

A faint, blue-toned map of the United States serves as the background for the slide. The map shows state boundaries and major cities, with the words "NORTH AMERICA" and "ATLANTIC" visible in large, light blue letters across the map.

US State Comprehensive Privacy Laws Report

2025 LEGISLATIVE SESSION



Table of contents

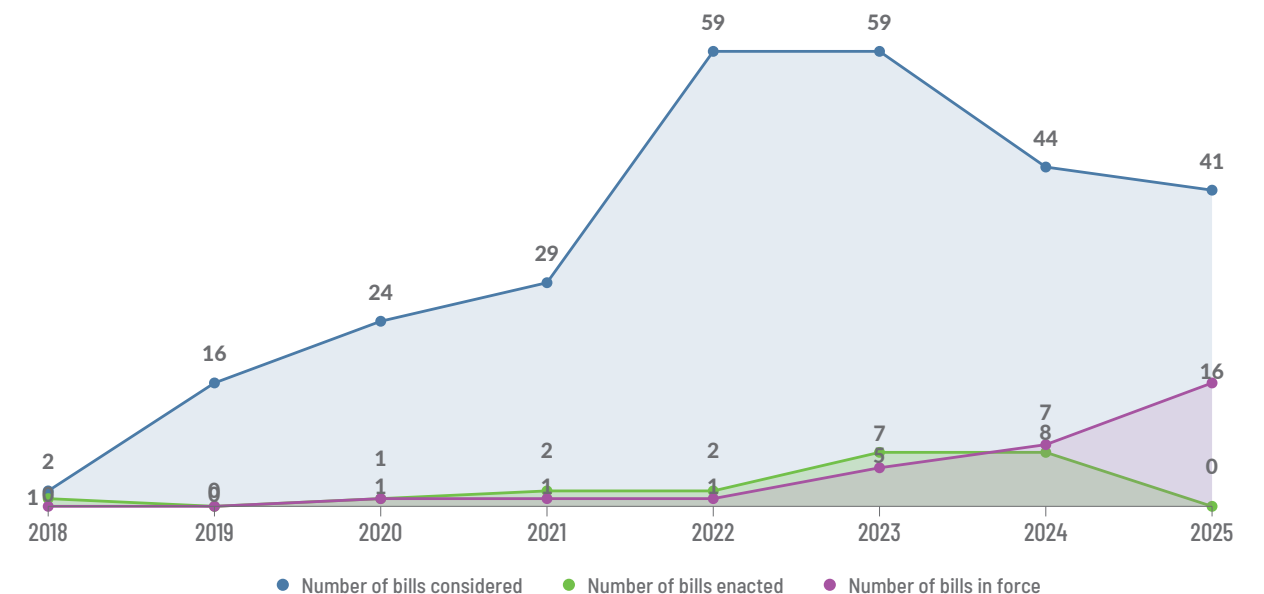
What's inside?

2025 Legislative session.....	3
Overview	5
Scope.....	11
Exemptions.....	15
Consumer rights	18
Business obligations	21
Sensitive information	24
Rulemaking.....	28
Enforcement.....	30
Comprehensive US state privacy laws at-a-glance	32
Contacts	52

2025 Legislative Session

The growth of U.S. state privacy law began slowly, but continues to develop exponentially with new laws introduced, enacted, and coming into force each year. It was not long ago, in 2018, that the California Consumer Privacy Act became the first comprehensive U.S. state privacy law to pass. It was not until 2021 that a data privacy law outside of the state of California was passed, with enactments in Virginia and Colorado. In 2022, that was matched when two more bills became laws in Utah and Connecticut. In 2023, seven bills became law in Delaware, Indiana, Iowa, Montana, Oregon, Tennessee and Texas, while 2024 matched that with seven more bills becoming law in New Hampshire, New Jersey, Kentucky, Maryland, Minnesota, Nebraska and Rhode Island.

The growth of US state privacy legislation



Most US state privacy laws are now in force

While no new U.S. state privacy laws have been passed in 2025 — as of the time of this writing — this year has been defined by a high number of the previously enacted laws coming into force and/or being amended. As of the end of 2024, a total of eight U.S. comprehensive state privacy laws were in force. By the end of 2025, the total number in effect will be double that, with 16 states having a privacy law in force by 31 December. Only three remaining states — Indiana, Kentucky and Rhode Island — have passed laws that have not yet gone into effect; all are slated to do so on 1 January 2026.

In addition, nearly half of the states that had enacted a comprehensive privacy law passed an amendment bill in 2025. Of the eight states that amended their privacy law this year, the changes in Connecticut, Montana and Oregon were particularly significant, expanding the scope of applicability, enhancing consumer rights, and/or putting in place further business obligations regarding the control and processing of consumers' personal data.

Given this pace of change, U.S. state privacy law remains an ever-evolving, dynamic law and policy arena. Keeping informed of significant developments, trends and enforcement priorities will continue to be an ongoing task for privacy professionals.

Disclaimer

This report is limited to comprehensive U.S. state privacy laws enacted as of July 2025. Further information on IAPP's methodology and definition of "comprehensive" can be found on the IAPP [website](#). The IAPP [US State Privacy Legislation Tracker](#), maintained with an identical scope in mind, lists any U.S. state privacy law proposed or passed since this report was published.

Enactment and effective dates of comprehensive US state privacy laws, listed by date of enactment

STATE PRIVACY LAW	DATE OF PASSAGE	DATE OF ENFORCEMENT
California Consumer Privacy Act	28 June 2018	1 Jan. 2020
California Privacy Rights Act	3 Nov. 2020	9 Feb. 2024
Virginia Consumer Data Protection Act	2 March 2021	1 Jan. 2023
Colorado Privacy Act	7 July 2021	1 July 2023
Connecticut Data Privacy Act	10 May 2022	1 July 2023
Utah Consumer Privacy Act	24 March 2022	31 Dec. 2023
Oregon Consumer Privacy Act	22 June 2023	1 July 2024
Texas Data Privacy and Security Act	16 June 2023	1 July 2024
Montana Consumer Data Protection Act	19 May 2023	1 Oct. 2024
Iowa Consumer Data Protection Act	29 March 2023	1 Jan. 2025
Tennessee Information Protection Act	11 May 2023	1 July 2025
Indiana Consumer Data Protection Act	1 May 2023	1 Jan. 2026
Delaware Personal Data Privacy Act	11 Sept. 2023	1 Jan. 2025
New Jersey Data Privacy Law	16 Jan. 2024	15 Jan. 2025
New Hampshire Data Privacy Act	6 March 2024	1 Jan. 2025
Kentucky Consumer Data Protection Act	4 April 2024	1 Jan. 2026
Nebraska Data Privacy Act	17 April 2024	1 Jan. 2025
Maryland Online Data Privacy Act	9 May 2024	1 Oct. 2025
Minnesota Consumer Data Privacy Act	24 May 2024	31 July 2025
Rhode Island Data Transparency and Privacy Protection Act	25 June 2024	1 Jan. 2026

In total, 19 states have enacted privacy laws that meet the IAPP's definition of "comprehensive," which excludes narrower legislation such as Florida's Digital Bill of Rights and Washington state's My Health My Data Act.



Overview

The expanding scope of US state privacy laws

While no new states have added comprehensive data privacy laws to their ledgers in 2025, half of those with laws already on the books have made significant amendments to their scopes and requirements. As of mid-2025, eight states — Colorado, Connecticut, Kentucky, Montana, Oregon, Texas, Utah and Virginia — have amended their comprehensive privacy laws; further proposed amendments are pending in California and New Jersey.

Indeed, with eight laws coming into force and eight laws being amended, 2025 may be the year when the scope of existing U.S. state privacy laws expanded the most.

Lower thresholds of applicability in Connecticut and Montana

Some of the most significant new threads added to the patchwork have come from Connecticut's SB 1295, which amends the Connecticut Data Privacy Act and takes effect 1 July 2026. It significantly expands the act's scope by lowering the applicability thresholds regarding the control, processing and sale of consumers' sensitive and personal data as well as removing the entity-level exemption for the Gramm-Leach-Bliley Act. These amendments to the Connecticut Data Privacy Act — the second such overhaul of the law following amendments in 2023 that focused on protections for minors and consumer health data — also expanded its definition of sensitive data; created additional privacy notice obligations; added new requirements for "impact assessments" for profiling, which are separate from the act's existing data protection impact assessments; and brought about additional protection for children's data.

Sweeping amendments to Montana's Consumer Data Privacy Act via SB 297 similarly expanded the law's scope by lowering the processing thresholds and narrowing the GLBA exemption. With these changes, Montana's privacy law applies to entities doing business in Montana that control or process the personal data of 25,000 or more Montana consumers annually — previously 50,000 — or that control or process the personal data of 15,000 or more Montana consumers — previously 25,000 — and derive 25% of their gross annual revenue from the sale of personal data. Montana's SB 297 also re-legislates children's privacy through its adding of a "willfully disregards" knowledge standard for teenager opt-ins, explicitly disclaiming any age-verification requirement and implementing youth privacy protections.

Added protections for sensitive data and prohibitions on sale

A few states also saw relatively minor amendments to their comprehensive privacy laws. In Colorado, SB 25-276, a bill that protects civil rights based on immigration status, also amends the definition of "precise geolocation data," folds that term into its definition of and protections for "sensitive data," and prohibits controllers from selling a consumer's sensitive data without first obtaining their consent. Kentucky's amendment bill adds an entity-level exemption for the Health Insurance Portability and Accountability Act and a data protection impact assessment requirement for profiling that presents "a reasonably foreseeable risk" of "unlawful, disparate impact on consumers." Oregon's HB

2008 increases protections for personal data collected from consumers under the age of 16 and for precise geolocation data. The state's HB 3875 expands the Oregon Consumer Privacy Act's scope to include motor vehicle manufacturers that control or process data obtained from consumers' vehicular use. Utah added a right to correction and imposed various obligations related to the rights to access, data portability, and interoperability on social media companies through the passage of HB 418. Finally, Virginia successfully again amended the Virginia Consumer Data Protection Act through passage of SB 854 to require social media platforms to use "commercially reasonable methods," such as a neutral age screen mechanism, to determine if a user is a minor, i.e., younger than 16, and to limit their use of the platform to one hour per day, which can be increased or decreased via parental consent.

Not all amendment efforts succeeded — Yet

Failed amendment bills include one in Iowa that would have expanded the definitions of "health record" and "sensitive data." In Minnesota, a failed amendment would have made "consumer health data" a form of sensitive data and appended additional protections for it. A bill that died in committee in Oregon would have lowered the applicability thresholds and prohibited the processing and selling of sensitive data for targeted advertising or profiling without consent. In Tennessee, a bill stalled that would have lowered the processing thresholds for applicability and prohibited the processing and selling of sensitive

data for targeted advertising or profiling without consent. Two bills failed in Texas that would have included "real-time driving data" within the definition of "sensitive data" and required controllers to enable web browsers to recognize and comply with a consumer's global privacy control preference. Similarly, a bill Virginia failed that would have prohibited the sale of precise geolocation data.

In California and New Jersey, where this year's lawmaking sessions end 12 September and 31 December, respectively, several amendment proposals remain pending as of the time of this writing. In California, AB 364 would require companies to disclose and obtain consent if any personal data they control and process is being stored outside the U.S., while AB 566 would impose a requirement for all browsers to recognize global opt-out signals. In New Jersey, proposals are in committee that would require controllers and processors to de-identify personal data and prohibit re-identification of de-identified data and add an exemption for personal data collected, processed, sold or disclosed for the purposes of detecting or preventing fraud.

