CCPA Website Compliance Checklist

Due to CCPA, Californians can now ask to see all kinds of personal information that a business operating in the state holds on them. Review your web policy and update your site to be CCPA compliant with this checklist.

1. UPDATE PRIVACY NOTICES AND POLICIES

Your privacy policy must be updated every 12 months to comply with the California Consumer Privacy Act and should include:

- [ ] A description of the new rights afforded California residents
- [ ] The methods for submitting a personal information or erasure request
- [ ] A link to an opt-out page on the website
- [ ] The types of personal information collected in the past 12 months
- [ ] The types of personal information sold in the past 12 months
- [ ] The types of personal information disclosed for a business purpose in the past 12 months
- [ ] The categories of sources for each piece of personal data
- [ ] The purpose of use for each category of collected information

2. UPDATE DATA STRATEGIES, INVENTORIES, AND BUSINESS PROCESSES

Data inventories are directories for managing sensitive data throughout a business. There are a few columns that will have to be added to the offline data inventory or data inventory web page. These include:

- [ ] Identifying data uses that involve the “sale” of information
- [ ] Identifying categories of information that are transferred to third parties
- [ ] Identifying categories of personal information that are covered by HIPAA, the FCRA, or another law that would exempt the data from the CCPA’s scope
- [ ] Identifying if the data was collected more than 12 months ago and, thus, is potentially exempt

3. USE PROTOCOLS TO ENSURE CUSTOMER RIGHTS

The CCPA crystalizes certain consumers’ rights, and a business must have protocols in place to ensure that these rights are granted.

- [ ] Provide a toll-free telephone number for requests
- [ ] Provide an “interactive webform” that handles access requests and opt-out requests.
- [ ] A clearly labeled “Do Not Sell My Personal Information” link must also be posted on the business’s homepage.

4. MAKE SECURITY UPDATES

Businesses covered by the CCPA must protect personal data with “reasonable” security. This means assessing threats to data within the organization, ranking the detected vulnerabilities in order of risk, and addressing the highest risks first.

5. UPDATE THIRD PARTY CONTRACTS AND PROCESSOR AGREEMENTS

- [ ] Create a list of all the vendors, service providers, and other third parties that receive data from your organization
- [ ] Update third-party contracts and processor agreements to include the provision of processing records, requirements for the syncing of consumer response processes, and more.

6. EDUCATE EMPLOYEES

Ensure that employees have the necessary training to make sense of the CCPA requirements. Employees handling consumer inquiries must have good knowledge of the statute and know how to direct consumers to exercise their rights.

Need Assistance?

Chat with us
https://www.zesty.org

Ask in our Community Slack
https://chat.zesty.io