Checklist for State Privacy Law Compliance

ACXIOM
KINESSO
MATTERKIND

Organizational Policies, Procedures, and Practices

a. Update Website Privacy Policy (see details below under "Notices," subsection (b))
b. Implement/update internal policies to address every aspect of this checklist
c. Review other internal policies or procedures to ensure that any inconsistencies with California, Colorado, Connecticut, Utah, and Virginia requirements are resolved (e.g., HR policies, IT policies, etc.)

Inventory the Organization's Data Processing Activities

a. Identify Categories of Personal Information Collected[1]
    i. Determine whether sensitive personal information is collected, used, or disclosed
    ii. Determine whether personal information is sold, shared, or used for targeted advertising
    iii. Determine whether any uses/disclosures of personal information would trigger data protection assessment requirements
    iv. Determine whether personal information is maintained in aggregated or deidentified form during storage or transmission
    v. Identify personal information that can be used in aggregated or deidentified form
    vi. Develop a de-identification/anonymization standard and procedure
    vii. Assess whether your organization has the capability to separate personal information of California, Colorado, Connecticut, Utah, and Virginia residents from that of other states' residents
b. Identify Purposes of Collection or Processing
c. Identify Sources of Collection
d. Identify Categories of Personal Information Disclosed
e. Identify Recipients of Sales, Shares, and Other Disclosures
f. Identify Categories of Personal Information Sold
    i. Consider whether personal information of consumers less than 16 years of age is involved. If so, determine whether affirmative authorization has been obtained from the consumers (13-16 years old) or their parents or guardians (<13 years old) for the sale.
g. **CPRA**: Assess your data retention periods for personal and sensitive personal information

[1] As used herein, "personal information" refers to personal information under the CPRA and personal data under the CPA and VCDPA, unless otherwise specified. Similarly, as used herein, "sensitive personal information" refers to sensitive personal information under the CPRA and sensitive data under the CPA and VCDPA.

Notices

a. **CPRA**: Implement Notice at Point of Collection
    i. Evaluate data flows to identify points at which consumer interaction occurs, and identify sources of personal information
    ii. Check that notices are provided whenever information is collected, not just when you actually collect information directly from a consumer
    iii. Content requirements:
        1. Personal information:
            a. Categories of personal information you collect or use
            b. Purposes for which you collect personal information
            c. Whether such information is sold or shared
        2. Sensitive personal information:
            a. Categories of sensitive personal information you collect
            b. Purposes for which you collect sensitive personal information
            c. Whether such information is sold or shared
        3. The length of time your organization intends to retain each category of personal information or sensitive personal information, and the criteria used to determine those retention periods
b. Website Privacy Policy
    i. **CPRA**: Must be updated every 12 months
    ii. Content requirements:
        1. 2+ methods for submitting consumer requests, including a toll-free phone number
        2. The categories of personal information you collect and process about consumers, including all categories thereof collected/processed in the past 12 months
        3. The categories of sources from which such personal information is collected
        4. The purposes for which you collect, sell, share, or process personal information
        5. The categories of third parties to whom personal information is disclosed
        6. The categories of personal information you disclose to third parties
        7. If personal information is sold or processed for purposes of targeted advertising, or otherwise sold or shared, a disclosure of the same, a list of the categories of personal information you have sold or shared in the preceding 12 months, an opt-out link, and instructions for opting-out.[2]
            a. **CPRA**: If you have not sold or shared consumer personal information in the preceding twelve months, a prominent disclosure that you have not done so.
            b. **CPRA**: If you disclose consumers' personal information for business purposes, the categories of personal information you have disclosed about consumers for a business purpose in the preceding 12 months. If you have not disclosed consumers' personal information for a business purpose in the preceding 12 months, a statement disclosing the same.
        8. **CPRA only**: A description of consumers' rights to make the following requests no more than twice in every 12-month period:

[2] Consider implementing a universal opt-out method. The use of such a method will be required in Colorado, effective July 1, 2024.

a. Right to receive notice at or before the point of collection
b. Right to request correction of inaccurate personal information
c. Right to request deletion
d. Right to access:
    i. The categories of personal information you have collected about them;
    ii. The categories of sources from which you collect personal information;
    iii. The business or commercial purpose for collecting, selling, or sharing personal information;
    iv. The categories of third parties to whom you disclose personal information;
    v. The specific pieces of personal information you have collected about them
e. Right to receive information about onward disclosures:
    i. If you sell or share their personal information, or disclose it for a business purpose:
        1. The categories of personal information you have collected about them;
        2. The categories of personal information you have sold or shared about them, and the categories of third parties to whom you sold or shared their personal information; and
        3. The categories of personal information you have disclosed about them for a business purpose, and the categories of persons to whom it was disclosed for a business purpose.
f. Right to not be discriminated against because of the consumer's exercise of any of the above rights, including the following:
    i. You will not deny the consumer goods or services;
    ii. You will not charge the consumer different prices or rates for goods or services or give them different discounts, benefits, or penalties;
    iii. You will not provide the consumer a different level of quality of goods or services; and
    iv. You will not suggest to the consumer that they will receive a different price or rate for goods or services or a different level or quality of goods or services

