacy laws.

- [ ] Your business collects personal data from individuals residing in the EU

If you checked the above box, then you are required to adhere to GDPR.

Understand user rights granted by privacy laws

The basis of consumer privacy laws is a guarantee of certain rights to consumers and users. Structurally, US laws are very similar to the GDPR. To understand how to become compliant, you should first understand these important rights you must grant to consumers:

- [ ] The right to know what data you have collected about them, allowing them to request a report of the data you have collected about them from the past 12 months at no cost
- [ ] The right to opt out of having their data sold
- [ ] The right to request that you delete the data you have collected about them
- [ ] The right to request correction of inaccurate personal information
- [ ] The right to be notified of the data you are collecting
- [ ] The right to non-discrimination, meaning that they are entitled to the same services at the same cost as others regardless of the additional rights they have as residents of CA, CO, CT, UT, and/or VA, regardless of whether they choose to exercise their rights
- [ ] The right to limit the use and sharing of Sensitive Personal Information
- [ ] The right to opt-out of targeted advertising
- [ ] The right to opt-out of automated decision making with a legal or similarly significant consequence
- [ ] The right to opt-out of PII processing using a global agent mechanism such as “Do Not Track”

Data privacy compliance

Once you have an understanding of the foundation of data privacy laws and whether they apply to your organization, it’s time to get into the details. Follow this checklist to work toward compliance:

- [ ] Investigate your system and policies for compliance to identify which compliance requirements you already meet and which requirements you need to address.
  - Review and update your privacy policy
    - Detail what categories of data you are collecting, disclosing, sharing, or selling about users or consumers
    - Set up your privacy notice to appear for users or consumers at or before the point when you start collecting their data
    - Include a description of the new rights users have under each privacy law
    - Add instructions for how consumers can make privacy-related requests

  - Ensure the Privacy Policy/Notice is reasonably accessible to consumers with disabilities in accordance with Web Content Accessibility guidelines version 2.1
  - Make the privacy notice available in all languages in which your company does business
  - Privacy Notice for Mobile Applications and Web Pages: if you collect personal information that a consumer would not reasonably expect from a mobile device, you must provide a just-in-time notice containing a summary of categories collected and a link to the full notice
- Ensure inclusion of:
  - The categories of personal data processed by your company
  - The purpose for processing personal data
  - At least two methods by which consumers may exercise their consumer rights
  - The categories of personal data that you share with third parties, if any
  - An active electronic mail address or other online mechanism that the consumer may use to contact you
  - Data retention policy for each category of personal information (or the criteria used to determine that period)

- Ensure your website honors Global privacy opt out schemes such as https://allaboutdnt.com/ and https://globalprivacycontrol.org/, which may be implemented in the user's web browser

- Allow users to opt out of the targeted advertising or sale of the their personal data

- Allow users to opt out of automated processing decisions that produce legal or similarly significant effects concerning the user

- Update your data processes and data inventories
  - Establish a data inventory that tracks your data processing activities, including information such as:
    - Systems and vendors who store or process PII
    - Systems and vendors who store or process Sensitive Personal Information
    - Tracking data-related consumer requests such as requests to delete data
  - Update your policies and protocols to enforce and protect users' privacy rights
    - Create a process for promptly and efficiently deleting a consumer's data upon request
    - Set up at least two methods for consumers to make data-related requests including a toll-free phone number and an online option
    - Create a policy to update your privacy policy every 12 months

- Put reasonable data security measures in place to protect users' data
  - If you possess de-identified data you should:
    - Take reasonable measures to ensure that the data cannot be associated with an individual
    - Publicly commit to maintaining and using de-identified data without attempting to re-identify the data; and
    - Contractually obligate any recipients of the deidentified data to comply with these measures
  - Update your agreements with third-party data processors to ensure that consumers' data is protected while it's in their hands
    - Ensure that each person processing personal data is subject to a duty of confidentiality with respect to the data

- At the controller s direction, delete or return all personal data to the controller as requested at the end of the provision of services, unless retention of the personal data is required by law;
- Notify the controller if it makes a determination that it can no longer meet its obligations
- Grant the controller the right, upon notice, to take reasonable and appropriate steps to stop and remediate unauthorized use of personal information
- Implement reasonable security procedures and practices appropriate to the nature of the personal information to protect the personal information from unauthorized or illegal access, destruction, use, modification, or disclosure
- Upon the reasonable request of the controller, make available to the controller all information in its possession necessary to demonstrate the processor's compliance with its obligations
- After providing the controller an opportunity to object, engage any subcontractor pursuant to a written contract that requires the subcontractor to meet the obligations of the processor with respect to the personal data; and
- Allow, and cooperate with, reasonable assessments by the controller or the controller s designated assessor, or the processor may arrange for a qualified and independent assessor to conduct an assessment of the processor s policies and technical and organizational measures in support of its obligations, using an appropriate and accepted control standard or framework and assessment procedure for such assessments.
- The processor shall provide a report of such assessment to the controller upon request.

Design and implement privacy compliance training for your employees and contractors to make them aware of the policies and ensure that they follow them.

- Organizations with employees in California will need to do several things:
  - Create employee-facing privacy notices/policies
  - Determine how the consumer rights will be applied to applicants and employees (both current and former)
  - Determine when consumer rights will NOT be honored and the legal justification (ex. there will be times when a business will not delete records of current and former employees which the business must maintain to be compliant with wage and hour laws)
  - Determine a process for responding to SAR requests from current and former employees