Passed, proposed and failed amendments to comprehensive US state privacy laws in 2025

State	Amendment bill	Status	Main provisions
California	AB 364		Requires companies to disclose if personal data is being stored outside the U.S. and to obtain explicit consent before doing so
	AB 566		Requires global opt-out signal for all browsers
Colorado	SB 25-276		Modifies definition of "precise geolocation data" and includes it within the definition of "sensitive data"; prohibits controllers from "selling" sensitive data without consent
Connecticut	SB 1295		Modifies definitions of "consumer health data," "publicly available information" and "sensitive data"; adds "neural data" to definition of "sensitive data"; lowers applicability thresholds; expands consumer right to access; and adds children's privacy protections
Iowa	SF 143/HF 503		Changes definition of "child" from younger than 13 to younger than 18; expands the definitions of "health record" and "sensitive data"
Kentucky	HB 473		Adds entity-level exemption for HIPAA and requires data protection impact assessments for profiling that presents "a reasonably foreseeable risk" of "unlawful, disparate impact on consumers"
New Jersey	A4741		Requires controllers/processors to de-identify personal data and prohibits re-identification of de-identified data; requires the Director of the Division of Consumer Affairs in the Department of Law and Public Safety to establish standards for the de-identification of personal data
	A5017		Exempts personal data collected, processed, sold or disclosed for the purpose of detecting or preventing fraud
Minnesota	SF 2940/HF 2700		Makes "consumer health data" a form of sensitive data and adds additional protections for sensitive data
Montana	SB 297		Lowers the processing thresholds for applicability, narrows the GLBA exemption and adds protections for children's privacy
Oregon	HB 2008		Prohibits the sale of personal data collected from consumers younger than 16 and of precise geolocation data
	HB 3875		Expands scope to include motor vehicle manufacturers that control or process data obtained from consumers' vehicular use
	HB 3899		Lowers applicability thresholds, adds protections for minors' and sensitive data, and imposes data minimization restrictions
Tennessee	SB 0663		Prohibits the processing and selling of sensitive data for targeted advertising or profiling without consent and lowers the processing thresholds for applicability
Texas	HB 4636		Defines "real-time driving data" and includes it within the definition of "sensitive data"
	HB 5495		Requires controllers to enable web browsers to recognize and comply with a consumer's global privacy control preferences, imposing a USD5,000 fine for each violation and giving courts the discretion for higher fines for repeated violations
Utah	HB 418		Adds a right to correction and imposes requirements related to social media data portability and interoperability
Virginia	SB 854		Requires social media platforms to use "commercially reasonable methods" to determine if a user is a minor, under the age of 16; and limits a minor's use of the platform to one hour per day by default; this limit can be changed with parental consent
	SB 1023		Prohibits the sale of precise geolocation data



Passed



In-committee



Failed

Passed, proposed, and failed amendments to comprehensive US state privacy laws in 2024

State	Amendment bill	Status	Main provisions
Colorado	HB 1058	✓	Adds biological and neural data to the definition of sensitive data
	HB 1130	✓	Adds obligations and consent requirements related to biometric data and biometric identifiers
	SB 041	✓	Expands protections and obligations relating to minors; requires controllers and processors to implement age verification
Utah	HB 0342	✗	Amends applicability requirements; adds a private right of action
Virginia	HB 1161	✗	Requires social media platforms to obtain verifiable parental consent prior to permitting any minor to make a social media account
	HB 707/SB 361	✓	Requires parental consent before controllers can collect or process a known child's personal or geolocation data; adds purpose limitations to such collection or processing
	HB 821	✗	Requires parental consent before a controller can register a child with their service or process a child's data for targeted advertising, selling the data or profiling
	HB 821/SB 432	✗	Requires parental consent before a child can register with a controller and before collecting or processing a child's data; changes the definition of child to include people under 18
	SB 252	✗	Requires controllers to add a method to opt out of cookies in their privacy notices; limits cookie use to those that are strictly necessary
	SB 359	✗	Prohibits social media platforms from providing addictive feeds to children under 18 without parental consent

✓ Passed

✗ Failed

Passed, proposed, and failed amendments to comprehensive US state privacy laws in 2023

State	Amendment bill	Status	Main provisions
California	AB 1008	✓	Excludes biometric information collected without a consumer's knowledge from the definition of publicly available information; includes abstract digital formats in the definition of personal information; includes neural data in the definition of sensitive personal information
	AB 1194	✓	Broadens the scope of California Consumer Privacy Act to cover personal information that contains information about reproductive care, including abortions
	AB 1546	✗	Prohibits administrative actions commencing more than five years after the cause of action accrues
	AB 1824	✓	When there is a merger, acquisition, bankruptcy or other situation where a business transfers personal information to another entity, that entity must respect a consumer's opt-out request
	AB 1949	✗	Requires consent from consumers between ages 13 and 18 to process their personal information; requires a parent's or guardian's consent to process personal information from consumers under 13
	AB 2877	✗	Prohibits AI developers from using personal information from people under 16 to train their AI
	AB 3048	✓	Requires businesses that develop browsers or mobile operating systems to enable opt-out preference signals
	AB 3286	✓	Apportions funds to the California Privacy Protection Agency and requires the CPPA, not the attorney general, to adjust monetary thresholds
	AB 947	✓	Adds information concerning a consumer's citizenship or immigration status to the definition of sensitive personal information
	SB 1223	✓	Amends the definition of sensitive personal information to include neural data
Connecticut	HB 06249	✗	Applies the Connecticut Data Privacy Act to state agencies
	SB 00003	✓	Imposes new requirements related to consumer health data and children's privacy
Utah	SB 0299	✗	Includes reproductive health data in the definition of sensitive personal data; prohibits governmental entities from obtaining a consumer's reproductive health data in some circumstances

✓ Passed

✗ Failed

What's in store for US state privacy law?

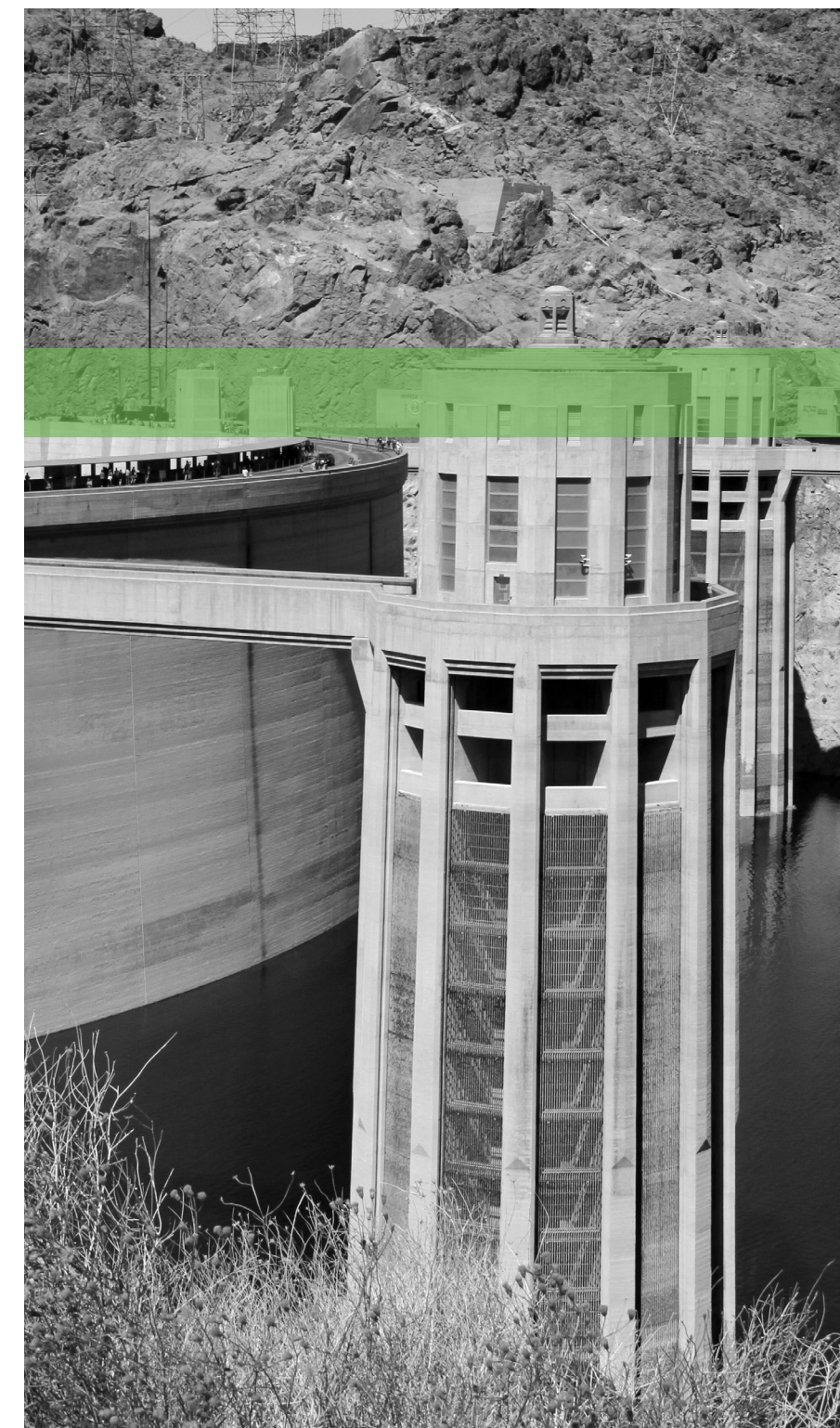
While 2025 has been a relatively inactive year, passage of new state privacy laws has outpaced prior years in terms of further expanding the remit of existing state privacy laws through legislative amendments. With no signs of slowing down, it remains as crucial as ever for privacy pros to understand the evolving contours of U.S. state privacy law.

Moreover, in the midst of all these efforts to amend existing laws, dozens of new comprehensive privacy bills remain under [deliberation](#) in 16 states: Arkansas, Georgia, Hawaii, Illinois, Maine, Massachusetts, Michigan, New York, North Carolina, Oklahoma, Pennsylvania, South Carolina, Vermont, Washington, West Virginia, and Wisconsin, with [SB 546](#) in Oklahoma and [S. 71](#) in Vermont having advanced furthest in the legislative process to date.

In parallel to this legislative activity within U.S. state capitols around consumer privacy, calls continue for Congress to pass a comprehensive federal privacy law. Although no such federal lawmaking initiative has been undertaken in 2025 as of yet that would match the ambit of the American Privacy Rights Act of 2024 or the American Data Privacy and Protection Act of

2023, the House of Representatives voted in June to approve a 10-year federal moratorium on the enforcement of state-level laws targeting AI and automated decision-making systems. While that provision was removed by the [Senate](#) in final amendments to the budget bill, the episode revealed both support and opposition within Congress, both across and within parties, for halting state-level AI legislative activity. It is easy to imagine a similar debate — as indeed has happened in the past when both APRA and ADPPA were introduced — around federal preemption of state-level privacy laws.

Alongside the IAPP [US State Privacy Legislation Tracker](#), this report provides an in-depth and refreshed analysis of the evolving scope, applicability, exemptions, consumer rights, business obligations, rulemaking activities, enforcement duties and key definitions for each of the 19 states that have passed comprehensive privacy laws to date. It sketches the contours of the nationwide portrait of privacy regulation that has emerged, while highlighting the idiosyncrasies of each state law that constitutes the U.S. state [privacy kaleidoscope](#). Overall, this report aims to keep privacy professionals informed about all the comprehensive privacy bills that have become law, the rights they offer to consumers and the obligations they require from regulated entities.



Scope

Applicability thresholds for US state privacy laws

Each U.S. state privacy law has a unique scope of applicability based on a variety of thresholds related to an entity's jurisdiction, revenue, volume of personal data processing and revenue from the sale of personal data. The applicability of each U.S. state privacy law can be determined through a multistep process. First, the entity must be doing business in the state in question. Tennessee and Utah are the only two states with an independent revenue threshold, as their laws apply only to entities that exceed USD25 million in annual revenue.

If an entity meets the jurisdictional criteria, then it usually must also meet one of two thresholds to be subject to the law. One of these is based on the volume of personal data of in-state residents it processes; the other is based on its sales of residents' personal data.

