



## Comprehensive Consumer Data Privacy State Law Summaries

Updated: April 5, 2023

The internet and new technologies continually raise new policy questions about privacy, and state lawmakers are continuing to address the array of privacy issues arising from online activities. This memorandum documents state comprehensive data privacy laws.

Six states—California, Colorado, Connecticut, Iowa, Utah and Virginia—have enacted comprehensive consumer data privacy laws. The laws have several provisions in common, such as the right to access and delete personal information and to opt-out of the sale of personal information, among others. Other provisions require commercial websites or online services to post a privacy policy that describes the types of personal information collected, what information is shared with third parties, and how consumers can request changes to certain information.

### California\*\*

Cal. Civ. Code §§1798.100 et seq. California Consumer Privacy Act of 2018 (CCPA)

Allows consumers the right to request a business to disclose the categories and specific pieces of personal information that the business has collected about the consumers as well as the source of that information and business purpose for collecting the information. Provides that consumers may request that a business delete personal information that the business collected from the consumers. Provides that consumers have the right to opt-out of a business's sale of their personal information, and a business may not discriminate against consumers who opt-out. Applies to California residents. (2018 AB 375, Effective Jan. 1, 2020. Amended by 2018 SB 1121.)

Related CCPA Information:

- [CCPA Regulations](#), California Office of the Attorney General
- California Attorney General, [Background on the CCPA and the Rulemaking Process](#)
- [Standardized Regulatory Impact Assessment: California Consumer Privacy Act of 2018 Regulations](#), prepared for California Attorney General's Office, Aug. 2019

California Consumer Privacy Rights Act (CPRA)

Proposition 24, approved Nov. 2020, effective Jan. 1, 2023

Expands the consumer data privacy laws. Permits consumers to: (1) prevent businesses from sharing personal information; (2) correct inaccurate personal information; and (3) limit businesses' use of "sensitive personal information"—including precise geolocation; race; ethnicity; religion; genetic data; private communications;



sexual orientation; and specified health information. Establishes the California Privacy Protection Agency to additionally enforce and implement consumer privacy laws and impose fines. Changes criteria for which businesses must comply with laws. Prohibits businesses' retention of personal information for longer than reasonably necessary. Triples maximum penalties for violations concerning consumers under age 16. Authorizes civil penalties for theft of consumer login information, as specified. (Amended by [2021 A.B. 1490](#))

## Colorado

[Colo. Rev. Stat. §6-1-1301 et seq.](#) Colorado Privacy Act

Creates the Colorado Privacy Act within the Colorado Consumer Protection Act. Addresses consumers' rights to privacy, companies' responsibility to protect personal data, and authorizes the attorney general and district attorneys to take enforcement action for violations. Defines various terms related to covered businesses, consumers, and data, including defining the term "controller" as the person or group of people who determine how data is used and processed. The effective date is July 1, 2023. ([2021 SB 190](#))

## Connecticut\*\*

[Conn. Gen. Stat. §42-515 et seq.](#) Personal Data Privacy and Online Monitoring

The Connecticut act establishes a framework for controlling and processing personal data; provides responsibilities and privacy protection standards for data controllers and processors; and grants consumers the right to access, correct, delete and obtain a copy of personal data, and opt out of the processing of personal data. The effective date is July 1 2023. ([2022 SB 6](#))

## Iowa

[2023 SF 262](#) Consumer Data Protection

This act relates to consumer data protection. The bill provides that persons conducting business in the state or producing products or services targeted to Iowans that annually control or process personal data of over 99,999 consumers or control or process personal data of 25,000 consumers with 50% of gross revenue derived from the sale of the personal data shall be subject to the provisions of the bill. The state and political subdivisions of the state, financial institutions or data subject to the federal Gramm-Leach-Bliley Act of 1999, certain organizations governed by rules by the department of health and human services, certain federal governance laws and the federal Health Insurance Portability and Accountability Act, nonprofit organizations, higher learning institutions, and certain protected information and personal data collected under state or federal laws are exempt from provisions in the bill. The bill provides that controllers must disclose to the consumer the types of data being collected and obtain consent from the consumers regarding the collection of personal data and sensitive



personal data processing. A controller or processor found to be in violation of provisions of the bill is subject to a civil penalty of up to \$7,500 per violation. Moneys collected by the attorney general under the bill shall be paid into the consumer education and litigation fund established under Code section 714.16C. The effective date is Jan. 1, 2025.

## Utah

Utah Code Ann. §13-61-101 et seq. Consumer Privacy Act

Utah's Consumer Privacy Act provides consumers the right to know what personal data a business collects, how the business uses the personal data, and whether the business sells the personal data. It also provides that consumers may access and delete personal data maintained by businesses and opt out of the collection and use of personal data. It also requires specified businesses to safeguard personal data, provide clear information about how consumers' personal data are used, and accept and comply with consumer requests to access, delete or stop selling personal data. The law authorizes the attorney general to take enforcement action and impose penalties. The effective date is Dec. 31, 2023. (2022 SB 227)

## Virginia\*\*

Va. Code §59.1-575 et seq. Consumer Data Protection Act

Virginia's Consumer Data Protection Act establishes a framework for controlling and processing personal data in the commonwealth. The law applies to all persons that conduct business in the commonwealth and either (i) control or process personal data of at least 100,000 consumers or (ii) derive over 50% of gross revenue from the sale of personal data and control or process personal data of at least 25,000 consumers. The law outlines responsibilities and privacy protection standards for data controllers and processors. The bill does not apply to state or local governmental entities and contains exceptions for certain types of data and information governed by federal law. The law grants consumer rights to access, correct, delete, obtain a copy of personal data, and to opt-out of the processing of personal data for the purposes of targeted advertising. The law provides that the attorney general has exclusive authority to enforce violations of the law, and the Consumer Privacy Fund is created to support this effort. The law directs the Joint Commission on Technology and Science to establish a workgroup to review the provisions of this act and issues related to its implementation and to report on its findings by Nov. 1, 2021. The effective date is Jan. 1, 2023. (2021 HB 2307 / 2021 SB 1392)

**NCSL Contact:** Heather Morton, 303-856-1475, [heather.morton@ncsl.org](mailto:heather.morton@ncsl.org)