	CCPA requirements (as amended by the CPRA)	CDPA requirements
Data subject rights (of authenticated/verified consumers)		
Right to know/access	Consumers have the **right to know** what personal information has been **collected**, from **where**, and **why**, and to whom that information is disclosed (selling or sharing).	Consumers have the **right to confirm** whether a controller is processing personal data, **and to access** such data.
Right to correct/rectify	Under the CPRA, consumers can have the business correct inaccurate data.	Consumers have the right to correct inaccurate data.
Right to portability	Consumers have a right to a copy of their personal information in a **structured, commonly used, exportable format.**	Consumers have a right to receive a copy of their personal data **in a usable format that can be transferred** to another controller.
Right to delete	Consumers can request that a business delete personal information that was collected from the consumer.	Consumers can request that a business delete personal data provided by or obtained about them.
Right to restrict or opt out of use	A consumer shall have the right, at any time, to opt out of a business's sale or sharing (for cross-contextual advertising) of their personal information.	Under the statute, a consumer shall have the right to: - Opt out of the processing of personal data for the purposes of targeted advertising - Restrict the processing of personal data in certain circumstances
Right to nondiscrimination	A business shall not discriminate against a consumer for exercising their rights.	Controllers are prohibited from discriminating against a consumer for exercising their rights.
Scope		
Application	Applies to "businesses" that both conduct business in CA and: - Have collected data of more than 50,000 residents (under CCPA)/ 100,000 residents (under CPRA); or - Have a gross revenue of more than $25 million; or - Derive more than 50% of revenue from sale or sharing (under CPRA) of personal data The CPRA explicitly expands coverage to joint ventures and partnerships.	Applies to any "legal entity" that conducts business in VA or produces products/services that are targeted to VA residents and: - Controls or processes data of 100,000 VA residents within a calendar year; or - Controls or processes data of 25,000 residents and derives over 50% of revenue from the sale of personal data.

Exemptions	Certain categories of information (including information regulated under HIPAA and the GLBA) are exempt from the requirements of the statutes.	The CDPA does not apply to: - Individuals acting in a **commercial or employment context** - State and local governments - Entities that are subject to GLBA or HIPAA regulation
Definitions		
Personal information and personal data	"Personal information" is information that identifies, relates to, describes, is capable of being associated with, or could be reasonably linked, directly or indirectly, with a specific consumer or household. - Excludes deidentified information or aggregate consumer information - Excludes publicly available information that is from federal, state, or local government records, such as professional licenses and public real estate/property records	"Personal data" means any information that is linked or reasonably linkable to an identified or identifiable natural person. - Excludes deidentified information or publicly available information
Sensitive personal information and data	Under the CPRA, consumers will be able to limit the use and processing of sensitive personal information. The CPRA defines "sensitive personal information" to include: government identifiers; financial account and login information; precise geolocation; the content of nonpublic communications; genetic, biometric, or health information; and information related to a consumer's racial or ethnic origin, religious beliefs, union membership, or sex life or sexual orientation.	"Sensitive data" means: - Personal data revealing racial or ethnic origin, religious beliefs, mental or physical health condition or diagnosis, or sex life or sexual orientation - The processing of genetic or biometric data for the purpose of uniquely identifying a natural person - The personal data of an individual known to be a child
Privacy notices and consent requirements		
Consumer privacy notices and consent requirements	Must inform consumers 1) about what categories of personal information have been processed in the last year, from what sources, and for what purpose; 2) about what kinds of third parties will receive the personal information (or a prominent statement that the business does not sell or share personal information); 3) about their consumer rights, as enumerated; and 4) how to exercise their consumer rights. Must provide **clear and conspicuous** notice, via a link on the business's homepage with "Do Not Sell" language, to consumers regarding 1) their rights to opt out of the sale and sharing (for cross-contextual advertising) of their information and 2) their right to limit the use of sensitive personal information. Must have a minimum of two methods for consumers to submit requests, with one being a toll-free number. The CPRA also requires that covered entities disclose the retention period for collected data or the criteria used to determine that period.	Must inform consumers 1) about what categories of personal data are being processed, and for what purpose; 2) how to exercise their consumer rights; and 3) about the categories of data being shared with third parties, and what kinds of third parties. If selling personal data, must **clearly and conspicuously** disclose this, and describe how the consumer may opt out. **In order to process sensitive data, express consent by the consumer is required.**

