Morgan Lewis

STATE PRIVACY LAW

2023 CHECKLIST FOR CPRA PLUS COMPLIANCE

Companies that devoted significant effort over the last few years to ensuring compliance with the **California Consumer Privacy Act (CCPA)** face additional potential compliance burdens arising from the **California Privacy Rights Act (CPRA)**, **Colorado Privacy Act (CPA)**, **Connecticut Data Privacy Act (CTDPA)**, **Utah Consumer Privacy Act (UCPA)**, and **Virginia Consumer Data Protection Act (VCDPA)**.

Given the myriad compliance pitfalls, we developed the below checklist to help guide those companies that are already substantially compliant with the CCPA in taking on the next compliance challenge.

✓ Determine which state privacy law(s) apply to your business

- The CPRA, effective January 1, 2023, applies just like the CCPA—applicable to all for-profit businesses that do business in California and meet the revenue or collection thresholds and for which an exception does not apply.
- The VCDPA (effective January 1, 2023), CPA (effective July 1, 2023), CTDPA (effective July 1, 2023), and UCPA (effective December 31, 2023) apply to any for-profit business that conducts business in, or produces products or services targeted to residents of, Virginia, Colorado, Connecticut, or Utah, respectively, and meets one of the following conditions, subject to exceptions:
  a. Annually controls or processes the personal information of 100,000 or more state residents (Connecticut excludes personal data controlled or processed solely for the purpose of completing payment transactions); or
  b. Controls or processes personal data of at least 25,000 state residents; and

     For Utah and Virginia: derives over 50% of gross revenue from the sale of personal data.

     For Colorado: derives revenue or receives a discount on the price of goods or services from the sale of personal data.

     For Connecticut: derives over 25% of gross revenue from the sale of personal data.
  c. Utah also has an annual revenue threshold of $25 million before the requirements apply.

Employment and business-to-business exemptions. The CPA, CTDPA, UCPA, and VCDPA exempt personal information collected from employees, applicants, officers, directors, contractors, and business representatives. The CPRA extends the CCPA's limited exemption on these categories, but only through January 1, 2023.

✓ Create a process for new right to correct consumers' personal information

California, Colorado, Connecticut, and Virginia provide consumers with a new right to correction. To effectuate this right, businesses shall process a consumer's right to correct inaccuracies in the consumer's personal information.

✓ Build in processes for new opt-out rights—advertising and sharing

- Businesses must implement a means for consumers to opt out of the processing of their personal information for purposes of the following:

a. Sharing of their personal information used for "cross-context behavioral advertising," even where no money is exchanged between the business and the third party—with requirement for a "Do Not Sell or Share My Personal Information" link added to a company's homepage (CPRA).
b. Targeted advertising (CPA, CTDPA, UCPA, and VCDPA).
c. Profiling in furtherance of decisions that produce legal or similarly significant effects concerning a consumer (CPA, CTDPA, and VCDPA).

✓ Create a process to provide disclosed information to consumers

- In all five states, in response to a verifiable request, businesses are required to provide the specific pieces of personal information obtained from the consumer in a format that is easily understandable to the average consumer and, to the extent technically feasible, in a commonly used format.
- The CPRA provides for the right to know what information was collected on or after January 1, 2022, unless doing so proves impossible (i.e., a shorter data retention period) or would involve a disproportionate effort, which extends the current 12-month lookback period for requests to know under the CCPA.
- The CPA, CTDPA, UCPA, and VCDPA do not set an express time period for how far back a consumer's portability request may extend, so it can be presumed that portability obligations cover all personal information collected beginning on the date those statutes go into effect.

✓ Develop a process for processing sensitive personal information

- Virginia, Colorado, and Connecticut require affirmative consent to process a consumer's sensitive personal information.
- The CPRA and UCPA do not impose an opt-in requirement to process sensitive personal information, but they do require businesses to honor a resident's request to limit the use of their sensitive personal information.
  a. For the UCPA, businesses must provide the consumer clear notice and an opportunity to opt out of the processing of their sensitive personal information.
  b. For the CPRA, businesses must provide a clear and conspicuous link on their homepage—titled "Limit the Use of My Sensitive Personal Information"—that enables a consumer to limit the use or disclosure of their sensitive personal information.
- By 2024 and 2025, respectively, the CPA and CTDPA require businesses to provide consumers with a universal opt-out option that allows a resident to click one button to exercise all opt-out rights. No such requirement exists under the CPRA, VCDPA, or UCPA.

