wiley

# U.S. State Privacy Law Guide

## 2023 Omnibus Privacy Laws

| | California Privacy Rights Act of 2020 (CPRA) | Virginia Consumer Data Protection Act (VCDPA) | Colorado Privacy Act (CPA) | Connecticut Data Privacy Act (CTDPA) | Utah Consumer Privacy Act (UCPA) |
|---|---|---|---|---|---|
| **Overview** | The CPRA, approved by voters in 2020, amends the CCPA and imposes significant new privacy compliance obligations on businesses. It will take effect on ***January 1, 2023***. | In 2021, Virginia enacted the VCDPA, a comprehensive consumer data privacy law that will take effect on ***January 1, 2023***. | Also in 2021, Colorado enacted the CPA, a comprehensive privacy law that will take effect on ***July 1, 2023***. | In May 2022, Connecticut enacted the Personal Data Privacy and Online Monitoring Act (CTDPA). This new law will go into effect on ***July 1, 2023***. | In March 2022, Utah enacted the UCPA, a comprehensive consumer data privacy law that will take effect on ***December 31, 2023***. |
| **What Entities Are Covered?** | The CPRA applies to for-profit entities that (1) collect and control the processing of a California resident's personal information; (2) do business in California; and (3) meet at least one of the following threshold requirements:<br>• Have annual gross revenues in excess of $25 million;<br>• Receive or disclose the personal information of 100,000 or more consumers, households, or devices per year (double that of the CCPA); or<br>• Derive 50% or more of their annual revenues from selling or sharing the personal information of California residents. | The VCDPA applies to entities (including for-profit entities and certain nonprofit entities) or individuals that (1) conduct business in Virginia or target their products or services to Virginia residents; and (2) meet one or both of the following thresholds:<br>• Control or process personal data of at least 100,000 consumers over the course of a calendar year; or<br>• Control or process personal data of at least 25,000 consumers and derive over 50% of gross revenue from the sale of personal data. | The CPA applies to entities (including nonprofit entities) that (1) either do business in Colorado or produce or deliver commercial products that are targeted to Colorado residents; and (2) meet one or both of the following thresholds:<br>• Control or process the personal data of 100,000 or more consumers over a calendar year; or<br>• Derive revenue or receive a discount on the price of goods or services from the sale of personal data and process or control the personal data of 25,000 or more consumers. | The CTDPA applies to entities (including for-profit entities and certain nonprofit entities) that (1) either do business in Connecticut or produce products or services that are targeted to Connecticut residents; and (2) meet one or both of the following thresholds:<br>• Control or process the personal data of 100,000 or more consumers during a calendar year (excluding personal data controlled or processed solely for the purpose of completing a payment transaction); or<br>• Control or process the personal data of 25,000 or more consumers and derive more than 25% of their gross revenue from the sale of personal data during a calendar year. | The UCPA applies to a for-profit "controller" or "processor" entity that (1) conducts business in Utah or produces a product or services that targets Utah residents; (2) has an annual revenue of $25 million or more; and (3) meets at least one of the following thresholds:<br>• Controls or processes the personal data of 100,000 or more consumers; or<br>• Derives over 50% of the entity's gross revenue from the sale of personal data and controls or processes personal data of 25,000 or more consumers. |

wiley

# U.S. State Privacy Law Guide

## 2023 Omnibus Privacy Laws

| | CPRA | VCDPA | CPA | CTDPA | UCPA |
|---|---|---|---|---|---|
| **What Information Is Protected?** | The CPRA uses the same definition of personal information as the CCPA, but adds a new subcategory: sensitive personal information. Sensitive personal information is defined to include:<br>• Social Security, driver's license, state identification card, or passport number;<br>• Account login, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account;<br>• Precise geolocation;<br>• Racial or ethnic origin, religious or philosophical beliefs, or union membership;<br>• The contents of a consumer's mail, email, and text messages unless the business is the intended recipient of the communication;<br>• Genetic data; or<br>• The processing of biometric information for the purpose of uniquely identifying a consumer, such as data pertaining to health, sexual orientation, and sexual interactions. | The VCDPA defines personal data as "any information that is linked or reasonably linkable to an identified or identifiable natural person."<br>The VCDPA provides additional protections for sensitive data. Sensitive data is defined to include:<br>• Racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship status;<br>• Genetic or biometric data processed for the purpose of uniquely identifying an individual;<br>• Personal data collected from a known child; or<br>• Precise geolocation data. | The CPA defines personal data as "information that is linked or reasonably linkable to an identified or identifiable individual."<br>The CPA provides additional protections for sensitive data. Sensitive data is defined to include:<br>• Racial or ethnic origin, religious beliefs, a mental or physical health condition, sex life or sexual orientation, citizenship or citizenship status;<br>• Genetic or biometric data processed for identification purposes; or<br>• Personal data from a child. | The CTDPA defines personal data as "information that is linked or reasonably linkable to an identified or identifiable individual."<br>The CTDPA provides additional protections for sensitive data. Sensitive data is defined to include:<br>• Data revealing racial or ethnic origin, religious beliefs, mental or physical health condition or diagnosis, sex life, sexual orientation or citizenship or immigration status;<br>• The processing of genetic or biometric data for the purpose of uniquely identifying an individual;<br>• Personal data collected from a known child; or<br>• Precise geolocation data. | The UCPA defines personal data as "information that is linked or reasonably linkable to an identified individual or an identifiable individual."<br>The UCPA provides additional protections for sensitive data. Sensitive data is defined to include:<br>• Information that reveals racial or ethnic origin, religious beliefs, sexual orientation, citizenship or immigration status, or medical history, mental or physical health condition, or medical treatment or diagnosis by a health care professional;<br>• Genetic personal data or biometric data, if the processing is for the purpose of identifying a specific individual, or<br>• Specifical geolocation data. |