Applicability factors



JURISDICTION



REVENUE



VOLUME OF
PERSONAL DATA
PROCESSING



REVENUE FROM
THE SALE OF
PERSONAL DATA

Threshold for processing of personal data

U.S. state privacy laws establish at least five different thresholds for processing residents' personal data:

- Nebraska and Texas have no such threshold
- 25,000 or more unique consumers in Montana
- 35,000 or more unique consumers in Connecticut, Delaware, Maryland, New Hampshire and Rhode Island
- 100,000 or more unique consumers in California, Colorado, Indiana, Iowa, Kentucky, Minnesota, New Jersey, Oregon, Utah and Virginia
- 175,000 or more unique consumers in Tennessee

Nebraska and Texas have the lowest thresholds, as any processing of personal data would make an entity subject to the law's applicability, so long as the entity also engages in the sale of some data. Most states fall somewhere between a raw threshold of 35,000 and 100,000

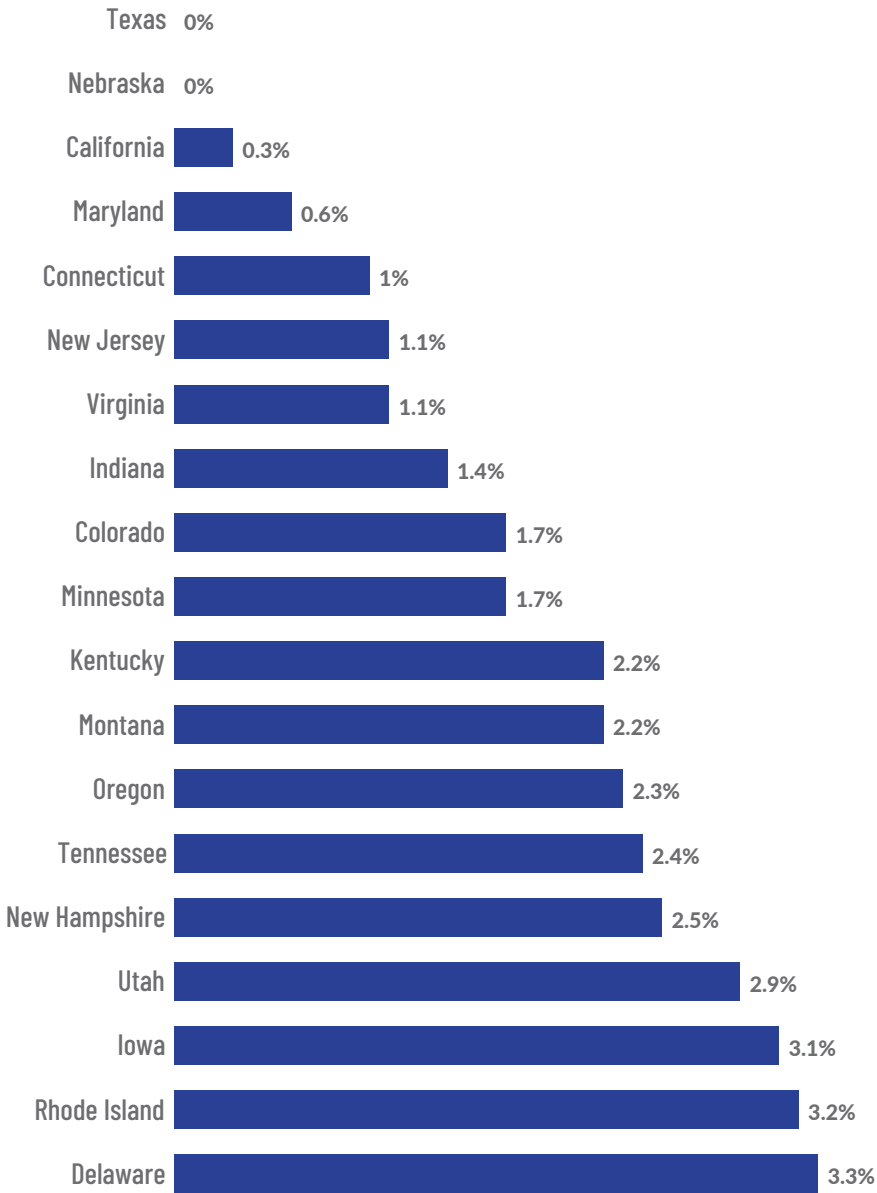
or more unique consumers. In terms of raw numbers, Tennessee is at the far end of the spectrum, placing the threshold of personal data processing at 175,000 or more unique customers. But, if adjusted by state population, Delaware has the highest threshold as a percentage of its population.

The thresholds for personal data processing generally exclude personal data that is controlled or processed solely for the purpose of completing a payment transaction.

The bar graph illustrates the thresholds for the processing of personal data across each state considering differences in the sizes of their populations. Thus, it shows the percentage of each state's population whose data an entity must process to meet that state's threshold.

For example, while Maryland and Delaware both have a processing threshold of 35,000 or more consumers, Maryland's threshold is lower in relative terms, as this equates to just about 0.6% of the population of Maryland compared to about 3.3% of the population of Delaware.

Percentage of a state's population whose data must be processed for an entity to meet that state's applicability threshold





Threshold for sale of personal data

The second independent threshold entities may meet for a state's privacy law to apply concerns the sale of personal data. In general, this threshold consists of a dual requirement. One component relates to the volume of data processing/control, which is similar in nature to but typically lower than the previously listed thresholds; the other relates to the percentage of revenue an entity obtains from the sale of personal data overall. Across various states, to fall within the scope of that state's comprehensive privacy law, an entity must:

- Nebraska and Texas: Control or process any personal data or engage in any sale of personal data.
- Connecticut: Control or process any sensitive data or offer personal data for sale in trade or commerce.
- California: Control or process any personal data and derive 50% or more of its revenues from the sale of personal data.
- Colorado and New Jersey: Control or process the personal data of 25,000 or more unique consumers and derive any revenue or discount on the price of any goods or services from the sale of personal data.
- Delaware, Maryland and Rhode Island: Control or process the personal data of 10,000 or more unique consumers and derive more than 20% of its revenue from the sale of personal data in.

- New Hampshire: Control or process the personal data of 10,000 or more unique consumers and derive more than 25% of its revenue from the sale of personal data.
- Montana: Control or process the personal data of 15,000 or more unique consumers and derive more than 25% of its revenue from the sale of personal data.
- Minnesota and Oregon: Control or process the personal data of 25,000 or more unique consumers and derive more than 25% of its revenue from the sale of personal data.
- Indiana, Iowa, Kentucky, Tennessee, Utah and Virginia: Control or process the personal data of 25,000 or more unique consumers and derive more than 50% of its revenue from the sale of personal data.

Again, Nebraska and Texas set the lowest thresholds, as any data processing combined with any sale of personal data would bring an entity within the scope of the law. Even so, both states also have small business exemptions. The most common threshold set by states, however, is to process the personal data of 25,000 or more unique individuals and derive somewhere between 25% and 50% of their revenue from the sale of personal data.

Only California provides a third threshold that may be met based on an entity's overall revenue. If an entity doing business in California generates at least USD25 million in annual revenue, it is subject to the CCPA.

Applicability thresholds across US state privacy laws

		Nebraska and Texas	Connecticut	California	Delaware, Maryland and Rhode Island	New Hampshire	Montana	Colorado and New Jersey	Minnesota and Oregon	Indiana, Iowa, Kentucky, Utah and Virginia	Tennessee
TO BE SUBJECT TO A STATE'S PRIVACY LAW, AN ENTITY MUST MEET ITS JURISDICTIONAL THRESHOLD ...											
JURISDICTIONAL		Does business in the state	Does business in the state	Does business in the state	Does business in the state	Does business in the state	Does business in the state	Does business in the state	Does business in the state	Does business in the state	Does business in the state
AND IT MUST ALSO MEET ONE OF THE FOLLOWING THRESHOLDS FOR PERSONAL DATA PROCESSING OR SALE OF PERSONAL DATA ...											
PERSONAL DATA PROCESSING		Any consumers	≥ 35,000 consumers	≥ 100,000 consumers	≥ 35,000 consumers	≥ 35,000 consumers	≥ 25,000 consumers	≥ 100,000 consumers	≥ 100,000 consumers	≥ 100,000 consumers	≥ 175,000 consumers
SALE OF PERSONAL DATA	CONTROLS OR PROCESSES THE PERSONAL DATA OF ...	Any consumers	Any consumers (sensitive data)	Any consumers	≥ 10,000 consumers	≥ 10,000 consumers	> 15,000 consumers	≥ 25,000 consumers	≥ 25,000 consumers	≥ 25,000 consumers	≥ 25,000 consumers
	PERCENT OF GROSS REVENUE DERIVED FROM SELLING PERSONAL DATA IS ...	Any*	Any	> 50%	> 20%	> 25%	> 25%	Any	> 25%	> 50%	> 50%

Note: Within each U.S. state privacy law, a consumer is generally defined as a resident of that state. *Most non-manufacturing businesses with overall revenue below USD7.5 million are subject to a limited small business exemption in these states.

Exemptions

Which entities and data are excluded?

Each of the 19 state privacy laws exclude from their scope various entities — such as government agencies, nonprofits and institutions of higher education — as well as entities already subject to federal, sectoral privacy legislation, such as the Gramm-Leach-Bliley Act, Health Insurance Portability and Accountability Act, Family Educational Rights and Privacy Act, Fair Credit Reporting Act and the Drivers Privacy Protection Act.

Across these categories of exemptions, there are two distinct types: entity-level exemptions and data-level exemptions. As the names suggest, an entity-level exemption removes an entire organization from the scope of the law. By contrast, data-level exemptions only exempt a certain type of data an entity holds, while the entity itself may still be subject to the law's requirements.

The two distinct types of exemptions



ENTITY-LEVEL



DATA-LEVEL

Entity-level and data-level exemptions across US state privacy laws

	Government	Nonprofits	Higher education	National securities associations	Employee/commercial business to business	GLBA	HIPAA	FERPA	FCRA	DPPA
California	E	E	⊗	⊗	⊗	D	D	D	D	D
Colorado	D	⊗	E	E	D*	E/D	D	D	D	D
Connecticut	E	E	E	E	D	D	E / D	D	D	D
Delaware	E	⊗*	⊗	E	D	E	D	D	D	D
Indiana	E	E	E	⊗	D	E/D	E/D	D	D	D
Iowa	E	E	E	⊗	D	E/D	E/D	D	D	D
Kentucky	E	E	E	⊗	D	E/D	E/D	D	D	D
Maryland	E	E*	⊗	E	D	E	D	D	D	D
Minnesota	E	⊗*	⊗*	⊗	D	D	D	D	D	D
Montana	E	⊗*	E	E	D	D	E/D	D	D	D
Nebraska	E	E	E	⊗	D	E	E/D	D	D	D
New Hampshire	E	E	E	E	D	E/D	D	D	D	D
New Jersey	E	⊗	⊗	⊗	D*	E	D	⊗	D	D
Oregon	E	⊗*	⊗	⊗	D	D	D	D	D	D
Rhode Island	E	E	E	E	D	E/D	D	D	D	D
Tennessee	E	E	E	⊗	D	E/D	E/D	D	D	D
Texas	E	E	E	⊗	D	E/D	E/D	D	D	D
Utah	E	E	E	⊗	D	E/D	E/D	D	D	D
Virginia	E	E	E	⊗	D	E/D	E/D	D	D	D

E Entity-level exemption

D Data-level exemption

⊗ No exemption

*Please see the following section on exemption nuances.

In terms of entity-level exemptions, all states but one provide an entity-level exemption for states or political subdivisions of the states. Colorado is the only state to provide an exemption for state bodies in the form of a data-level exemption. All the states except Colorado, Delaware, Minnesota, Montana, New Jersey and Oregon exempt nonprofits at the entity level, while all but California, Delaware, New Jersey and Oregon exempt institutions of higher education at the entity level.

Another entity-level exemption found across most U.S. state privacy laws are for national securities associations, i.e., the Financial Industry Regulation Authority. Just under half of the states — Colorado, Delaware, Maryland, Minnesota, Montana, New Hampshire and Rhode Island — provide this exemption.

Meanwhile, most states also provide either a data-level exemption or a combination of data-level and entity-level exemptions for the collection and processing of data that is already subject to regulation by GLBA, HIPAA, FERPA, FCRA and DPPA. For example, all states provide data-level exemptions for FCRA and DPPA; all but Colorado and New Jersey provide data-level exemptions for FERPA. Moreover, all states provide either data-level or entity-level exemption for HIPAA and GLBA-regulated data and entities. All states but California also provide an exemption for employee data and business-to-business data.

Lastly, there are small business exemptions in Minnesota, Nebraska and Texas. Within these states, a small business, as defined by the United States Small Business Administration, is exempt from that state's privacy law; small businesses in Texas must still obtain consumer consent to sell sensitive data.

Exemption nuances

- * The Colorado Privacy Act, as amended by HB 24-1130, applies to employers' collection and use of biometric data of employees and independent contractors.
- * In Delaware, only some nonprofit data is exempt. The law does not apply to certain data held by nonprofits that provide services to victims or witnesses of child abuse, domestic violence, human trafficking, sexual assault, violent felony or stalking.
- * In Maryland, only nonprofits that process or share personal data solely for the purpose of assisting either law enforcement agencies in investigating insurance-related crimes or fraud or first responders responding to catastrophic events are exempt.

- * In Minnesota, Montana and Oregon, only nonprofits that detect or prevent insurance fraud are exempt. Journalistic nonprofits are also exempt in Oregon.
- * In Minnesota, postsecondary institutions regulated by the Office of Higher Education are not required to comply until 31 July 2029.



Consumer rights

What types of data requests can consumers make?

Each U.S. comprehensive state privacy law establishes various consumer rights, including the ability to access, correct and delete personal data held by companies. These laws also provide opt-out rights for targeted or cross-contextual behavioral advertising, sale of personal data and profiling.

