Comparison of Comprehensive Data Privacy Laws in Virginia, California and Colorado

By IAPP Legal Research Fellow Cathy Cosgrove and IAPP Westin Research Fellow Sarah Rippy

Created July 2021

Note: This tool is for informational purposes only and is not legal advice. Specific requirements should be verified via official sources.

	Virginia's Consumer Data Protection Act	California Consumer Privacy Act	California Privacy Rights Act	Colorado Privacy Act
KEY DATES	**Key dates.** Section 4 of H2307. • Operative Jan. 1, 2023.	**Key dates.** Section 1798.198, Section 1798.185(c). • Operative Jan. 1, 2020. • Enforcement began July 1, 2020.	**Key dates.** CPRA Ballot Initiative, Section 31, Section 1798.185(d). • Effective Dec. 16, 2020. • Most provisions are not operative until Jan. 1, 2023. Provisions operative now include certain exemptions, the Regulations provisions, and certain provision regarding the California Privacy Protection Agency. • Enforcement begins July 1, 2023.	**Key Dates.** Section 7 of Act, Section 1, 6-1-1311(1)(d), 6-1-1313(2). • Effective July 1, 2023. • Cure provision sunsets Jan. 1, 2025. • Attorney general may adopt rules prior to Jan. 1, 2025. Such rules must become effective by July 1, 2025. • Attorney general must adopt rules outlining technical specifications for universal opt-out button prior to July 1, 2023.

	Virginia's Consumer Data Protection Act	California Consumer Privacy Act	California Privacy Rights Act	Colorado Privacy Act
SCOPE	**Scope.** Section 59.1-572(A). Applies to persons that conduct business in Virginia or produce products or services that are targeted to Virginia residents and that: • Control or process personal data of at least 100,000 consumers annually. • Control or process personal data of at least 25,000 consumers and derive more than 50% of gross revenue from the sale of personal data.	**Scope.** Section 1798.140(c). Defines a "business" subject to CCPA as a for-profit entity doing business in California that collects or processes consumers' personal information and meets one or more of these thresholds: • Annual gross revenues in excess of $25,000,000. • Annually buys, receives, sells or shares the personal information of 50,000 or more consumers, households or devices. • Derives 50% or more of its annual revenues from selling consumers' personal information.	**Scope.** Section 1798.140(d). Defines a "business" subject to the CPRA as a for-profit entity doing business in California that collects or processes consumers' personal information and meets one of these thresholds: • Annual gross revenues in excess of $25,000,000 in the preceding calendar year. • Annually buys, sells or shares the personal information of 100,000 or more consumers or households. • Derives 50% or more of its annual revenues from selling or sharing consumers' personal information.	**Scope.** Section 6-1-1304(1). Applies to a controller that conducts business in Colorado or produces or delivers commercial products or services that are intentionally targeted to residents of Colorado; and • Controls or processes the personal data of 100,000 consumers or more during a calendar year; or • Derives revenue or receives a discount on the price of goods or services from the sale of personal data and processes or controls the personal data of 25,000 consumers or more.
EXEMPTIONS AND LIMITS OF APPLICABILITY	**Exemptions.** Section 59.1-572(B). CDPA does not apply to state government entities, nonprofits, institutions of higher education, financial institutions or data subject to Title V of Gramm-Leach-Bliley Act, covered entities or business associates subject to the Health Insurance Portability and Accountability Act and the Health Information Technology for Economic Clinical Health Act. Section 59.1-572(C). There are 14 categories of exempt information and data, including protected health information under HIPAA and other health-related information, data regulated by the Family Educational Rights and Privacy Act, the Fair Credit Reporting Act and others.	**Exemptions.** Section 1798.145. Contains numerous exemptions, including: Businesses can collect, use, retain, sell or disclose deidentified or aggregate consumer information. Businesses can collect or sell personal information if every aspect of that commercial conduct takes place wholly outside of California.	**Exemptions.** Section 1798.145. Like the CCPA, contains numerous exemptions, including: Businesses can collect, use, retain, sell, share or disclose deidentified or aggregate consumer information. Businesses can collect, sell or share personal information if every aspect of that commercial conduct takes place wholly outside of California.	**Exemptions.** 6-1-1304(2) The act does not apply to financial institutions or affiliates subject to the "Gramm-Leach-Bliley Act." Likewise, the law also does not apply to various other types of data including certain health care information, certain activities undertaken by a consumer reporting agency, data processed pursuant to the Gramm-Leach-Bliley Act, data regulated by the Children's Online Privacy Protection Act, data maintained for employment purposes, data maintained by a state institution of higher learning, etc.