Data collection notice requirements	At or before the point of data collection, must inform consumers 1) what categories of personal data are being collected; 2) for what purpose; and 3) of the business' privacy policy, and if the business sells personal information, must provide a link to opt out.	Must inform consumers: 1) that certain categories of personal data are being collected and 2) whether that data is sold to data brokers, and, if relevant, provide consumers with access to personal data being maintained by a controller.
Consumer and data subject requests		
Verifying consumer requests	A business may require authentication that is "reasonable in light of the nature of the personal information," but may not require a consumer to create a new account. - For consumers exercising the right to know about categories of information, the business must verify their identity to a reasonable degree of certainty (a reasonably high degree of certainty is required for knowing particular pieces of information about an individual). This verification standard may be met by matching up elements or data points of personal information.	A business can use "commercially reasonable efforts" to authenticate a request, but may not require a consumer to create a new account. No further clarification is provided about what constitutes such efforts.
Responding to consumer requests	After receiving a verifiable consumer request, covered businesses must respond within 45 days. - Businesses may extend the time to respond/delete/correct by an additional 45 days when reasonably necessary, provided that they notify the consumer of the delay within the first 45-day period.	After receiving a verifiable consumer request, covered entities must respond within 30 days. - Entities may extend that period by an additional 60 days where reasonably necessary, but must: 1) inform the consumer of any extensions within 30 days of the original request and 2) provide reasons for the delay.
Training and recordkeeping	Those handling consumer inquiries must be informed about the law's requirements, and know how to direct consumers on how to exercise their data subject rights. Businesses must maintain records of consumer requests made, and how those requests were answered/responded to for **at least 24 months**. Businesses may maintain a confidential record of deletion requests exclusively for the purposes of compliance.	**N/A**
Additional controller obligations		
Data minimization requirements	A business must minimize retention of personal information to what is **reasonably necessary and proportionate** to achieve the purposes of collection or processing.	A controller shall limit the collection of personal data to what is adequate, relevant, and reasonably necessary for the purposes of the processing.

Data protection obligations	Covered businesses must implement reasonable security procedures and practices, considering the nature of the personal information.	Covered entities must maintain reasonable administrative, technical, and physical data security measures.
Risk assessment requirements	Under the CPRA, entities must complete annual audits and periodic risk assessments for processing activities that present a significant risk to consumer privacy.	Covered entities must conduct data protection assessments when a controller is 1) processing personal data for targeted advertising purposes; 2) selling personal data; 3) processing personal data for profiling purposes (with some exceptions); 4) processing sensitive data; or 5) conducting any processing activity that presents a heightened privacy risk. Such assessments must be made available to the attorney general upon request.
Obligations with respect to third parties		
	Designates "businesses," "service providers," and "third parties." Contracts with service providers must include certain requirements **to not sell or process data outside the scope of the services provided** under the contract.	Designates "controller" and "processor." **Specific contractual provisions are required** around the nature, purpose, duration, etc. of the processing, as well as specific obligations of the processor to cooperate with security assessments and to assist with data subject requests, among other items. Subcontracting agreements by the processor must also include these provisions.
Enforcement and penalties		
Methods of enforcement	**- Private right of action** for data breaches - Attorney general enforcement with 30-day cure period **Plus**, under the CPRA: - No longer a cure period - Establishment of a new agency (CIPPA) empowered with rulemaking and enforcement authority	Attorney general exclusive enforcement; **no private right of action** - 30-day cure period

Penalties	Private right of action (for data breaches) may seek: - Statutory damages ($100-$750 per violation) or actual damages, whichever is greater - Injunctive relief - Attorneys' fees Attorneys general may issue maximum administrative fees of $2,500 (negligent violations) and $7,500 (intentional violations or those involving minors' personal data) - Fines are deposited into the Consumer Privacy Fund,	Maximum $7,500 per violation Penalties awarded pursuant to an enforcement action will be deposited into the Consumer Privacy Fund.