Consumer rights



ACCESS, CORRECT AND DELETE DATA



OPT OUT OF PROCESSING



DATA PORTABILITY



LIMIT USE AND DISCLOSURE OF SENSITIVE PERSONAL INFORMATION

The rights to access, correct and delete data

All state laws provide at least one of the rights to access, correct and delete personal data; most provide all three. The only deviations are found in Indiana, where the right to correct data only applies to consumer-provided data, and in Utah, which limits the right to delete to consumer-provided data and limits the right to correct to social media companies. The specification of consumer-provided data is generally meant to exempt personal data that the business inferred or derived about the consumer.

The right to opt out of processing

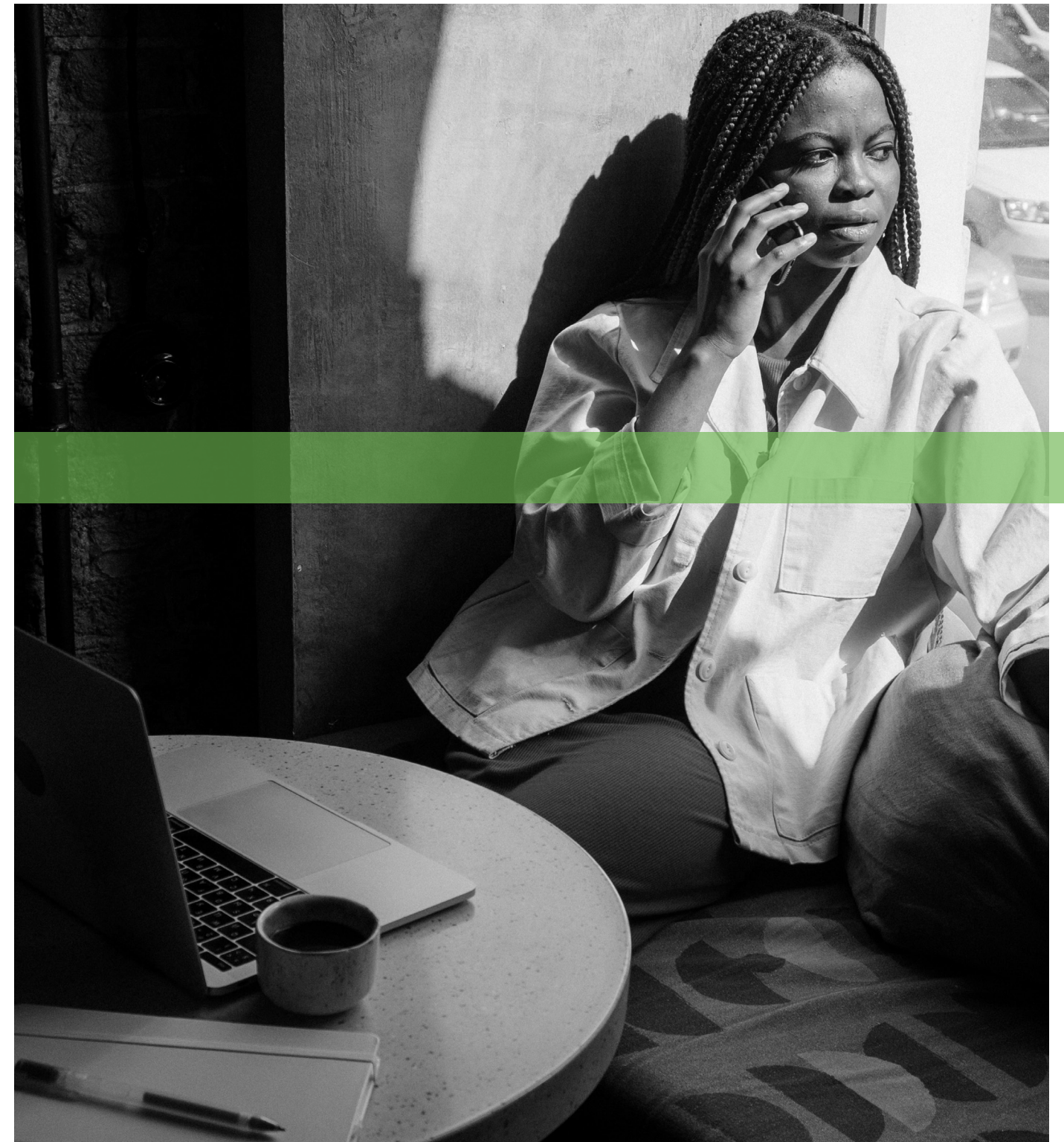
The state laws are also mostly consistent in terms of providing the right to opt out of processing for targeted or cross-contextual behavioral advertising, sale of personal data and profiling. For the deviations, Iowa's privacy law lacks the right to opt out of processing for targeted advertising and profiling, although it does establish the right to opt out of the sale of personal data. Utah does not provide the right to opt out of processing for profiling purposes.

The right to data portability

Among all the consumer rights, the right to data portability is perhaps the least uniform across the states. In most states, individuals have the right to data portability for any personal data held by a regulated entity. Yet, in a minority of states — Delaware, Indiana, Iowa, Montana, Tennessee, Texas, Utah and Virginia — the right to data portability only applies to information directly provided by a consumer.

The right to limit the use and disclosure of sensitive personal information

California is the only state to provide consumers with the right to limit the use and disclosure of sensitive personal information.



Consumer rights across US state privacy laws

	Access	Correct	Delete	Opt out of processing for...			Portability	
				Targeted advertising/cross-contextual behavioral advertising	Sale of personal data	Profiling		
California	✓	✓	✓	✓	✓	✓	✓	✓ Applies to all personal data of a consumer held by a regulated entity
Colorado	✓	✓	✓	✓	✓	✓	✓	
Connecticut	✓	✓	✓	✓	✓	✓	✓	✓ Applies to consumer-provided data only
Delaware	✓	✓	✓	✓	✓	✓	✓	
Indiana	✓	✓	✓	✓	✓	✓	✓	
Iowa	✓	✗	✓	✗	✓	✗	✓	✗ Does not apply
Kentucky	✓	✓	✓	✓	✓	✓	✓	
Maryland	✓	✓	✓	✓	✓	✓	✓	
Minnesota	✓	✓	✓	✓	✓	✓	✓	
Montana	✓	✓	✓	✓	✓	✓	✓	
Nebraska	✓	✓	✓	✓	✓	✓	✓	
New Hampshire	✓	✓	✓	✓	✓	✓	✓	
New Jersey	✓	✓	✓	✓	✓	✓	✓	
Oregon	✓	✓	✓	✓	✓	✓	✓	
Rhode Island	✓	✓	✓	✓	✓	✓	✓	
Tennessee	✓	✓	✓	✓	✓	✓	✓	
Texas	✓	✓	✓	✓	✓	✓	✓	
Utah	✓	✓	✓	✓	✓	✗	✓	
Virginia	✓	✓	✓	✓	✓	✓	✓	

Business obligations

What must businesses do to comply?

In addition to granting a series of rights to consumers, U.S. state privacy laws impose a series of obligations for entities that fall within their scope. In general, these obligations revolve around privacy notices, data minimization and purpose limitation of data collection and processing, sensitive personal information, data protection assessments, and universal opt-out mechanisms.

Business obligations



PRIVACY NOTICES



DATA MINIMIZATION AND PURPOSE LIMITATION
OF DATA COLLECTION AND PROCESSING



PROTECT SENSITIVE PERSONAL INFORMATION



DATA PROTECTION ASSESSMENTS



UNIVERSAL OPT-OUT MECHANISMS

Privacy notices

All U.S. state privacy laws require regulated entities to provide consumers with a notice that discloses their privacy practices. California is the only state that requires notice at the point of collection. Most state privacy laws require privacy notices to describe "all categories of third parties" with which a controller has shared personal data in sufficient detail so consumers can understand the nature of these third-party entities and how they process personal data. Additionally, some states require disclosing — upon consumer request — the specific third parties to which a business has disclosed that particular consumer's personal data or the specific third parties to which it has disclosed any personal data.

Data minimization and purpose limitation of data collection and processing

All state laws also include some kind of requirement to limit the collection and/or processing of data. The data minimization clauses typically require regulated entities to ensure the collection, use, retention and sharing of a consumer's personal information is limited to what is "adequate, relevant, and reasonably necessary" and that it is proportionate to achieving the purposes for which it was collected or processed. Similarly, purpose limitation clauses tend to require that personal data be used only in ways that are compatible with the original purpose of collection and not further processed in an incompatible manner without first obtaining consumer consent.

Only Rhode Island and Utah's privacy laws do not include requirements for data minimization or purpose limitation.





Protect sensitive personal information

In general, all U.S. state privacy laws require entities to obtain consent from consumers before processing their sensitive personal information.

California is unique in not embracing this consent requirement. Instead, regulated entities must give consumers notice that their sensitive personal information may be sold or shared, as well as the right to opt-out of the sale or sharing of their personal information.

Maryland also has unique guardrails in place with respect to sensitive information, adopting a data-minimization provision that prohibits the collection and processing of sensitive data unless it is strictly necessary to provide or maintain a specific product or service requested by the consumer. Maryland also entirely prohibits the sale of sensitive data.

Note: Refer to the section on [sensitive information](#) to see which different categories of information are considered sensitive across each state.

Data protection assessments

Data protection assessments are required by most U.S. state privacy laws for any processing activities that involve a "heightened risk of harm to consumers." The exceptions to this are Iowa and Utah. On the other hand, in Delaware, Indiana and Virginia, data protection assessments are specifically required for activities such as targeted advertising, sales of personal data and profiling, as well as any processing that presents a reasonably foreseeable risk of harm to consumers.

Universal opt-out mechanism

Recognition of universal opt-out mechanisms is required in California and Colorado, albeit limited to the Colorado attorney general's Universal Opt-Out Shortlist. Beginning in January 2025, recognition of universal opt-out mechanisms has been required in Delaware, Montana, New Hampshire and Texas. As of July 2025, it is required in Minnesota and New Jersey, and by October 2025, in Maryland. Lastly, in January 2026, universal opt-out mechanism recognition will be required in Connecticut and Oregon.



Sensitive information

What types of information receive heightened protection?

Each U.S. state privacy law recognizes at least some types of information as sensitive and deserving of heightened legal protection. Companies that collect and process any of the defined categories of sensitive personal information must comply with heightened requirements to protect it from misuse, loss or abuse. For most states, covered entities are required to obtain valid consent to collect and process sensitive data and subject the processing to a data protection assessment. This is not true in California, where entities must provide consumers with the option to limit the use of their sensitive data, unless an exception applies. Utah and Iowa similarly embrace an opt-out model, but one that comes close to opt-in consent as it requires an up-front notice with an opportunity to opt out before collection. Colorado includes special rules about the processing of sensitive data inferences; Texas requires a special up-front notice if an entity sells sensitive data.

Across all U.S. state privacy laws, any data about or relating to an individual's racial or ethnic origin or religious beliefs is defined as sensitive information. Without exception, all 19 U.S. state privacy laws recognize these types of information as sensitive and provide heightened protections for them.

The categories of information that are generally recognized as sensitive across most U.S. state privacy laws include any data about or relating to an individual's:

- Citizenship or immigration status.
- Mental or physical health data, e.g., conditions, diagnoses and treatments.
- Genetic or biometric data for purposes of uniquely identifying an individual.
- Sexual orientation, sexuality or sex life.
- Precise geolocation.
- Children's data.

Moreover, several additional types of information are recognized as sensitive in only one or a few U.S. state privacy laws. These include data about or relating to an individual's:

- National origin in Maryland and Oregon.
- Philosophical beliefs, union membership, and contents of a consumer's mail, email and

text messages in California.

- Consumer health data in California and Connecticut, though other state laws may apply.
- Biological or neural data in California, Connecticut and Colorado.
- Genetic or biometric data in Delaware, Maryland, New Hampshire and Oregon, though other state laws may apply.
- Status as transgender or nonbinary in Connecticut, Delaware, Maryland, New Jersey and Oregon.
- Status as victim of a crime in Connecticut and Oregon.
- Finance-related information in California, Connecticut and New Jersey.
- Government-issued identification numbers, including, but not limited to, Social Security, passport, state identification card or driver's license number in California and Connecticut.