	Virginia's Consumer Data Protection Act	California Consumer Privacy Act	California Privacy Rights Act	Colorado Privacy Act
EXEMPTIONS AND LIMITS OF APPLICABILITY	**Limitations.** Section 59.1-578. CDPA does not restrict a controller or processor from complying with laws or investigations, cooperating with law enforcement, or exercising or defending legal claims. CDPA does not restrict a controller or processor from providing a product or service specifically requested by a consumer, taking steps to protect an interest that is essential for the life or physical safety of a consumer or another natural person, protecting again security incidents, engaging in peer-reviewed scientific research, etcetera.	The CCPA does not apply to medical information or providers governed by California's Confidentiality of Medical Information Act, protected health information subject to the Health Insurance Portability and Accountability Act or a covered entity, clinical trials, information collected, processed, sold, or disclosed pursuant to the Gramm-Leach-Bliley Act, etcetera. The CCPA does not apply to information de-identified in accordance with HIPAA (Section 1798.146).	The CPRA does not apply to medical information or providers governed by California's Confidentiality of Medical Information Act, protected health information subject to the Health Insurance Portability and Accountability Act or a covered entity, clinical trials, information collected, processed, sold or disclosed subject to the Gramm-Leach-Bliley Act, etcetera. **NOTE:** CCPA Section 1798.146 is not included in the CPRA ballot initiative, as it was a September 2020 amendment to the CCPA.	
KEY DEFINITIONS	**Definitions.** Section 59.1-571. **Consumer** means a natural person who is a Virginia resident acting in an individual or household context. Acting in a commercial or employee context is specifically excluded from the definition. **Controller** means the natural or legal person that determines the purpose and means of processing personal data. **Personal data** means any information that is linked or reasonably linked to an identified or identifiable natural person. It does not include deidentified data or publicly available information (a separately defined term).	**Definitions.** Section 1798.140. **Consumer** means a natural person who is a California resident, as defined in Section 17014 of Title 18 of the California Code of Regulations, as that section read Sept. 1, 2017. In addition to "business," the CCPA uses the terms "**service provider**" (a for profit entity that processes information on behalf of a business pursuant to a written contract) and "**third party**" (defined in the negative as a person who is not a business that collects personal information or subject to service-provider type contractual requirements).	**Definitions.** Section 1798.140. **Consumer** means a natural person who is a California resident, as defined in Section 17014 of Title 18 of the California Code of Regulations, as that section read Sept. 1, 2017. **Contractor** means a person to whom the business makes available a consumer's personal information for a business purpose, pursuant to a written contract. The contractual requirements are similar to those for service providers, but a contractor must certify it understands the contractual restrictions and will comply with them. The contract also must permit the business to monitor the contractor's compliance.	**Definitions.** Section 6-1-1303. **Consumer** means an individual who is a Colorado resident acting only in an individual or household context. Explicitly excludes individuals acting in a commercial or employment context, as a job applicant, or as a beneficiary of someone acting in an employment context. **Controller** means a person that, alone or jointly with others, determines the purposes for and means of processing personal data. **Personal data** means information that is linked or reasonably linkable to an identified or identifiable individual. Explicitly excludes publicly available information (defined separately).

	Virginia's Consumer Data Protection Act	California Consumer Privacy Act	California Privacy Rights Act	Colorado Privacy Act
KEY DEFINITIONS	**Sensitive data** means a category of personal data that includes data revealing racial or ethnic origin, religious beliefs, physical or mental health diagnosis, sexual orientation, or citizen or immigrant status, as well as processing of genetic or biometric data for identification, precise geolocation data, and personal data collected from a known child. **Sale of personal data** means the exchange of personal data for monetary consideration by the controller to a third party. It does not include disclosure (1) to a processor processing data on behalf of the controller; (2) to a third party for purposes of a product or service requested by the consumer; (3) to a controller's affiliate; (4) of information a consumer intentionally made available to the general public via mass media and did not restrict to a specific audience; and (5) to a third party as an asset that is part of a business transaction where the third party assumes control of the controller's assets.	**Personal information** is defined broadly as information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. It does not include publicly available information or deidentified or aggregate consumer information. **Sale** means selling, renting, releasing, disclosing, disseminating, making available or transferring a consumer's personal information by the business to another business or a third party for monetary or other valuable consideration.	**Service provider** means a person that processes personal information on behalf of a business pursuant to a written contract, if the contract includes certain restrictions, including prohibiting selling or sharing the personal information, using the information for any purpose other than those specified in the contract, using the information outside of the direct business relationship, and combining personal information except under certain circumstances. The contract may permit the business to monitor the service provider's compliance. **Third party** means a person who is not a contractor, a service provider or a business that collects personal information from the consumer. *See Section 1798.100(d) regarding contractual requirements for service providers, contractors and third parties. **Personal information** is defined broadly as information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. It does not include publicly available information or deidentified or aggregate consumer information.	**Processor** means a person that processes personal data on behalf of a controller. **Sensitive data** means personal data revealing racial or ethnic origin, religious beliefs, a mental or physical health condition or diagnosis, a person's sex life or sexual orientation, citizenship, or citizenship status, as well as genetic or biometric data that may be processed for the purpose of uniquely identifying an individual. The definition also includes personal data from a known child. **Sale** means the exchange of personal data for monetary or other valuable consideration by a controller to a third party. It does not include (1) disclosures to processors, (2) disclosures to a third party for purposes of providing a product or service requested by the consumer, (3) disclosure or transfer of personal data to an affiliate of the controller, (4) disclosure or transfer to a third party of personal data as an asset in a transaction in which the third party assumes control of the controller's assets, (5) disclosure of personal data per the direction of the consumer.