wiley

# U.S. State Privacy Law Guide

## 2023 Omnibus Privacy Laws

| | CPRA | VCDPA | CPA | CTDPA | UCPA |
|---|---|---|---|---|---|
| **What Individuals Are Covered?** | Consumers, defined as California residents, including employees and B2B data. | Consumers, defined as Virginia residents acting only in an individual or household context, excluding residents acting in a commercial or employment context. | Consumers, defined as Colorado residents acting only in an individual or household context, excluding individuals acting in a commercial or employment context. | Consumers, defined as Connecticut residents, excluding individuals acting in a commercial or employment context. | Consumers, defined as Utah residents acting in an individual or household context, excluding residents acting in employment or commercial context. |
| **What Rights Do Consumers Have?** | • Right to Know<br>• Right to Access/Portability<br>• Right to Correction<br>• Right to Deletion<br>• Right to Opt-Out of the Sale of personal information (for <16, must obtain opt-in)<br>• Right to Opt-Out of the Sharing of personal information for cross-context behavioral advertising (for <16, must obtain opt-in)<br>• Right to Limit/Restrict Use of Sensitive personal information<br>• Rights related to automated decision-making | • Right to Know/Access<br>• Right to Correction<br>• Right to Deletion<br>• Right to Data Portability<br>• Right to Opt-Out of targeted advertising, the sale of personal information, and certain automated profiling | • Right to Know/Access<br>• Right to Correction<br>• Right to Deletion<br>• Right to Data Portability<br>• Right to Opt-Out of targeted advertising, the sale of personal information, and certain automated profiling | • Right to Know/Access<br>• Right to Correction<br>• Right to Deletion<br>• Right to Data Portability<br>• Right to Opt-Out of targeted advertising, the sale of personal information, and certain automated profiling | • Right to Know/Access<br>• Right to Deletion<br>• Right to Data Portability<br>• Right to Opt-Out of targeted advertising and the sale of personal data |

wiley

# U.S. State Privacy Law Guide

## 2023 Omnibus Privacy Laws

| | CPRA | VCDPA | CPA | CTDPA | UCPA |
|---|---|---|---|---|---|
| **What Affirmative Obligations Do Businesses/ Controllers Have?** | • Notice/transparency<br>• Purpose specification<br>• Retention standards<br>• Opt-Out link/mechanism<br>• Risk assessments and cybersecurity audits for certain activities<br>• Training<br>• Reasonable security<br>• Certain recordkeeping<br>• No discrimination<br>• Service provider/processor contract requirements | • Notice/transparency<br>• Purpose specification<br>• Data Minimization<br>• Opt-In consent for processing sensitive data<br>• Privacy risk assessments for certain activities<br>• Reasonable security<br>• Certain recordkeeping<br>• Consumer request appeal process<br>• No discrimination<br>• Service provider/processor contract requirements | • Notice/transparency<br>• Purpose specification<br>• Data Minimization<br>• Opt-Out method and mechanism<br>• Opt-In consent for processing sensitive data<br>• Privacy risk assessments for certain activities<br>• Reasonable security<br>• Consumer request appeal process<br>• Certain recordkeeping<br>• No discrimination<br>• Service provider/processor contract requirements | • Notice/transparency<br>• Purpose specification<br>• Data Minimization<br>• Opt-Out link and mechanism<br>• Opt-In consent for processing sensitive data<br>• Privacy risk assessments for certain activities<br>• Reasonable security<br>• Consumer request appeal process<br>• Certain recordkeeping<br>• No discrimination<br>• Service provider/processor contract requirements | • Notice/Transparency<br>• Opt-Out consent for processing sensitive data<br>• Reasonable security<br>• Certain recordkeeping<br>• No discrimination<br>• Service provider/processor contract requirements |
| **How Will It Be Enforced?** | (1) Limited Private Right of Action (PRA): The PRA applies if certain (limited) personal information is the subject of a breach. **Damages are $100-$750 per consumer, per incident, or actual damages, whichever is higher.**<br><br>(2) CPPA & AG Enforcement: Enforcement by both the CPPA (the new privacy agency established by the CPRA) and the AG. **Civil penalties of $2,500-$7,500 per violation.** | The Virginia AG has exclusive enforcement authority. **Civil penalties of up to $7,500 per violation.** | The Colorado AG and district attorneys may enforce. Violations of the CPA may result in **fines of up to $20,000 per violation.** | The Connecticut AG has exclusive enforcement authority. Violations of the CTDPA may be result in civil **fines of up to $5,000 for each violation.** | The Utah AG has exclusive enforcement authority. Violations of the UCPA may result in **fines of up to $7,500 for each violation.** |