Recognized categories of sensitive information across US state privacy laws

	Racial or ethnic origin	National origin	Citizenship or immigration/ citizenship status	Religious beliefs	Philosophical beliefs	Consumer health data	Mental or physical health data e.g., conditions, diagnoses, treatments	Sexual orientation/ sexuality	Sex life	Status as transgender or nonbinary	Children's data
California	✓	✗	✓	✓	✓	✓	✓	✓	✓	✗	✓
Colorado	✓	✗	✓	✓	✗	✗	✓	✓	✓	✗	✓
Connecticut	✓	✗	✓	✓	✗	✓	✓	✓	✓	✓	✓
Delaware	✓	✗	✓	✓	✗	✗	✓	✓	✓	✓	✓
Indiana	✓	✗	✓	✓	✗	✗	✓	✓	✗	✗	✓
Iowa	✓	✗	✓	✓	✗	✗	✓	✓	✗	✗	✓
Kentucky	✓	✗	✓	✓	✗	✗	✓	✓	✗	✗	✓
Maryland	✓	✓	✓	✓	✗	✓	✗	✓	✓	✓	✓
Minnesota	✓	✗	✓	✓	✗	✗	✓	✓	✗	✗	✓
Montana	✓	✗	✓	✓	✗	✗	✓	✓	✓	✗	✓
Nebraska	✓	✗	✓	✓	✗	✗	✓	✓	✗	✗	✓
New Hampshire	✓	✗	✓	✓	✗	✗	✓	✓	✓	✗	✓
New Jersey	✓	✗	✓	✓	✗	✗	✓	✓	✓	✓	✓
Oregon	✓	✓	✓	✓	✗	✗	✓	✓	✗	✓	✓
Rhode Island	✓	✗	✓	✓	✗	✗	✓	✓	✓	✗	✓
Tennessee	✓	✗	✓	✓	✗	✗	✓	✓	✗	✗	✓
Texas	✓	✗	✓	✓	✗	✗	✓	✓	✗	✗	✓
Utah	✓	✗	✓	✓	✗	✗	✓	✓	✗	✗	✗
Virginia	✓	✗	✓	✓	✗	✗	✓	✓	✗	✗	✓

- ✓ Recognized as a category of sensitive information
- ✗ Not recognized as a category of sensitive information

Recognized categories of sensitive information across US state privacy laws

	Genetic or biometric data for purposes of uniquely identifying an individual	Genetic or biometric data	Biological or neural data	Precise geolocation	Status as victim of crime	Social Security numbers, driver's licenses, state identification cards or passport numbers	Finance-related information	Union membership	Contents of a consumer's mail, email and text messages unless the business is the intended recipient of the communication
California	✓	✓	✓	✓	✗	✓	✓	✓	✓
Colorado	✓	✗	✓	✓	✗	✗	✗	✗	✗
Connecticut	✓	✗	✓	✓	✓	✓	✓	✗	✗
Delaware	✗	✓	✗	✓	✗	✗	✗	✗	✗
Indiana	✓	✗	✗	✓	✗	✗	✗	✗	✗
Iowa	✓	✗	✗	✓	✗	✗	✗	✗	✗
Kentucky	✓	✗	✗	✓	✗	✗	✗	✗	✗
Maryland	✓	✓	✗	✓	✗	✗	✗	✗	✗
Minnesota	✓	✗	✗	✓	✗	✗	✗	✗	✗
Montana	✓	✗	✗	✓	✗	✗	✗	✗	✗
Nebraska	✓	✗	✗	✓	✗	✗	✗	✗	✗
New Hampshire	✓	✗	✗	✗	✗	✗	✗	✗	✗
New Jersey	✓	✗	✗	✓	✗	✗	✓	✗	✗
Oregon	✗	✓	✗	✓	✓	✗	✗	✗	✗
Rhode Island	✓	✗	✗	✓	✗	✗	✗	✗	✗
Tennessee	✓	✗	✗	✓	✗	✗	✗	✗	✗
Texas	✓	✗	✗	✓	✗	✗	✗	✗	✗
Utah	✓	✗	✗	✓	✗	✗	✗	✗	✗
Virginia	✓	✗	✗	✓	✗	✗	✗	✗	✗

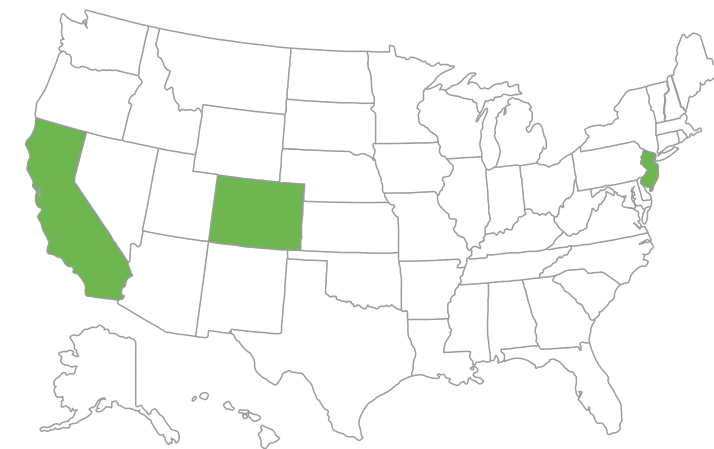
- ✓ Recognized as a category of sensitive information
- ✗ Not recognized as a category of sensitive information

Rulemaking

Three states — Colorado, California and New Jersey — give rulemaking authority to a state agency.

Only California has a dedicated enforcement agency, the California Privacy Protection Agency, for the promulgation of [rulemaking](#). In November 2024, the CPPA commenced formal rulemaking on subjects that included making updates to existing [CCPA regulations](#). These subjects also encompassed requirements for certain businesses to complete annual [cybersecurity audits](#) and conduct risk assessments, implement consumers' rights to access and opt-out of automated decision-making technology, and clarifying the conditions under which insurance companies must be CCPA compliant.

States with rulemaking authority

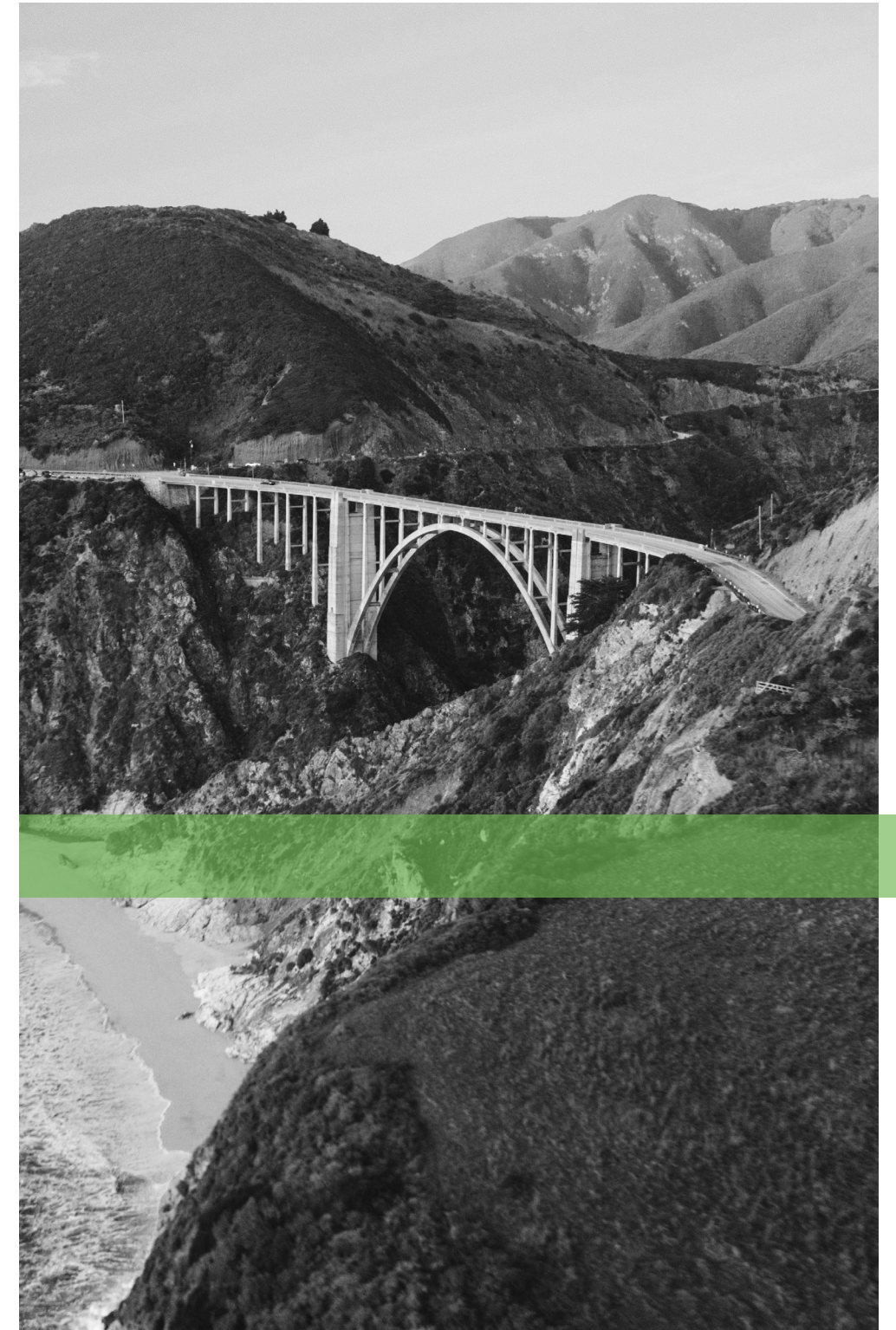


California's most recent set of regulations were initiated in November 2024. After two rounds of public comments and substantial [revisions](#) to the proposals, final rules were approved by the CPPA Board and the California Office of Administrative Law. The final rules become operational on 1 January 2026 and provide clarity on issues including cybersecurity audits, risk assessments, and automated decisionmaking technology.

In Colorado, the attorney general's office released the finalized [Colorado Privacy Act Rules](#) in March 2023 to implement the Colorado Privacy Act. Following the passage of [SB 24-041](#) in October 2024, which added protections for the online activity of minors, the Department of Law is considering [amendments](#) to the Colorado Privacy Act Rules. Prior to commencing a formal notice-and-comment rulemaking period, the Department of Law accepted public input on targeted pre-rulemaking [questions](#) — on issues such as system design features, the "willfully disregards" standard, and additional topics — until 11 July.

In New Jersey, the Office of Consumer Protection proposed rules under the New Jersey Data Privacy Act on 2 June 2025. The office is currently working to finalize the proposed rules, reviewing public comments after an active comment period that closed on 2 September 2025.

Meanwhile, the New Jersey legislature is considering an amendment bill, [A4741](#), which is in committee as of the time of this writing, that would clarify rulemaking in that state and require the Director of the Division of Consumer Affairs in the Department of Law and Public Safety to establish standards for the de-identification of personal data. The bill would also permit the director to allow exceptions to the requirements of de-identification or prohibitions on de-identification, provided there is an expected public benefit and that such exceptions are limited to purposes of medical studies or preventing/alleviating environmental hazards.





Enforcement

How are US privacy laws being enforced?

Privacy-related enforcement and compliance activities picked up in 2025 across the states, especially in California and Texas. While the CCPA is the sole comprehensive state privacy law to include a private right of action and enable [private enforcement](#) over data breaches, the bulk of the enforcement of U.S. state privacy laws is carried out by public agencies.

In July, California Attorney General Rob Bonta settled with Healthline.com for alleged [CCPA violations](#), levying a fine of USD1.55 million — the largest settlement under the CCPA to date. The California Privacy Protection Agency has also stepped into its role as CCPA enforcer with vigor, settling allegations against auto manufacturer [Honda](#) and clothing retailer [Todd Snyder](#). It has also taken action against data brokers for failing to register and pay a fine in violation of California's DELETE Act, inking multiple [settlements](#) as well as an [order](#) requiring a Florida data broker to pay a USD46,000 fine, the maximum possible under the law.

Meanwhile, Connecticut settled its first enforcement action under its consumer privacy law when [TicketNetwork](#) agreed to pay USD85,000 for alleged deficiencies related to its privacy policy and data rights mechanisms, which it did not resolve during the cure period.

Texas Attorney General Ken Paxton filed the first ever [formal lawsuit](#) under a state comprehensive privacy law in January 2025, alleging that Allstate and its subsidiary Arity tracked consumers' driving data in violation of the Texas Data Privacy and Security Act. As an expanded team of attorneys covering privacy and data matters came online, the Texas AG has made a splash beyond the state's comprehensive consumer privacy law. The office has announced investigations and lawsuits over the past year related to a half-dozen other Texas consumer protection, privacy and security laws, and has garnered billions of dollars in settlements under the state's biometric privacy law.