9. **CPA** and **VCDPA**: Information about how to appeal denials of consumer requests
10. If you plan to offer financial incentives, including payment to consumers as compensation for the collection, sale, or deletion of personal information, your website privacy policy must clearly:
    a. Describe the material terms of the financial incentive program;
    b. Obtain prior opt-in consent from the consumer; and
    c. Inform the consumer that they may revoke their consent at any time

Consumer Request Mechanism

a. **CPRA**: Establish a toll-free number for submission of consumer requests, and provide at least one additional method for receiving consumer requests
b. Create a website form to receive consumer requests
c. Provide an opt-out link for consumer opt-outs from the sale/sharing of personal information
d. **CPRA**: Create a "Do Not Sell or Share My Personal Information" button and opt-out website, and post the button on all webpages where you collect personal information
e. **CPRA**: Create a "Limit the Use of My Sensitive Personal Information" button, and post the button on your internet homepages
f. Consider developing a universal opt-out mechanism

Request Handling Procedures

a. Establish procedures to:
    i. Respond to requests to access personal information
    ii. Respond to requests to receive copies of personal information
    iii. Respond to requests for information about sales, shares, or other disclosures of personal information
    iv. Respond to requests to opt-out of the sale/sharing of personal information
    v. Respond to requests to delete personal information, including by identifying exceptions likely applicable to various use cases
    vi. **CPRA**: Respond to requests to limit the use or disclosure of sensitive personal information
    vii. **CPA & VCDPA**: Respond to requests to opt-out of the use of personal information for purposes of targeted advertising
    viii. **CPA & VCDPA**: Respond to requests to opt-out of profiling in furtherance of decisions that produce legal consequences
    ix. **CPA & VCDPA**: Respond to appeals of consumer request denials
b. Establish procedures to obtain consent prior to:
    i. **CPA & VCDPA**: Processing for purposes beyond those disclosed in initial notice; processing sensitive data; processing personal data of a known child
    ii. **CPRA**: Selling or sharing personal information of a consumer who has opted-out of the same; selling or sharing personal information of a minor; using or disclosing sensitive personal information of a consumer who has opted-out of the same; entering a consumer into a financial incentive program
c. Establish and implement your preferred administrative approach to routing, escalating, tracking, recording, and responding to consumer requests
d. Develop a standardized format for responding to consumer requests, including standard email and mail formats for different types of requests
e. Create a registry of systems where information that may be subject to a consumer request is stored, and develop processes for keeping the registry up to date and for extracting information therefrom in response to consumer requests

f. Develop a registry of relationships that need to be characterized as "selling," "sharing," or disclosing personal information for purposes of targeted advertising, for use in responding to opt-out requests
g. Identify processing activities that may constitute processing for purposes of targeted advertising, for use in responding to opt-out requests
h. Identify and classify relationships with third parties that involve selling, sharing, or otherwise disclosing personal information
i. Develop registry of relationships that involve disclosures or sales of personal information that must be provided to a consumer in response to a request for information

Data Protection Assessments

a. Determine whether any personal information collected or processed would trigger data protection assessment requirements under the CPA, VCDPA, or CPRA
b. Develop procedures to conduct and document data protection assessments
c. Re-evaluate data flows at appropriate intervals
d. Make the assessments available to the AG upon request or to the CPPA "on a regular basis" as further defined by CPRA regulations, when published

Contracts

a. Identify existing contracts that relate to personal information and determine whether revision or renegotiation is required
b. Review contracts to determine whether any contracts seek to waive or limit in any way consumers' rights under the CPRA; if so, these provisions will be void and unenforceable
c. Identify contracts that need to be renegotiated or revised

Reasonable Security Procedures and Practices

a. **CPRA**: Establish and implement procedures to cure an alleged data breach within 30 days and inform the complainant that no further breach will occur
b. For guidance regarding implementation of reasonable security procedures and practices, see:
    i. Center for Information Security's Critical Security Controls
    ii. Guidance from the California AG on cybersecurity matters (here)
    iii. Guidance from the Colorado AG on data security best practices (here)
    iv. Relevant industry standards

Training

a. Develop training materials and conduct training regarding:
    i. CPRA requirements
    ii. Verifying and responding to consumer requests
    iii. Other topics, as needed