Summary of State Privacy Laws

| | California CCPA/CPRA | Virginia CDPA | Colorado CPA |
|---|---|---|---|
| **Effective date** | CCPA – in effect since January 1, 2020; enforcement began July 1, 2020<br>*CPRA – goes into effect January 1, 2023* | January 1, 2023 | July 1, 2023 |
| **Scope** | For-profit legal entities doing business in CA that collect consumers' personal data <u>and</u> (i) have gross annual revenues of over $25M; (ii) buy, receive, or sell the personal data of 50K or more CA consumers, households, or devices annually; <u>or</u> (iii) derive 50% or more of their annual revenue selling CA residents' personal data.<br>**CPRA changes the above requirements to:*<br>*For-profit legal entities doing business in CA that collect consumers' personal data <u>and</u> (i) have annual gross revenues in excess of $25M in the preceding calendar year; (ii) buy, sell, or share the personal data of **100K** or more CA consumers or households annually; <u>or</u> (iii) derive 50% or more of their annual revenue selling or sharing consumers' personal data.*<br>*- CPRA also clarifies that the law applies to businesses that generate most of their revenue from **sharing** personal data (not just selling). "Sharing" will be defined as "sharing, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to a third party for cross-* | Businesses that conduct business in VA or produce products or services targeted to residents of VA and <u>either</u> (1) control or process personal data of at least 100K VA residents in a calendar year, <u>or</u> (2) control or process personal data of at least 25K consumers and derive over 50% of gross revenue from sale of personal data. | Legal entities that conduct business or produce products/ services that are intentionally targeted to CO residents and <u>either</u> (1) control or process data from at least 100K consumers per calendar year, or (2) derive revenue from the sale of personal data of at least 25k consumers. |

| | | | |
|---|---|---|---|
| | *context behavioral advertising, whether or not for monetary or other valuable consideration, including transactions between a business and a third party for cross-context behavioral advertising for the benefit of a business in which no money is exchanged.* | | |
| **Entity exceptions/exemptions** | Non-profit companies and government agencies | Non-profit organizations, state governmental bodies, financial institutions subject to the Gramm-Leach-Bliley Act, entities subject to HIPAA, institutions of higher education | None specified |
| **Protected "consumers"** | CA residents (even if temporarily out of state) | • VA residents acting in an individual or household capacity<br>• Does not include individuals acting in a commercial or employment context | • CO residents acting only in an individual or household context<br>• Does not include individuals acting in a commercial or employment context, such as a job applicant |
| **Covered personal data** | Personal information that identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked with a consumer or household. | Any information that is linked or reasonably linkable to an identified or identifiable natural person. | Information that is linked to, or reasonably linkable to, and identified or identifiable individual. |
| **Excluded data** | • Publicly available information from government records<br>• De-identified and aggregate consumer data<br>**CPRA extends exemption for employment and B2B data until January 1, 2023.* | • De-identified data and publicly available information<br>• Information processed in connection with human resources and benefits administration, including information about employees and job applicants | • De-identified data and publicly available information<br>• Data processed in a commercial or employment context, such as a job applicant<br>• Data subject to federal privacy regulations such as |

| | | | |
|---|---|---|---|
| | | • Personal Health Information (PHI) subject to HIPAA and data subject to federal privacy regulations, such as FCRA and FERPA | Gramm-Leach-Bliley, COPPA, FERPA, and HIPAA |
| **Sensitive data requirements**<br>**(**Data pertaining to racial or ethnic origin, religious beliefs, mental or physical health condition or diagnosis, sex life or sexual orientation, citizenship or citizenship status); genetic or biometric data used to uniquely identify an individual; personal data from a known child) | No separate requirements under CCPA.<br>** CPRA imposes new requirements on the use and disclosure of sensitive data, including opt-out requirements, opt-in consent requirements for use and disclosure, and purpose limitation requirements.* | Consent required. | Prior to use, must obtain consent, or consent from the child's parent or guardian. |
| **Right to Know**<br>(Request personal data collected, shared, sold, and why it was collected, shared, or sold.) | Yes<br>**CPRA requires inclusion of personal data collected beyond the prior 12 months, if collected post 1/1/22.* | Yes | No |
| **Right of Access**<br>(Right to confirm whether a controller is processing personal data concerning the consumer and to access such personal data) | Yes<br>**CPRA adds the right to access information about automated decision making.* | Yes | Yes |
| **Right to Correction**<br>(Right to correct inaccuracies in the consumer's personal data) | Yes | Yes | Yes |
| **Right to Delete**<br>(Request that a business delete personal data that the business has collected from the consumer) | Yes (with some exceptions such as debt collectors)<br>**CPRA requires businesses who receive a request to delete a consumer's personal data to notify third parties to delete such personal data purchased or received, with some exceptions.* | Yes | Yes |
| **Right to Data Portability**<br>(Right to obtain personal data in a portable and readily usable format that allows the | Yes | Yes | Yes |