On the less visible side of enforcement, many states' privacy laws provide a cure period, where the attorney general must send notice of potential violations to controllers and give them an opportunity to remedy the issue and avoid official action. These notices are private, so there are no hard numbers. However, the attorneys general of Connecticut and [Oregon](#) have released reports indicating that they have sent dozens of cure notices in the initial enforcement periods — in the first year for [Connecticut](#) and the first six months for Oregon.

Stepping up their privacy enforcement actions, state attorneys general and the CPPA have been simultaneously proactive in releasing compliance guidance and resources for the business community and consumers alike. The reports mentioned above provide guidance for businesses and consumers on what the enforcers are focusing on. Oregon followed up on its six-month report with a quarterly [report](#) on enforcement in Q1 2025 that summarizes consumer complaints submitted to their web portal. [Connecticut](#) and [New Jersey](#) have published FAQs about their respective laws on their websites. These and subsequent pieces of such guidance are intended to provide the regulated community with principles to follow and to highlight the agency's observations of noncompliance.

At the IAPP's Global Privacy Summit in April 2025, a [panel](#) of enforcers from the CCPA, Colorado, and Oregon emphasized the need for cooperation and transparency across sectors. Along those lines, multiple states have come together to form the [Consortium of Privacy Regulators](#), which aims to combine forces and coordinate enforcement among its members. Regulators are still feeling out how best to enforce their states' laws, but they are learning quickly — and with more and more state privacy laws coming into effect, it looks like enforcement is not going to slow down anytime soon.

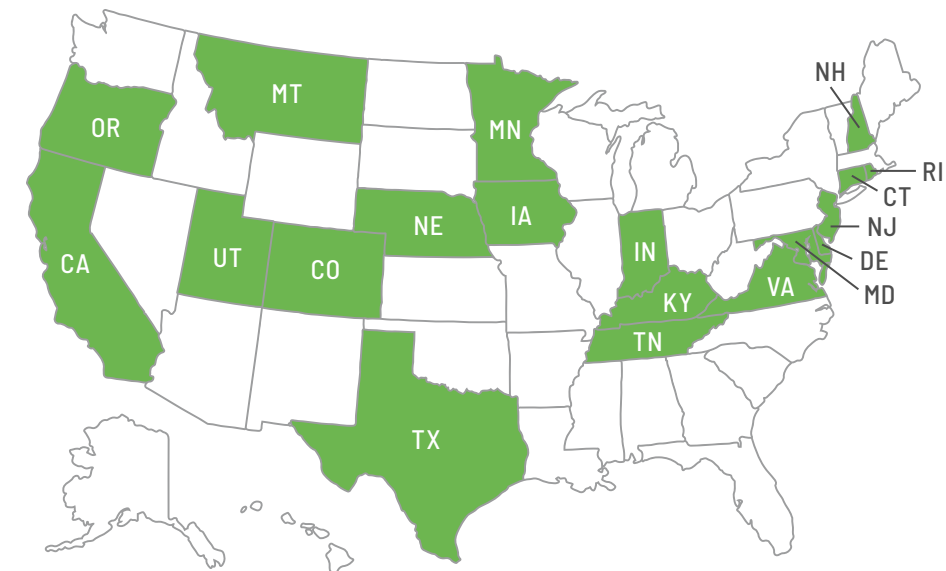


Comprehensive US state privacy laws at-a-glance

The US state privacy quilt

Across the 19 comprehensive U.S. state privacy laws that have been enacted so far, legislatures have taken at least two primary approaches to lawmaking. While California crafted its own approach, the other states initially based their laws on a version of the yet-to-pass Washington Privacy Act, which was introduced in 2019. Some of the latest states to pass these laws, including Maryland and Minnesota, have made more substantial tweaks, such as enhanced data minimization requirements and expanded automated decision-making rules, respectively. As these state-level snapshots reveal, each newly enacted, comprehensive privacy law brings iterative changes to definitions, scope and enforceability of existing legislation.

Comprehensive US state privacy laws



Note: Clicking on each state will bring you to the corresponding page.

California Consumer Privacy Act

CAL. CIV. CODE § 1798.100, ET SEQ
AMENDED BY THE CALIFORNIA PRIVACY RIGHTS ACT OF 2020
Enacted: 28 June 2018
Effective: 1 Jan. 2020

As the first U.S. comprehensive privacy law to be passed, the CCPA has long stood out. Amended by the CPRA ballot measure passed in 2020, California's CCPA is unique in several respects. For example, California is also the only state requiring notice at collection. Also, with the CPRA amendments to the CCPA, California is now the only state that gives consumers the right to limit the use and disclosure of sensitive personal information, though other states require opt-in consent for the sale of this data. Also, California is the only state with a dedicated privacy rulemaking and enforcement agency, the CPPA, and the only one that allows for a limited PRA for data breaches.

APPLICABILITY THRESHOLDS		
Does business in the state of California	AND	generates at least USD25 million in annual revenue
		OR
		controls or processes the personal data of 100,000 or more unique consumers
		OR
		derives more than 50% of its revenue from the sale of personal data

KEY DEFINITIONS	
Consumer	"A natural person who is a California resident."
Business	"A sole proprietorship, partnership, limited liability company, corporation, association or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that collects consumers' personal information, or on the behalf of which such information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information, that does business in the State of California."
Service provider	"A person that processes personal information on behalf of a business and that receives from or on behalf of the business consumer's personal information for a business purpose pursuant to a written contract."
Third party	"The business with whom the consumer intentionally interacts and that collects personal information from the consumer as part of the consumer's current interaction with the business," a service provider to the business or a contractor.
Personal information	"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."
	Does not include publicly available information, lawfully obtained, truthful information that is a matter of public concern, aggregated or deidentified data.
Sale	"Selling, 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 monetary or other valuable consideration."
	"A business does not sell personal information when: a. A consumer uses or directs the business to intentionally disclose personal information or interact with one or more third parties. b. The business uses or shares an identifier for a consumer who has opted out of the sale of the consumer's personal information or limited the use of the consumer's sensitive personal information for the purposes of alerting persons that the consumer has opted out of the sale of the consumer's personal information or limited the use of the consumer's sensitive personal information. c. The business transfers to a third party the personal information of a consumer as part of a merger (or) acquisition."
Child	The same meaning as provided in the Children's Online Privacy Protection Act, which designates a child as someone under 13 years of age.

EXEMPTIONS	
Government	E
Nonprofits	E
Higher education	⊗
National securities associations	⊗
Employee/commercial B2B	⊗
GLBA	D
HIPAA	D
FERPA	D
FCRA	D
DPPA	D

E Entity-level exemption D Data-level exemption ⊗ No exemption

CONSUMER RIGHTS		
Access		✓
Correct		✓
Delete		✓
Opt out of processing for ...	Targeted advertising/cross-contextual behavioral advertising	✓
	Sale of personal data	✓
	Profiling	✓
Portability		✓
Limit the use and disclosure of sensitive personal information		✓

✓ Applies to all personal data of a consumer held by a regulated entity

SENSITIVE INFORMATION	
Recognized categories of sensitive information:	✓
→ Racial or ethnic origin	
→ Religious beliefs	
→ Philosophical beliefs	
→ Sexual orientation/sexuality	
→ Sex life	
→ Citizenship or immigration/citizenship status	
→ Genetic or biometric data for purposes of uniquely identifying an individual	
→ Genetic or biometric data	
→ Precise geolocation	
→ Consumer health data	
→ Social Security numbers, driver's licenses, state identification cards or passport numbers	
→ Finance-related information	
→ Union membership	
→ Contents of a consumer's mail, email and text messages unless the business is the intended recipient of the communication	
→ Biological or neural data	
→ Mental or physical health data e.g., conditions, diagnoses, treatments	
→ Children's Data	

Colorado Privacy Act

COLO. REV. STAT. § 6-1-1301, ET SEQ.
AMENDED BY SB 25-276

Enacted: 7 July 2021
Effective: 1 July 2023

Colorado has been one of the busiest states adding to and amending its privacy law, having promulgated rules in 2023 and amended them three times in 2024. Those amendments include a first-in-the-nation designation of neural data as sensitive, a new duty of care to avoid heightened risk of harm to minors and extended protections for biometric data. In 2025, Colorado's SB 25-276 was one of the most significant amendment bills passed; the bill modified the definition of "precise geolocation data" and included it within the definition of "sensitive data"; it also prohibited controllers from "selling" sensitive data without consent.

APPLICABILITY THRESHOLDS		
Does business in the state of Colorado	AND	controls or processes the personal data of 100,000 or more unique consumers
		OR controls or processes the personal data of 25,000 or more unique consumers and derives any revenue or discount on the price of any goods or services from the sale of personal data

KEY DEFINITIONS	
Consumer	"An individual who is a Colorado resident acting only in an individual or household context."
	"Does not include an individual acting in a commercial or employment context, as a job applicant, or as a beneficiary of someone acting in an employment context."
Controller	"A person that, alone or jointly with others, determines the purposes for and means of processing personal data."
Processor	"A person that processes personal data on behalf of a controller."
Third party	"A person, public authority, agency, or body other than the consumer, controller, processor, or an affiliate of the processor or the controller."
Personal data	"Information that is linked or reasonably linkable to an identified or identifiable individual."
	"Does not include de-identified data or publicly available information."
Sale	"The exchange of personal data for monetary or other valuable consideration by the controller to a third party."
	Does not include the disclosure of personal data: → To a processor that processes personal data on behalf of the controller. → To third party for the purposes of providing a product or service requested by the consumer. → To a controller's affiliate. → That the consumer intentionally made available to the general public via a channel of mass media and did not restrict to a specific audience. → To a third party as part of a merger, acquisition, bankruptcy or other transaction.
Child	"An individual under thirteen years of age."

EXEMPTIONS	
Government	D
Nonprofits	⊗
Higher education	E
National securities associations	E
Employee/commercial B2B	D*
GLBA	E/D
HIPAA	D
FERPA	D
FCRA	D
DPPA	D

E Entity-level exemption D Data-level exemption ⊗ No exemption

*Note: The Colorado Privacy Act, as amended by HB24-1130, applies to employers' collection and use of biometric data of employees and independent contractors.

SENSITIVE INFORMATION	
Recognized categories of sensitive information:	✓
→ Racial or ethnic origin	
→ Religious beliefs	
→ Mental or physical health data e.g., conditions, diagnoses, treatments	
→ Sexual orientation/sexuality	
→ Sex life	
→ Citizenship or immigration/ citizenship status	
→ Genetic or biometric data for purposes of uniquely identifying an individual	
→ Children's data	
→ Biological or neural data	
→ Precise geolocation	

CONSUMER RIGHTS		
Access		✓
Correct		✓
Delete		✓
Opt out of processing for ...	Targeted advertising/cross-contextual behavioral advertising	✓
	Sale of personal data	✓
	Profiling	✓
Portability		✓

✓ Applies to all personal data of a consumer held by a regulated entity

Connecticut Data Privacy Act

CONN. GEN STAT. § 42-515, ET SEQ.
AMENDED BY SB 1295

Enacted: 10 May 2022
Effective: 1 July 2023

The fifth state to pass comprehensive privacy legislation, Connecticut also drew heavily from the Virginia-Colorado consensus that was the dominant model for U.S. state privacy legislation through 2022. Through the amendments of SB 1295, which were passed in June 2025 and take effect July 2026, the Connecticut Data Privacy Act sees significant changes to its scope. These amendments include lowering the applicability thresholds for the control, processing and sale of consumers' sensitive and personal data; removing the entity-level exemption for GLBA; revising the definition of sensitive data; expanding privacy notice obligations; adding new requirements for "impact assessments" for profiling, which are separate from the Connecticut Data Privacy Act's existing data protection impact assessments; and adding enhanced protections for children's data.

APPLICABILITY THRESHOLDS		
Does business in the state of Connecticut	AND	controls or processes the personal data of 35,000 or more unique consumers OR controls or processes any consumers' sensitive data OR offers consumers' personal data for sale in trade or commerce*

KEY DEFINITIONS	
Consumer	An individual who is a Connecticut resident.
	"Does not include an individual acting in a commercial or employment context."
Controller	"An individual who, or legal entity that, alone or jointly with others determines the purpose and means of processing personal data."
Processor	"An individual who, or legal entity that, processes personal data on behalf of a controller."
Third party	"An individual or legal entity, such as a public authority, agency or body, other than the consumer, controller or processor or an affiliate of the processor or the controller."
Personal data	"Any information that is linked or reasonably linkable to an identified or identifiable individual."
	"Does not include de-identified data or publicly available information."
Sale	"The exchange of personal data for monetary or other valuable consideration by the controller to a third party."
	Does not include the disclosure of personal data: → To a processor that processes personal data on behalf of the controller. → To third party for purposes of providing a product or service requested by the consumer. → To a controller's affiliate. → When the consumer directs the controller to disclose the personal data or intentionally uses the controller to interact with a third party. → That the consumer intentionally made available to the general public via a channel of mass media and did not restrict to a specific audience. → To a third party as part of a merger, acquisition, bankruptcy or other transaction.
Child	The same meaning as provided in COPPA, which designates a child as someone under 13 years of age.