	Virginia's Consumer Data Protection Act	California Consumer Privacy Act	California Privacy Rights Act	Colorado Privacy Act
KEY DEFINITIONS			**Sensitive personal information** means personal information that reveals certain information about a consumer. The specific categories of sensitive personal information are listed in the statute and include items like Social Security, driver's license, state identification card or passport numbers, account log-in, financial account, debit card or credit card numbers in combination with any required security or access code, password or credentials allowing access to an account, and precise geolocation. *Note: This is not a complete list. **Sale** means selling, renting, releasing, disclosing, disseminating, making available or transferring a consumer's personal information by the business to a third party for monetary or other valuable consideration. **Sharing** means sharing, renting, releasing, disclosing, disseminating, making available or transferring a consumer's personal information by the business to a third party for cross-context behavioral advertising, whether or not for monetary or other valuable consideration. **Cross-context behavioral advertising** means the targeting of advertising to a consumer based on the consumer's personal information obtained from the consumer's activity across businesses, distinctly branded websites, etcetera.	

	Virginia's Consumer Data Protection Act	California Consumer Privacy Act	California Privacy Rights Act	Colorado Privacy Act
CONSUMER RIGHTS	Section 59.1-573(A). **Right to Know** whether a controller is processing the consumer's personal data. **Right to Access** personal data processed by a controller. **Right to Correct**. **Right to Delete**. **Right to Data Portability**. **Right to Opt Out** of **targeted advertising**, **the sale of personal data or profiling**.	**Right to Know** what personal information is collected and **Right to Access** personal information. Section 1798.100, Section 1798.110. **Right to Know if Personal Information is Sold**. Section 1798.115. **Right to Delete**. Section 1798.105, subject to certain exceptions. **Right to Data Portability**. Section 1798.100(d), Section 130(a)(2). **Right to Opt Out of Sale**. Section 1798.120.	**Right to Know what Personal Information is Being Collected** and **Right to Access** personal information. Section 1798.110. **Right to Know what Personal Information is Sold or Shared and to Whom**. Section 1798.115. **Right to Correct**. Section 1798.106. **Right to Delete**. Section 1798.105, subject to certain exceptions. **Right to Data Portability**. Section 1798.130(a)(3)(B)(iii). **Right to Opt Out of Sale or Sharing**. Section 1798.120. Definition of sharing includes "cross-context behavioral advertising," a separately defined term. **Right to Limit Use and Disclosure of Sensitive Personal Information**. Section 1798.121. **NOTE:** The CPRA generally expands on or modifies the existing CCPA rights.	Section 6-1-1306. **Right of access**. A consumer has the right to confirm whether a controller is processing Personal data concerning the consumer and to access such data. **Right to Correction**. **Right to Deletion**. **Right to Data Portability**. **Right to Opt out of targeted advertising, the sale of personal data, or profiling via a universal opt-out mechanism.**
OBLIGATIONS	**Controllers.** **Data Minimization.** Section 59.1-574(A)(1). Controllers are required to limit the collection of personal data to what is adequate, relevant and reasonably necessary.	**Businesses.** **Opt-Out Methods.** Section 1798.135. A business that sells personal information about consumers to third parties is required to provide a clear and conspicuous link on its internet homepage titled "Do Not Sell My Personal Information" to a webpage that enables a consumer to opt out of the sale. A business is prohibited from requiring a consumer to create an account to opt out.	**Businesses.** **Methods of Limiting Sale, Sharing and Use of Personal Information and Sensitive Personal Information.** Section 1798.135. A business that sells or shares personal information or uses or discloses sensitive personal information for purposes other than those authorized by 1798.121(a) is required to:	**Controllers.** **Duty of Data Minimization.** 6-1-1308(3). A controller's collection of personal data must be adequate, relevant, and limited to what is reasonably necessary in relation to the specified purposes for which the data are processed.