| | | | |
|---|---|---|---|
| consumer to transmit the data to another entity) | **CPRA enables consumers to request that a business transmit personal data to a third party, to the extent technically feasible to provide the personal data in a structured, commonly used, and machine-readable format.* | | |
| **Right to Opt-out**<br>(Consumers can request that a business stop selling their personal data) | Yes (must have "Do Not Sell my Personal Information" link on website and in privacy policy)<br>**CPRA extends opt-out of all "sharing" of personal data (rather than just a sale) for cross-context behavioral advertising & adds right to opt out of automated decision-making technology.* | Yes, for targeted advertising, sale of personal data, or consumer profiling | Yes, can opt out of the sale, collection, and use of personal data in some circumstances; consumer has the right to opt out of processing personal data for purposes of targeted advertising, sale of personal data, and profiling<br>Must have clear and conspicuous way for consumers to opt out, and such method must also be included in the controller's privacy policy<br>By 2024, there will be a universal opt-out method, to be created by the CO Attorney General's office and used by all controllers who sell personal data or use it for targeted advertising |
| **Rights for Minors**<br>(Business cannot sell personal data of minors without their permission (ages 13-17) and without parental consent (under age 13)) | • Yes, businesses can only sell the personal data of a minor they know to be under the age of 16 with opt-in<br>• For children under the age of 13, the opt-in must come from the minor's parent or guardian. Minors who are at least 13 can provide their own opt-ins. | Personal data of a child under 13 is treated as "sensitive data," and requires parental consent for processing and must be processed in compliance with COPPA. | Personal data of a child under 13 is treated as "sensitive data." |

| | | | |
|---|---|---|---|
| | **CPRA expressly requires opt-in for sharing of minors' personal data for cross-context behavioral advertising purposes. Businesses will need to wait 12 months before seeking consent after the minor has declined to opt-in.* | | |
| **Right to Non-Discrimination**<br>(Business cannot discriminate against consumers who exercise their privacy rights) | Yes | No | No |
| **Time to respond to consumer requests** | 45 days, with a 45-day extension with written notice to the consumer | 45 days, with a 45-day extension with written notice to the consumer | 45 days, with a 45-day extension with written notice to the consumer |
| **Consent requirements** | • Must be a freely given, specific, informed and unambiguous, indicative of the consumer's wishes by which the consumer (or the consumer's legal guardian) signifies agreement to the processing of personal data relating the consumer for a narrowly defined purpose.<br>• Consent is not achieved by a consumer's acceptance of general or broad terms of use that contain descriptions of personal data.<br>• Hovering over, muting, pausing, or closing a given piece of content does not constitute consent.<br>• An agreement obtained through use of dark patterns does not constitute consent. | • Must be a clear, affirmative act signifying a consumer's freely given, specific, informed, and unambiguous agreement to process personal data.<br>• Consent can include a written statement, including one made by electronic means, or any other unambiguous affirmative action. | • Must be a clear, affirmative act signifying the consumer's freely given, specific, informed, and unambiguous agreement.<br>• Can be in writing or by electronic means. including written statements by electronic means.<br>•Cannot use (i) broad terms of use with embedded descriptions of use of personal data; (ii) hovering over, muting, pausing, or closing a given piece of content; or (iii) agreement through dark patterns." |

| | | | |
|---|---|---|---|
| **Privacy notice required** | Yes | Yes | Yes |
| **Required data protection assessment** | **CPRA authorizes regulations to require mandatory risk assessments and cybersecurity audits for high-risk activities. Such risk assessments will be required to be submitted to the newly-created California Privacy Protection Agency.* | • Yes, for some activities such as targeted advertising, sale of personal data, some profiling, processing sensitive data, and processing that creates a "heightened risk of harm to consumers."<br>• May be requested by the VA Attorney General. | • Yes, if engaged in processing personal data that presents a "heightened risk of harm" to consumers.<br>• Results must be provided to the CO Attorney General. |
| **Private right of action for consumers** | • Yes, for data breach under some circumstances; statutory damages of up to $750 per incident.<br>• Business gets written notice and 30 days to cure. | No | No |
| **Government enforcement** | Yes, CA Attorney General. Individual consumers can file a complaint with the AG.<br>**CPRA created the California Privacy Protection Agency.* | • Yes, VA Attorney General provides written notice of violation with 30-day cure period.<br>• Statutory damages of up to $7,500 for uncured violations. | • Yes, CO Attorney General and DAs issue a written notice of violation with 60-day cure period.<br>• Civil penalties up to $2,000 per violation, not to exceed $500K for related violations, or an injunction. |
| | | | |