EXEMPTIONS	
Government	E
Nonprofits	E
Higher education	E
National securities associations	E
Employee/commercial B2B	D
GLBA	D
HIPAA	E/D
FERPA	D
FCRA	D
DPPA	D

E Entity-level exemption

D Data-level exemption

CONSUMER RIGHTS		
Access		✔
Correct		✔
Delete		✔
Opt out of processing for ...	Targeted advertising/ cross-contextual behavioral advertising	✔
	Sale of personal data	✔
	Profiling	✔
Portability		✔

✔ Applies to all personal data of a consumer held by a regulated entity

SENSITIVE INFORMATION	
Recognized categories of sensitive information:	✔
→ Racial or ethnic origin	
→ Religious beliefs	
→ Mental or physical health data e.g., conditions, diagnoses, treatments	
→ Sexual orientation/sexuality	
→ Sex life	
→ Citizenship or immigration/ citizenship status	
→ Genetic or biometric data for purposes of uniquely identifying an individual	
→ Children's data	
→ Precise geolocation	
→ Status as victim of crime	
→ Consumer health data	
→ Status as transgender or nonbinary	
→ Social Security numbers, driver's licenses, state identification cards or passport numbers	
→ Biological or neural data-Social	
→ Finance-related information	

Enacted: 11 Sept. 2023
Effective: 1 Jan. 2025

APPLICABILITY THRESHOLDS

KEY DEFINITIONS	
Consumer	An individual who is a resident of Delaware.
	"Does not include an individual acting in a commercial or employment context."
Controller	"A person that, alone or jointly with others, determines the purpose and means of processing personal data."
Processor	"A person that processes personal data on behalf of a controller."
Third party	A natural or legal person, public authority or body other than the consumer, the controller, the processor, or an affiliate of the processor or controller.
Personal data	"Any information that is linked or reasonably linkable to an identified or identifiable individual."
	"Does not include identified data or publicly available information."
Sale	"The exchange of personal data for monetary or other valuable consideration by a controller to a third party."
	Does not include the disclosure of personal data: → To a processor that processes the personal data on the controller's behalf. → To a third party for purposes of providing a product or service requested by the consumer. → To the controller's affiliate. → When the consumer directs the controller to disclose the personal data or intentionally uses the controller to interact with a third party. → That the consumer intentionally made available to the general public through a mass media channel and did not restrict to a specific audience. → To a third party as part of a merger or acquisition.
Child	The same meaning as provided in COPPA, which designates a child as someone under 13 years of age.

Government	E
Nonprofits	⊗*
Higher education	⊗
National securities associations	E
Employee/commercial B2B	D
GLBA	E
HIPAA	D
FERPA	D
FCRA	D
DPPA	D

*Note: Only some nonprofit data is exempt. The law does not apply to certain data held by nonprofits "that provide services to victims or witnesses of child abuse, domestic violence, human trafficking, sexual assault, violent felonies or stalking."

Access	
Correct	
Delete	
Opt out of processing for ...	Targeted advertising/cross-contextual behavioral advertising
	Sale of personal data
	Profiling
Portability	

 Applies to consumer-provided data only

Recognized categories of sensitive information:

- Racial or ethnic origin
- Religious beliefs
- Mental or physical health data e.g., conditions, diagnoses, treatments
- Sexual orientation/sexuality
- Sex life
- Citizenship or immigration status
- Genetic or biometric data
- Children's data
- Precise geolocation
- Status as transgender or nonbinary

Indiana Consumer Data Protection Act

IND. CODE §§ 24-15-1-1, ET SEQ.

Enacted: 1 May 2023

Effective: 1 Jan. 2026

While an earlier version of the Indiana Consumer Data Protection Act was modeled loosely upon the EU General Data Protection Regulation and the CCPA, the version passed unanimously by the Indiana House and Senate the following year mostly followed Virginia's example set. Without introducing any significant burdens or unforeseen modifications to the emerging U.S. state privacy law framework, Indiana's law was one of the last to pass before the wave of unique laws passed in 2024 washed away the pattern of uniformity.

APPLICABILITY THRESHOLDS		
Does business in the state of Indiana	AND	controls or processes the personal data of 100,000 or more unique consumers
		OR controls or processes the personal data of 25,000 or more unique consumers and derives more than 50% of its revenue from the sale of personal data

KEY DEFINITIONS	
Consumer	"An individual who is a resident of Indiana and is acting only for a personal, family, or household purpose."
	"Does not include a natural person acting in a commercial or employment context."
Controller	"A person that, alone or jointly with others, determines the purpose and means of processing personal data."
Processor	"A person that processes personal data on behalf of a controller."
Third party	"A natural or legal person, public authority, or body other than the consumer, the controller, the processor, or an affiliate of the processor or controller."
Personal data	"Information that is linked or reasonably linkable to an identified or identifiable individual."
	"Does not include identified data or publicly available information."
Sale	"The exchange of personal data for monetary or other valuable consideration by a controller to a third party."
	Does not include the disclosure of personal data: → To a processor that processes the personal data on the controller's behalf. → To a third party for the purposes of providing a product or service requested by the consumer or the parent of a child to whom the personal data pertains. → To the controller's affiliate. → That the consumer intentionally made available to the general public through a mass media channel and did not restrict to a specific audience. → To a third party as part of a merger or acquisition.
Child	"Any individual who is less than 13 years of age."

EXEMPTIONS	
Government	E
Nonprofits	E
Higher education	E
National securities associations	⊗
Employee/commercial B2B	D
GLBA	E/D
HIPAA	E/D
FERPA	D
FCRA	D
DPPA	D

E Entity-level exemption D Data-level exemption ⊗ No exemption

CONSUMER RIGHTS		
Access		
Correct		
Delete		
Opt out of processing for ...	Targeted advertising/cross-contextual behavioral advertising	
	Sale of personal data	
	Profiling	
Portability		

✓ Applies to all personal data of a consumer held by a regulated entity
☑ Applies to consumer-provided data only

SENSITIVE INFORMATION	
Recognized categories of sensitive information:	✓
→ Racial or ethnic origin	
→ Religious beliefs	
→ Mental or physical health data e.g., conditions, diagnoses, treatments	
→ Sexual orientation/sexuality	
→ Citizenship or immigration status	
→ Genetic or biometric data for purposes of uniquely identifying an individual	
→ Children's data	
→ Precise geolocation	

Iowa Consumer Data Protection Act

IOWA CODE §§ 715D.1, ET SEQ.

Enacted: 19 March 2023

Effective: 1 Jan. 2025

While it took several years for Iowa to pass its Consumer Data Protection Act, it adopted many of the same rights, obligations and exemptions as U.S. state privacy laws passed in the interim. It is one of the few states to leave out certain consumer rights, including the right to correct and the right to opt out of processing for targeted advertising and profiling. Before the state's General Assembly adjourned in May 2025, an amendment failed to gain momentum that would have changed the definition of a child from a person younger than 13 to younger than 18 and expanded the definitions of "health record" and "sensitive data."

APPLICABILITY THRESHOLDS		
Does business in the state of Iowa	AND	controls or processes the personal data of 100,000 or more unique consumers
		OR controls or processes the personal data of 25,000 or more unique consumers and derives more than 50% of its revenue from the sale of personal data

KEY DEFINITIONS	
Consumer	"A natural person who is a resident of the state acting only in an individual or household context."
	"Does not include a natural person acting in an employment or commercial context."
Controller	"A person who, alone or jointly with others, determines the purpose and means of processing personal data."
Processor	"A person processes personal data on behalf of a controller."
Third party	"An individual or legal entity, such as a public authority, agency or body, other than the consumer, controller or processor or an affiliate of the controller or processor."
Personal data	"Any information that is linked or reasonably linkable to an identified or identifiable individual."
	"Does not include deidentified data or publicly available information."
Sale	"The exchange of personal data for monetary consideration by the controller to a third party."
	Does not include the disclosure of personal data: → To a processor that processes the personal data on the controller's behalf. → To a third party for purposes of providing a product or service requested by a consumer. → To the controller's affiliate. → That the consumer intentionally made available to the general public through a mass media channel and did not restrict to a specific audience. → When the consumer directs the controller to disclose the personal data or intentionally uses the controller to interact with a third party → To a third party as part of a merger or acquisition.
Child	Any natural person younger than 13 years of age.

EXEMPTIONS	
Government	E
Nonprofits	E
Higher education	E
National securities associations	⊗
Employee/commercial B2B	D
GLBA	E/D
HIPAA	E/D
FERPA	D
FCRA	D
DPPA	D

E Entity-level exemption D Data-level exemption ⊗ No exemption

CONSUMER RIGHTS		
Access		✓
Correct		⊗
Delete		✓
Opt out of processing for ...	Targeted advertising/cross-contextual behavioral advertising	⊗
	Sale of personal data	✓
	Profiling	⊗
Portability		☑

✓ Applies to all personal data of a consumer held by a regulated entity
☑ Applies to consumer-provided data only ⊗ Does not apply

SENSITIVE INFORMATION	
Recognized categories of sensitive information:	✓
→ Racial or ethnic origin	
→ Religious beliefs	
→ Mental or physical health data e.g., conditions, diagnoses, treatments	
→ Sexual orientation/sexuality	
→ Citizenship or immigration status	
→ Genetic or biometric data for purposes of uniquely identifying an individual	
→ Children's data	
→ Precise geolocation	

Kentucky Consumer Data Protection Act

KEN. REV. STAT. § 367.3611, ET SEQ.
AMENDED BY HB 473

Enacted: 4 April 2024
Effective: 1 Jan. 2026

Another progeny of Virginia's law, Kentucky's HB 15 sought to bring the Bluegrass State into alignment with its neighbors in Tennessee and Indiana. With the passage of HB 473 in March 2025, Kentucky's privacy law has been amended to add an entity-level exemption for HIPAA and requires data protection impact assessments for profiling that presents "a reasonably foreseeable risk" of "unlawful, disparate impact on consumers."

APPLICABILITY THRESHOLDS		
Does business in the state of Kentucky	AND	controls or processes the personal data of 100,000 or more unique consumers
		OR controls or processes the personal data of 25,000 or more unique consumers and derives more than 50% of its revenue from the sale of personal data

KEY DEFINITIONS	
Consumer	"A natural person who is a resident of the Commonwealth of Kentucky acting only in an individual context."
	"Does not include a person acting in a commercial or employment context."
Controller	"The natural or legal person that, alone or jointly with others, determines the purpose and means of processing personal data."
Processor	"A natural or legal entity that processes personal data on behalf of a controller."
Third party	"A natural or legal person, public authority, agency, or body other than the consumer, controller, processor or an affiliate of the processor of the controller."
Personal data	"Any information that is linked or reasonably linkable to an identified or identifiable person."
	"Does not include de-identified data or publicly available information."
Sale	"The exchange of personal data for monetary consideration by the controller to a third party."
	Does not include the disclosure of personal data: → To a processor that processes the personal data on the controller's behalf. → To a third party for purposes of providing a product or service requested by the consumer. → To the controller's affiliate. → That the consumer intentionally made available to the general public through a mass media channel and did not restrict to a specific audience. → To a third party as part of a merger or acquisition..
Child	The same meaning as provided in COPPA, which designates a child as someone under 13 years of age.