	Virginia's Consumer Data Protection Act	California Consumer Privacy Act	California Privacy Rights Act	Colorado Privacy Act
OBLIGATIONS	**Purpose Limitation.** Section 59.1-574(A)(2). Controllers are prohibited from processing personal data for purposes that are neither reasonably necessary to nor compatible with the disclosed purposes for which the personal data is processed unless the controller obtains the consumer's consent. **Reasonable Data Security.** Section 59.1-574(A)(3). Controllers are required to establish, implement and maintain reasonable administrative, technical and physical data security practices to protect the confidentiality, integrity and accessibility of personal data. **Sensitive Data.** Section 59.1-574(A)(5). Controllers are prohibited from processing sensitive data without obtaining the consumer's consent or, in the case of processing sensitive data concerning a known child, without following the Children's Online Privacy Protection Act.	**Purpose Limitation.** Section 1798.100(b). A business shall not collect additional categories of personal information or use personal information collected for additional purposes without providing notice. **Reasonable Security Procedures.** Section 1798.150, the Private Right of Action provision, references a business's duty to implement and maintain reasonable security procedures and practices. **Required Notices.** Section 1798.100, notice at collection; Section 1798.120, notice of right to opt-out of sale; Section 1798.125, notice of financial incentive. See also CCPA Reg. Section 999.304, requiring notice at collection, notice of right to opt-out, notice of financial incentive. **Privacy Notice Required.** CCPA Reg. Section 999.304(a) requires businesses to provide a privacy policy in accordance with Section 999.308. Section 1798.130(a)(5) requires certain information be disclosed in a business's online privacy policy and in any California-specific description of consumer's privacy rights or on its website, including a description of a consumer's rights and one or more methods for submitting requests, as well as disclosures required by Section 1798.110 and Section 1798.115.	• Provide a clear and conspicuous link on its internet homepage titled "Do Not Sell or Share My Personal Information" to a webpage that enables a consumer to opt-out of the sale or sharing. • Provide a clear and conspicuous link on its internet homepage titled "Limit the Use of My Sensitive Personal Information" that enables a consumer to limit the use or disclosure of the consumer's sensitive personal information. A business can use one link to opt out of the sale or sharing and limit the use of sensitive personal information. A business is prohibited from requiring a consumer to create an account to opt out or limit the use of sensitive personal information. **Data Minimization.** Section 1798.100(a)(3). Prohibits a business from retaining a consumer's personal information or sensitive personal information for longer than is reasonably necessary for that disclosed purpose.	**Duty of Purpose Specification.** 6-1-1308(2). A controller shall specify the express purposes for which personal data are collected and processed. **Duty to avoid secondary use.** 6-1-1308(4). A controller shall not process personal data for purposes that are not reasonably necessary to or compatible with the specified purposes for which the personal data are processed, unless the controller first obtains the consumer's consent. **Duty of Care.** 6-1-1308(5). A controller shall take reasonable measures to secure personal data during both storage and use from unauthorized acquisition. **Duty regarding sensitive data.** 6-1-1308(7). A controller shall not process a consumer's sensitive data without first obtaining the consumer's consent.

	Virginia's Consumer Data Protection Act	California Consumer Privacy Act	California Privacy Rights Act	Colorado Privacy Act
OBLIGATIONS	**Privacy Notice Required.** Section 59.1-574(C). Controllers are required to provide consumers with a reasonably accessible, clear and meaningful privacy notice that includes (1) the categories of personal data processed by the controller; (2) the purpose for processing personal data; (3) how consumers may exercise their consumer rights, including appeal of a controller's decision; (4) categories of personal data shared with third parties; and (5) categories of third parties with whom the controller shares personal data. **Disclosure if Sales to Third Parties or Targeted Advertising.** Section 59.1-574(D) requires disclosures if a controller sells personal data to third parties or processes personal data for targeted advertising. **No Discrimination.** Section 59.1-574(A)(4). A controller cannot process personal data in violation of state and federal consumer anti-discrimination laws or discriminate against a consumer for exercising rights under the CDPA.	**No Discrimination.** Section 1798.125 prohibits businesses from discriminating against consumers for exercising their rights. Examples are listed in the provision. Pursuant to Section 1798.125(b), a business may offer financial incentives for the collection, sale or deletion of personal information. A business may also offer a different price, rate, level or quality of goods or services to the consumer if that price or difference is directly related to the value provided to the business by the consumer's data. Consumers are entitled to notice of any financial incentives and a business may enter a consumer into a financial incentive program only if the consumer gives prior opt-in consent.	**Purpose Limitation.** Section 1798.100(a)(1) includes same provision as in CCPA Section 1798.100(b). Also Section 1798.100(c) requires that a business's collection, use, retention and sharing of a consumer's personal information be reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed, or for another disclosed purpose that is compatible with the context in which the personal information was collected. **Reasonable Security Procedures.** Section 1798.100(e). A business that collects a consumer's personal information is required to implement reasonable security procedures and practices in accordance with Section 1798.81.5. Also Section 1798.150, the Private Right of Action provision, references a business' duty to implement and maintain reasonable security procedures and practices. **Sensitive Data.** Section 1798.121(b). A business that has received direction from a consumer not to use or disclose the consumer's sensitive personal information is prohibited from doing so.	**Duty of Transparency (Privacy Notice).** 6-1-1308(1). Controllers must provide consumers with a reasonably accessible, clear, and meaningful privacy notice that includes: (1) the categories of personal data collected or processed by a controller or processor; (2) the purposes for which the categories of personal data are processed; (3) how and where consumers may exercise their rights; (4) the categories of personal data that the controller shares with third parties and; (5) the categories of third parties with whom the controller shares personal data. **Required disclosure of sale.** 6-1-1308(1)(b). If a controller sells personal data to third parties or processes personal data for targeted advertising, the controller shall clearly and conspicuously disclose the sale or processing, as well as the manner in which a consumer may opt out. **Duty to avoid unlawful discrimination.** 6-1-1308(6). A controller shall not process personal data in violation of state or federal laws that prohibit unlawful discrimination against consumers.