✓ Create an appeal process for consumer requests

- The CPA, CTDPA, and VCDPA provide consumers with the right to appeal a business's denial to take action within a reasonable time period. There is no comparable right to appeal in California or Utah.
  a. Under the CTDPA and VCDPA, within 60 days of receiving an appeal, a business must inform the consumer in writing of its response to the appeal and, if the business denies the appeal, it must provide the consumer with an "online mechanism," if available, or other method through which the consumer may contact the state attorney general to submit a complaint.
  b. Under the CPA, businesses must provide an appeal process that is conspicuously available and easy to use. Within 45 days of receiving an appeal, a business must inform the consumer in writing of its response to the appeal. If an appeal is denied, the law requires the business to inform the consumer of their ability to contact the Colorado attorney general if they have concerns about the result of the appeal.

✓ Revise privacy policies

Businesses must disclose in their privacy policies—at or before the point of collection—the following:

- The categories of sensitive personal information collected and whether that information is sold or shared (CPRA).
- The length of time the business intends to retain each category of personal information or, if that is not possible, the criteria used to determine that period (CPRA).
- Any business that processes personal information for targeted advertising must clearly and conspicuously disclose such processing, as well as

the manner in which a consumer may exercise the right to opt out of such processing (CPA, CTDPA, UCPA, and VCDPA).

- How consumers can exercise their right to appeal a business's decision with regard to the consumer's request (CPA, CTDPA, and VCDPA).
- Revisions necessary to describe the new rights and processes identified above.

✓ Assess relationships with service providers and data processors

- In all five states, contracts between a business and a data processor shall be binding and clearly set forth instructions for processing data, the nature and purpose of processing, the type of data subject to processing, the duration of processing, and the rights and obligations of both parties.
  a. In California, contracts with service providers must also prohibit the service provider from (1) selling or sharing the business's personal information; (2) retaining, using, or disclosing personal information outside of the direct business relationship between the service provider and the business; and (3) combining personal information received from one business with information received from another business.
  b. In California, businesses will need to enter into a contract with any entity to which they disclose personal information, including third parties to which they sell personal information. The contract must include certain provisions, including (1) limiting use to specified purposes, and (2) providing the same level of privacy protections as required by the CPRA.
- The CPRA obligates businesses fulfilling legitimate deletion requests to also notify contracted service providers or other third parties to delete the consumer's personal information from those third-party records.

✓ Conduct risk assessments and implement data protection requirements

- Businesses are required, under certain circumstances, to conduct risk assessments to weigh the benefits resulting from the processing of consumers' personal information.
  a. The CPRA requires any business that processes consumers' personal information in a manner that presents "significant risk" to consumers' privacy or security to perform periodic (1) privacy risk assessments and (2) independent cybersecurity audits.
  b. Colorado, Connecticut, and Virginia require a mandatory data protection assessment for any of the following processing activities involving personal information: (1) sale of personal information, (2) processing of sensitive personal information, and (3) targeted advertising.
- No such requirement exists in Utah.

✓ Ensure data minimization and retention requirements are met

a. All five states establish data minimization principles and purpose limitations on a business's ability to collect personal information.

a. Businesses shall not retain a consumer's personal information or sensitive personal information for each disclosed purpose for a period longer than is reasonably necessary and proportionate to achieve its stated purposes.

Morgan Lewis

HOW WE CAN HELP

If we can be of assistance regarding any state privacy acts, please contact a Morgan Lewis lawyer listed below:

W. Reece Hirsch
+1.415.442.1422
reece.hirsch@morganlewis.com

Mark L. Krotoski
+1.650.843.7212
mark.krotoski@morganlewis.com

Carla B. Oakley
+1.415.442.1301
carla.oakley@morganlewis.com

Tess Blair
+1.215.963.5161
tess.blair@morganlewis.com

Joseph Duffy
+1.213.612.7378
joseph.duffy@morganlewis.com

J. Warren Rissier
+1.213.680.6860
warren.rissier@morganlewis.com

Gregory T. Parks
+1.215.963.5170
gregory.parks@morganlewis.com

Ezra D. Church
+1.215.963.5710
ezra.church@morganlewis.com

Michelle Park Chiu
+1.415.442.1184
michelle.chiu@morganlewis.com

Kristin M. Hadgis
+1.215.963.5563
kristin.hadgis@morganlewis.com

Bryan P. Goff
+1.212.309.6157
bryan.goff@morganlewis.com

Terese Schireson
+1.215.963.4830
terese.schireson@morganlewis.com

Martin Hirschprung
+1.212.309.6837
martin.hirschprung@morganlewis.com

Catherine Hounfodji
+1.713.890.5120
catherine.hounfodji@morganlewis.com

www.morganlewis.com

061622_220342