	Virginia's Consumer Data Protection Act	California Consumer Privacy Act	California Privacy Rights Act	Colorado Privacy Act
OBLIGATIONS	A controller is not prohibited from offering a different price, rate, level, quality or selection of goods or services to a consumer, including offering goods or services for no fee, if the consumer has exercised the right to opt out pursuant to Section 59.1-573 or the offer is related to a consumer's voluntary participation in a bona fide loyalty, rewards, premium features, discounts or club card program. **No Contractual Limitations.** Section 59.1-574(B). Any provision of a contract or agreement that purports to waive or limit in any way consumer rights in Section 59.1-573 shall be deemed contrary to public policy and shall be void and unenforceable.	CCPA Reg. Section 999.337 requires a business offering a financial incentive or price or service difference to use and document a reasonable and good faith method for calculating the value of the consumer's data. Examples are listed.	**Required Notices.** Section 1798.100, notice at collection, broadened to include sensitive personal information and retention information; Section 1798.120, notice of right to opt out of sale and sharing; Section 1798.121, notice regarding sensitive personal information required under certain circumstances; Section 1798.125, notice of financial incentive. Section 1798.130(a)(5) requires certain information be disclosed in a business's online privacy policy and in any California-specific description of consumer's privacy rights or on its website, including a description of a consumer's rights and two or more methods for submitting requests, as well as disclosures required by Sections 1798.110 and 1798.115. **No Discrimination.** Section 1798.125 prohibits businesses from discriminating against consumers for exercising their rights. Examples are listed in the provision. Section 1798.125(b) permits a business to offer financial incentives for the collection, sale or sharing of personal information, or the retention of personal information. A business may also offer a different price, rate, level or quality of goods or services to the consumer if that price or difference is reasonably related to the value provided to the business by the consumer's data.	

	Virginia's Consumer Data Protection Act	California Consumer Privacy Act	California Privacy Rights Act	Colorado Privacy Act
OBLIGATIONS			Consumers are entitled to notice of any financial incentives and a business may enter a consumer into a financial incentive program only if the consumer gives prior opt-in consent. If a consumer refuses to provide opt-in consent, then the business must wait at least 12 months before next requesting opt-in consent. Section 1798.125(a)(3). A business may offer loyalty, rewards, premium features, discounts or club card programs.	
ROLE OF PROCESSOR/SERVICE PROVIDER/ THIRD PARTY AND CONTRACTUAL REQUIREMENTS	**Role of Processors.** Section 59.1-575. Processors are required to follow a controller's instructions and assist the controller in meeting its obligations. A contract is required between the controller and the data processor to govern the processor's data processing procedures. The contract also needs to require that processors: 1. Ensure each person processing personal data is subject to a duty of confidentiality. 2. At the controller's direction, delete or return all personal data to the controller as requested after providing services, unless retention is required by law.	*See definitions of **Service Provider** and **Third Party**. **Service Provider** definition, Section 1798.140(v), includes requirement that there be a contract that prohibits the service provider from using the personal information for any purpose other than for the specific contractual purpose or using the personal information for a different commercial purpose. **Third Party**, Section 1798.140(w), is defined in the negative as a person who is not a business that collects personal information or subject to service-provider type contractual requirements, including those that prohibit the person from:	*See definitions of **Service Provider, Contractor** and **Third Party**. **Contractual Requirements.** Section 1798.100(d). A business that collects a consumer's personal information and sells it to or shares it with a third party or discloses it to a service provider or contractor for a business purpose is required to enter into an agreement with the third party, service provider or contractor that includes specific listed terms. **Definitions of Contractor/Service Provider** in Section 1798.140 require contracts that prohibit:	**Processor Obligations** 6-1-1305(2). Processors are required to adhere to the instructions of the controller and assist the controller in meeting its obligations by: (1) taking appropriate measures to assist the controller in responding to consumer requests to exercise their rights; (2) helping meet the controller's security obligations in relation to breach notification and system security and (3) providing information to the controller necessary to enable the controller to conduct and document any data protection assessments required. Additionally, processing by a processor must be governed by a binding contract between the processor and controller that sets out:

	Virginia's Consumer Data Protection Act	California Consumer Privacy Act	California Privacy Rights Act	Colorado Privacy Act
ROLE OF PROCESSOR/SERVICE PROVIDER/THIRD PARTY AND CONTRACTUAL REQUIREMENTS	3. Make available to the controller, at its request, all information in its possession necessary to demonstrate the processor's compliance with the obligations in the CDPA. 4. Allow and cooperate with reasonable assessments by the controller or arrange for a qualified and independent assessor to conduct an assessment of the processor's policies and technical and organizational measures, providing a report of such assessment to the controller upon request. 5. Engage any subcontractor pursuant to a written contract that requires the subcontractor to meet the obligations of the processor with respect to the personal data. Whether a person is acting as a controller or processor is a fact-based determination that depends upon the context in which personal data is to be processed. A processor that continues to adhere to a controller's instructions with respect to a specific processing of personal data remains a processor.	1. Selling the personal information. 2. Using the personal information for any purpose other than specified in the contract. 3. Using the information outside of the business relationship.	1. Selling or sharing personal information. 2. Using personal information for any purpose other than for the business purpose specified in the contract. 3. Using personal information outside of the direct business relationship. 4. Combining the personal information with other personal information, subject to certain exceptions. 5. For contractors, includes a certification it understands the restrictions. 6. Permits a business to monitor compliance.	1. Instructions, including the nature and purpose of the processing, to which the processor is bound. 2. The duration of processing and the type of personal data subject to the processing. 3. The requirement that each person processing the personal data is subject to a duty of confidentiality with respect to the data. 4. The requirement that a controller may only use a subcontractor pursuant to a contract requiring the subcontractor to meet the processor's obligations with respect to the data. The processor must also provide the controller with an opportunity to object. 5. The allocation of responsibility between the controller and processor for maintaining technical and organizational and technical measures to ensure appropriate security. 6. Whether the controller requires the processor return or delete all personal data to the controller at the end of the provision of services, unless that retention is required by law. 7. That the processor shall make all information necessary to demonstrate compliance with this law available to the controller.

	Virginia's Consumer Data Protection Act	California Consumer Privacy Act	California Privacy Rights Act	Colorado Privacy Act
ROLE OF PROCESSOR/SERVICE PROVIDER/THIRD PARTY AND CONTRACTUAL REQUIREMENTS				8. The processor shall allow for, and contribute to, reasonable audits and inspections by the controller or auditor. In no event may a contract relieve a controller or processor from the duties imposed by the CPA. Whether a person is acting as a controller or processor is a fact-based determination that depends upon the context in which personal data are to be processed. A person that would otherwise be a processor that is not limited to its processing of personal data pursuant to a controller's instructions, or that fails to adhere to the instructions, becomes controller. If a processor begins determining the purposes and means of the processing of personal data, it becomes a controller. A controller or processor is not liable for violations where it properly disclosed data to another controller or processor who subsequently processed the personal data in violation of the CPA so long as the disclosing party did not have actual knowledge that the recipient intended to commit a violation. A recipient of personal data does not violate the CPA if the disclosing party from which it receives the data violates the CPA.

	Virginia's Consumer Data Protection Act	California Consumer Privacy Act	California Privacy Rights Act	Colorado Privacy Act
ACCESS REQUESTS	**Access Requests.** Section 59.1-574(E). Controllers are required to establish and describe in a privacy notice one or more secure and reliable means for consumers to submit a request to exercise their rights. The method used needs to consider how consumers normally interact with the controller, the need for secure and reliable communication of such requests, and the ability of the controller to authenticate the requests. Controllers are prohibited from requiring a consumer to create a new account in order to exercise their consumer rights but may require a consumer to use an existing account. **45 days to respond.** Section 59.1-573(B)(1). Controllers are required to respond to consumer requests within 45 days. This time period may be extended once by 45 additional days if certain requirements are met. **No charge for information.** Section 59.1-573(B)(3). Controllers are required to provide information in response to a consumer request free of charge, up to twice annually per consumer. The controller may charge the consumer a reasonable fee or decline to act on the request if requests are manifestly unfounded, excessive or repetitive, but the burden of demonstrating the manifestly unfounded, excessive or repetitive nature of the request is on the controller.	**Submitting Requests.** Section 1798.130. Businesses need to make available to consumers two or more designated methods for submitting requests for information, including, at a minimum, a toll-free telephone number. A business that operates exclusively online and has a direct relationship with a consumer from whom it collects personal information is only required to provide an email address for submitting requests. The business may require authentication of the consumer but shall not require the consumer to create an account with the business to make a verifiable consumer request. If the consumer has an account with the business, the consumer may be required to use that account to submit a request. **45 days to respond.** Businesses are required to disclose and deliver the required information to a consumer within 45 days of receiving a verifiable consumer request. This time period may be extended once by an additional 45 days when reasonably necessary, provided the consumer is provided notice of the extension within the first 45-day period. **No charge for information.** The business must deliver the requested information free of charge.	**Notice, Disclosure, Correction and Deletion Requirements.** Section 1798.130. Make available to consumers two or more designated methods for submitting requests for information or requests for deletion or correction, including, at a minimum, a toll-free telephone number. A business that operates exclusively online and has a direct relationship with a consumer from whom it collects personal information shall only be required to provide an email address for submitting requests. The business may require authentication of the consumer, but shall not require the consumer to create an account with the business in order to make a verifiable consumer request. If the consumer has an account with the business, it may require the consumer to use that account to submit a request. **45 days to respond.** Businesses are required to disclose and deliver the required information to a consumer, correct inaccurate personal information or delete a consumer's personal information within 45 days of receiving a verifiable consumer request. This time period may be extended once by an additional 45 days when reasonably necessary, provided the consumer is provided notice of the extension within the first 45-day period.	**Access Requests.** Section 6-1-1306(1). Consumers may exercise their rights by submitting a request using a method specified by the controller in the required privacy notice. The method must take into account: (1) the ways in which consumers normally interact with the controller; (2) the need for secure and reliable communication relating to the request; and (3) the ability of the controller to authenticate the identity of the consumer making the request. Controllers shall not require a consumer to create a new account in order to exercise consumer rights. However, a controller may require a consumer to use an existing account. **45 days to respond.** Section 6-1-1306(2). A Controller shall inform a consumer of any action taken on a request within 45 days. In certain circumstances, this 45-day window to respond may be extended by an additional 45 days. **No charge for information.** 6-1-1306(2)(c). Controllers are required to provide the information requested free of charge once per year. For additional requests within a 12-month period, the controller may charge an additional amount.

	Virginia's Consumer Data Protection Act	California Consumer Privacy Act	California Privacy Rights Act	Colorado Privacy Act
ACCESS REQUESTS	**Justification for failure to act.** Section 59.1-573(B)(2). If a controller declines to act regarding the consumer's request, the controller shall inform the consumer why within 45 days and provide instructions for how to appeal the decision. **Denial of requests.** Section 59.1-573(B)(4). If a controller is unable to authenticate the request using commercially reasonable efforts, the controller shall not be required to comply with a request to initiate an action and may request additional information reasonably necessary to authenticate the consumer and the consumer's request. **Right to appeal.** Section 59.1-573(C). A controller is required to establish a process for a consumer to appeal its refusal to act on a request, and if the appeal is denied, an online mechanism or other method for the consumer to contact the attorney general to submit a complaint.	Pursuant to Section 1798.145(i)(3), if requests from a consumer are manifestly unfounded or excessive, a business may either charge a reasonable fee or refuse to act on the request. The business shall bear the burden of demonstrating any verified consumer request is manifestly unfounded or excessive. **Inform consumer why no action.** Section 1798.145(i)(2). If the business does not act on the consumer's request, it shall inform the consumer of its reasons and any rights the consumer may have to appeal the decision to the business.	**No charge for information.** The business must deliver the requested information free of charge. Pursuant to Section 1798.145(h)(3), if requests from a consumer are manifestly unfounded or excessive, a business may either charge a reasonable fee or refuse to act on the request. The business shall bear the burden of demonstrating any verifiable consumer request is manifestly unfounded or excessive. **Inform consumer why no action.** Section 1798.145(h)(2). If the business does not act on the consumer's request, the business shall inform the consumer of its reasons and any rights the consumer may have to appeal the decision to the business.	**Justification for failure to act.** 6-1-1306(2)(b) If a controller does not take action as requested by a consumer, the controller shall inform the consumer within 45 days after receipt of request of the reasons for not taking action and instructions for how to appeal the decision. **Denial of requests.** 6-1-1306(2)(d). A controller is not required to comply with a request to exercise any of the consumer's rights if the controller is unable to authenticate the request using commercially reasonable efforts and may request the provision of additional information reasonably necessary to authenticate the request. **Right to appeal.** 6-1-1306(3)(a). A controller shall establish an internal process whereby consumers may appeal a refusal to take action on a consumer request. Where a consumer wishes to appeal, they must do so within a reasonable time period after the controller notifies them that the controller is denying the request. The appeal process must be conspicuously available and easy to use. **Responding to an appeal.** 6-1-1306(3)(b). A controller shall inform the consumer of the result of the appeal as well as provide written explanation of the reasons in support of the outcome within 45 days of receipt of the appeal. This 45-day period may be extended by an additional 60 in certain circumstances.

	Virginia's Consumer Data Protection Act	California Consumer Privacy Act	California Privacy Rights Act	Colorado Privacy Act
TREATMENT OF MINORS	**Minors.** Section 59.1-572(D). Controllers and processors that comply with the verifiable parental consent requirements of COPPA shall be deemed compliant with any obligation to obtain parental consent under the CDPA. Section 59.1-573(A). A known child's parent or legal guardian may invoke consumer rights on behalf of the child regarding processing personal data belonging to the known child.	**Minors.** Section 1798.120(c). A business shall not sell the personal information of consumers if the business has actual knowledge the consumer is less than 16, unless the consumer, in the case of consumers at least 13 and less than 16, or the consumer's parent or guardian, in the case of consumers who are less than 13, has affirmatively authorized the sale of the consumer's personal information. A business that willfully disregards the consumer's age shall be deemed to have had actual knowledge of the consumer's age. This right may be referred to as the "right to opt-in." Section 1798.120(d). A business that has not received consent to sell the minor consumer's personal information shall be prohibited from selling the personal information unless the consumer subsequently provides express authorization. **NOTE:** See also CCPA Regs. Sections 999.330, 331, 332 for Special Rules Regarding Consumers Under 16 Years of Age.	**Minors.** Section 1798.120(c). A business shall not sell or share the personal information of consumers if the business has actual knowledge the consumer is less than 16, unless the consumer, in the case of consumers at least 13 and less than 16, or the consumer's parent or guardian, in the case of consumers who are less than 13, has affirmatively authorized the sale or sharing of the consumer's personal information. A business that willfully disregards the consumer's age shall be deemed to have had actual knowledge of the consumer's age. Section 1798.120(d). A business that has not received consent to sell or share the minor consumer's personal information shall be prohibited from selling or sharing the personal information unless the consumer subsequently provides consent.	**Minors.** 6-1-1308(7). A controller shall not process the personal data of a known child without first obtaining consent from the child's parent or lawful guardian.

	Virginia's Consumer Data Protection Act	California Consumer Privacy Act	California Privacy Rights Act	Colorado Privacy Act
DATA PROTECTION ASSESSMENTS	**Data Protection Assessments.** Section 59.1-576. Controllers are required to conduct and document a data protection assessment for each of the following processing activities involving personal data: 1. Targeted advertising. 2. Sale of personal data. 3. Profiling in certain circumstances. 4. Sensitive data. 5. Processing activities that present a heightened risk of harm to consumers. The statute provides further information regarding the requirements for data protection assessments. The attorney general may request and evaluate a controller's data protection assessment for compliance.	**NOTE:** CPRA Section 1798.185 is now operative.	**Data Protection Assessments.** Section 1798.185(a)(15). Provides for regulations requiring businesses whose processing of consumers' personal information presents significant risk to consumers' privacy or security, to: 1. Perform an annual cybersecurity audit. 2. Submit a risk assessment with respect to their processing of personal information to the CPPA, including whether the processing involves sensitive personal information, and identifying and weighing the benefits resulting from the processing against the potential risks, with the goal of restricting or prohibiting the processing if the risks to privacy of the consumer outweigh the benefits resulting from processing to the consumer, the business, other stakeholders and the public.	**Data Protection Assessments.** 6-1-1309. A controller must conduct a data protection assessment when conducting processing activities that present a heightened risk of harm. Processing that presents "a heightened risk of harm" to a consumer includes: 1. Targeted advertising where profiling presents a risk of a. Unfair or deceptive treatment of, or unlawful or disparate impact on consumers. b. Financial or physical injury to consumers. c. An intrusion upon a consumer's solitude or seclusion, or the private affairs or concerns of the consumer if such an intrusion would be offensive to a reasonable person. d. Other substantial injury to consumers. 2. Selling personal data. 3. Processing sensitive data. Controllers must make the data protection assessments available to the Attorney General upon request. The Attorney General may then evaluate the assessment for compliance.

	Virginia's Consumer Data Protection Act	California Consumer Privacy Act	California Privacy Rights Act	Colorado Privacy Act
ENFORCEMENT AND PENALTIES	**Attorney General Investigative and Enforcement Authority.** Section 59.1-579 and Section 59.1-580. The attorney general has investigative authority and exclusive authority to enforce violations of the CDPA. The CDPA specifically states there is no private right of action. Prior to initiating any action, the attorney general is required to provide the controller or processor a 30-day period to cure the alleged violation. If the controller or processor fails to cure the alleged violation, the attorney general may initiate an action and seek an injunction and civil penalties of up to $7,500 for each violation. The attorney general may recover reasonable expenses incurred in investigating and preparing the case, including attorney fees.	**Attorney General Enforcement.** Section 1798.155. Businesses have 30 days to cure alleged noncompliance before being in violation of the law. Businesses also may seek the opinion of the attorney general for guidance on compliance. A business, service provider or other person that violates the law is subject to an injunction and liable for a civil penalty of not more than $2,500 for each violation or $7,500 for each intentional violation, to be assessed and recovered in a civil action brought by the attorney general. **Private Right of Action.** Section 1798.150. Any consumer whose nonencrypted and nonredacted personal information, as defined in California's data breach law, Section 1798.81.5(d)(1)(A), is subject to an unauthorized access and exfiltration, theft or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices may bring a civil action. Consumers may recover injunctive or declaratory relief and damages in an amount not less than $100 and not greater than $750 per consumer per incident or actual damages, whichever is greater.	**Attorney General Enforcement.** Section 1798.199.90. Any business, service provider, contractor or other person that violates this title shall be subject to an injunction and liable for a civil penalty of not more than $2,500 for each violation or $7,500 for each intentional violation and each violation involving the personal information of minor consumers, to be assessed and recovered in a civil action brought by the attorney general. **Administrative Enforcement.** Section 1798.199.10 et seq. Establishes the CPPA, which has an enforcement function. Section 1798.155 provides any business, service provider, contractor or other person that violates this title shall be subject to an administrative fine of not more than $2,500 for each violation or $7,500 for each intentional violation or violations involving the personal information of consumers the business, service provider, contractor or other person has actual knowledge are under 16 years of age, in an administrative enforcement action brought by the CPPA.	**Attorney General and District Attorneys Enforcement.** 6-1-1311. The attorney general and district attorneys have exclusive authority to enforce the CPA. They may do so by bringing an action in the name of the state or on behalf of persons residing in the state. The CPA specifies that there is no private right of action. Pursuant to a sunset provision expiring Jan. 1, 2025, the attorney general is required to provide the controller or processor a 60-day period to cure the alleged violation prior to bringing an action. After January 1, 2025, no cure period is provided. Violations of the CPA constitute deceptive trade practices and therefore are subject to a $20,000 per violation fine pursuant to the Colorado Consumer Protection Act, C.R.S. 6-1-112(1)(a).

	Virginia's Consumer Data Protection Act	California Consumer Privacy Act	California Privacy Rights Act	Colorado Privacy Act
ENFORCEMENT AND PENALTIES		In an action for statutory damages, consumers are required to provide a business 30 days' written notice of the alleged violation and if the alleged violation is cured, no action for individual statutory damages can be brought.	**Private Right of Action.** Section 1798.150. Any consumer whose nonencrypted and nonredacted personal information, as defined in California's data breach law, Section 1798.81.5(d)(1)(A), or whose email address in combination with a password or security question and answer that would permit access to the account is subject to an unauthorized access and exfiltration, theft or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices may bring a civil action. Consumers may recover injunctive or declaratory relief and damages in an amount not less than $100 and not greater than $750 per consumer per incident or actual damages, whichever is greater. In an action for statutory damages, consumers are required to provide a business 30 days' written notice of the alleged violation and if the alleged violation is cured, no action for individual statutory damages can be brought.	