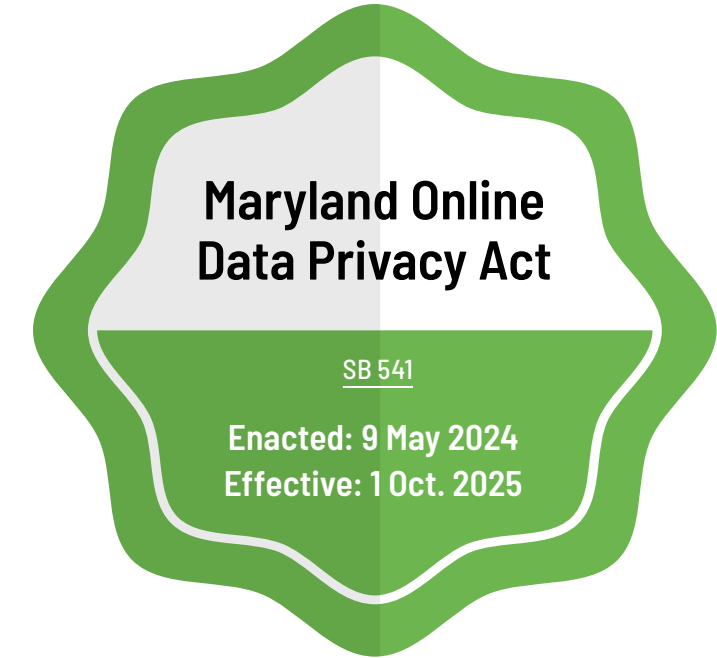
EXEMPTIONS	
Government	E
Nonprofits	E
Higher education	E
National securities associations	⊗
Employee/commercial B2B	D
GLBA	E/D
HIPAA	E/D
FERPA	D
FCRA	D
DPPA	D

E Entity-level exemption D Data-level exemption ⊗ No exemption

CONSUMER RIGHTS	
Access	✓
Correct	✓
Delete	✓
Opt out of processing for ...	Targeted advertising/cross-contextual behavioral advertising
	Sale of personal data
	Profiling
Portability	✓

✓ Applies to all personal data of a consumer held by a regulated entity

SENSITIVE INFORMATION	
Recognized categories of sensitive information:	✓
→ Racial or ethnic origin	
→ Religious beliefs	
→ Mental or physical health data e.g., conditions, diagnoses, treatments	
→ Sexual orientation/sexuality	
→ Citizenship or immigration status	
→ Genetic or biometric data for purposes of uniquely identifying an individual	
→ Children's data	
→ Precise geolocation	



Maryland's legislature caused waves when it introduced a heightened data-minimization standard limiting collection of personal data to what is "reasonably necessary and proportionate to provide or maintain a specific product or service requested by the consumer." For sensitive data, controllers can only collect, process or share sensitive data when it is strictly necessary to provide or maintain a requested product or service, and Maryland's law prohibits selling sensitive data entirely. Maryland's law becomes effective 1 Oct. 2025.

APPLICABILITY THRESHOLDS		
Does business in the state of Maryland	AND	controls or processes the personal data of 35,000 or more unique consumers
		OR controls or processes the personal data of 10,000 or more unique consumers and derives more than 20% of its revenue from the sale of personal data

KEY DEFINITIONS	
Consumer	An individual who is a resident of Maryland.
	"Does not include an individual acting in a commercial or employment context."
Controller	"A person that, alone or jointly with others, determines the purpose and means of processing personal data."
Processor	"A person that processes personal data on behalf of a controller."
Third party	"A person other than the relevant consumer, controller, processor or an affiliate of the processor of relevant personal data."
Personal data	"Any information that is linked or can be reasonably linked to an identified or identifiable consumer."
	"Does not include de-identified data or publicly available information."
Sale	"The exchange of personal data by a controller, a processor, or an affiliate of a controller or processor to a third party for monetary or other valuable consideration."
	Does not include the disclosure of personal data: → To a processor that processes the personal data on the controller's behalf. → To a third party for purposes of providing a product or service requested by the consumer. → To the controller's affiliate. → When the consumer directs the controller to disclose the personal data or intentionally uses the controller to interact with a third party. → That the consumer intentionally made available to the general public through a mass media channel and did not restrict to a specific audience. → To a third party as part of a merger or acquisition.
Child	The same meaning as provided in COPPA, which designates a child as someone under 13 years of age.

EXEMPTIONS	
Government	E
Nonprofits	E*
Higher education	⊗
National securities associations	E
Employee/commercial B2B	D
GLBA	E
HIPAA	D
FERPA	D
FCRA	D
DPPA	D

E Entity-level exemption D Data-level exemption ⊗ No exemption

*Note: Only nonprofits that process or share personal data solely for the purpose of assisting either law enforcement agencies in investigating criminal or fraudulent acts relating to insurance or first responders responding to catastrophic events are exempt.

CONSUMER RIGHTS		
Access		✓
Correct		✓
Delete		✓
Opt out of processing for ...	Targeted advertising/cross-contextual behavioral advertising	✓
	Sale of personal data	✓
	Profiling	✓
Portability		✓

✓ Applies to all personal data of a consumer held by a regulated entity

SENSITIVE INFORMATION	
Recognized categories of sensitive information:	✓
→ Citizenship or immigration status	
→ Consumer health data	
→ Racial or ethnic origin	
→ National origin	
→ Religious beliefs	
→ Sexual orientation/sexuality	
→ Sex life	
→ Status as transgender or nonbinary	
→ Genetic or biometric data for purposes of uniquely identifying an individual	
→ Genetic or biometric data	
→ Children's data	
→ Precise geolocation	

Minnesota Consumer Data Privacy Act

HF 4757

Enacted: 24 May 2024

Effective: 31 July 2025

Passed in 2024 as part of a larger omnibus bill, Minnesota's privacy law took the state privacy landscape in new directions with its provisions addressing profiling. Under the bill, a consumer "has the right to question the result of the profiling, to be informed of the reason that the profiling resulted in the decision, and, if feasible, to be informed of what actions the consumer might have taken to secure a different decision in the future." With increased reliance on privacy laws to address proliferating artificial intelligence harms, Minnesota's profiling framework could spread to other states.

APPLICABILITY THRESHOLDS		
Does business in the state of Minnesota	AND	controls or processes the personal data of 100,000 or more unique consumers
		OR controls or processes the personal data of 25,000 or more unique consumers and derives more than 25% of its revenue from the sale of personal data

KEY DEFINITIONS	
Consumer	"A natural person who is a Minnesota resident acting only in an individual or household context."
	"Does not include a natural person acting in a commercial or employment context."
Controller	"The natural or legal person who, alone or jointly with others, determines the purpose and means of the processing of personal data."
Processor	"A natural or legal person who processes personal data on behalf of the controller."
Third party	"A natural or legal person, public authority, agency, or body other than the consumer, controller, processor, or an affiliate of the processor or the controller."
Personal data	"Any information that is linked or reasonably linkable to an identified or identifiable natural person."
	"Does not include publicly deidentified data or publicly available information."
Sale	"The exchange of personal data for monetary or other valuable consideration by the controller to a third party."
	Does not include the disclosure of personal data: → To a processor that processes the personal data on the controller's behalf. → To a third party for purposes of providing a product or service requested by the consumer. → To the controller's affiliate. → When the consumer directs the controller to disclose the personal data or intentionally uses the controller to interact with a third party. → That the consumer intentionally made available to the general public through a mass media channel and did not restrict to a specific audience. → To a third party as part of a merger or acquisition.
Child	The same meaning as provided in the COPPA, which designates a child as someone under 13 years of age.

EXEMPTIONS	
Government	E
Nonprofits	⊗*
Higher education	⊗*
National securities associations	⊗
Employee/commercial B2B	D
GLBA	D
HIPAA	D
FERPA	D
FCRA	D
DPPA	D

E Entity-level exemption D Data-level exemption ⊗ No exemption

*Note: Nonprofits that detect insurance fraud are exempt. Postsecondary institutions regulated by the Office of Higher Education are not required to comply until 31 July 2029.

CONSUMER RIGHTS		
Access		✓
Correct		✓
Delete		✓
Opt out of processing for ...	Targeted advertising/cross-contextual behavioral advertising	✓
	Sale of personal data	✓
	Profiling	✓
Portability		✓

✓ Applies to all personal data of a consumer held by a regulated entity

SENSITIVE INFORMATION	
Recognized categories of sensitive information:	✓
→ Racial or ethnic origin	
→ Religious beliefs	
→ Mental or physical health data e.g., conditions, diagnoses, treatments	
→ Sexual orientation/sexuality	
→ Citizenship or immigration status	
→ Genetic or biometric data for purposes of uniquely identifying an individual	
→ Children's data	
→ Precise geolocation	

Montana Consumer Data Privacy Act

MONT. CODE §§ 30-14-2801, ET SEQ.
AMENDED BY SB 297

Enacted: 19 May 2023
Effective: 1 Oct. 2024

The Montana Consumer Privacy Act has been noted for its adherence to the language and standards set by Connecticut's privacy law. In further lockstep this year with developments in Connecticut, Montana also revised its privacy law this year, lowering its thresholds for applicability and thus expanding its scope. Montana removed the entity-level exemption for financial institutions and entities regulated under the Gramm-Leach-Bliley Act. It also narrowed the law's original, broad exemption for non-profits, making the law applicable to most non-profits operating in the state. Additionally, new requirements were added concerning the processing of personal data about consumers under the age of 18.

APPLICABILITY THRESHOLDS		
Does business in the state of Montana	AND	controls or processes the personal data of 25,000 or more unique consumers
		controls or processes the personal data of 15,000 or more unique consumers and OR derives more than 25% of its revenue from the sale of personal data

KEY DEFINITIONS	
Consumer	An individual who is a resident of Montana.
	"Does not include an individual acting in an employment or commercial context."
Controller	"An individual who or legal entity that, alone or jointly with others, determines the purpose and means of processing personal data."
Processor	"An individual who or legal entity that processes personal data on behalf of a controller."
Third party	"An individual or legal entity, such as a public authority, agency, or body, other than the consumer, controller, or processor or an affiliate of the controller or processor."
Personal data	"Any information that is linked or reasonably linkable to an identified or identifiable individual."
	"Does not include de-identified data or publicly available information."
Sale	"The exchange of personal data for monetary or other valuable consideration by the controller to a third party."
	Does not include the disclosure of personal data: → To a processor that processes the personal data on the controller's behalf. → To a third party for purposes of providing a product or service requested by a consumer. → To the controller's affiliate. → When the consumer directs the controller to disclose the personal data or intentionally uses the controller to interact with a third party → That the consumer intentionally made available to the general public through a mass media channel and did not restrict to a specific audience. → To a third party as part of a merger or acquisition.
Child	"An individual under 13 years of age."

EXEMPTIONS	
Government	E
Nonprofits	✗*
Higher education	E
National securities associations	E
Employee/commercial B2B	D
GLBA	D
HIPAA	E/D
FERPA	D
FCRA	D
DPPA	D

E Entity-level exemption D Data-level exemption

SENSITIVE INFORMATION	
Recognized categories of sensitive information:	✓
→ Racial or ethnic origin	
→ Religious beliefs	
→ Mental or physical health data e.g., conditions, diagnoses, treatments	
→ Sexual orientation/sexuality	
→ Sex life	
→ Citizenship or immigration status	
→ Genetic or biometric data for purposes of uniquely identifying an individual	
→ Children's data	
→ Precise geolocation	

CONSUMER RIGHTS		
Access		✓
Correct		✓
Delete		✓
Opt out of processing for ...	Targeted advertising/cross-contextual behavioral advertising	✓
	Sale of personal data	✓
	Profiling	✓
Portability		☑

✓ Applies to all personal data of a consumer held by a regulated entity
☑ Applies to consumer-provided data only

Nebraska
Data Privacy Act

LB 1074

Enacted: 17 April 2024
Effective: 1 Jan. 2026

Mirroring the unique applicability thresholds seen in Texas's privacy law, the Nebraska Data Privacy Act is notable for being the only other state to set the threshold at any control/processing or sale of personal data for an entity to fall within its scope. Like other entrants in the "class of 2024," Nebraska's law also contains provisions on universal opt-out mechanisms and dark patterns not seen in the earlier generations of U.S. state privacy legislation.

APPLICABILITY THRESHOLDS		
Does business in the state of Nebraska	AND	controls or processes the personal data of any consumers
	OR	engages in any sale of personal data

KEY DEFINITIONS	
Consumer	An individual who is a resident of Nebraska acting only in an individual or household context.
	"Does not include a person acting in a commercial or employment context."
Controller	"An individual or other person that, alone or jointly with others, determines the purpose and means of processing personal data."
Processor	A natural or legal entity "that processes personal data on behalf of a controller."
Third party	A natural or legal person, public authority, agency, or body other than the consumer, controller, processor or an affiliate of the processor of the controller.
Personal data	"Any information, including sensitive data, that is linked or reasonably linkable to an identified or identifiable individual, including pseudonymous data."
	"Does not include deidentified data or publicly available information."
Sale	"The exchange of personal data for monetary or other valuable consideration by the controller to a third party."
	Does not include the disclosure of personal data: → To a processor that processes the personal data on the controller's behalf. → To a third party for purposes of providing a product or service requested by the consumer. → To the controller's affiliate. → That the consumer intentionally made available to the general public through a mass media channel and did not restrict to a specific audience. → To a third party as part of a merger or acquisition.
Child	"An individual younger than thirteen years of age."

EXEMPTIONS	
Government	E
Nonprofits	E
Higher education	E
National securities associations	⊗
Employee/commercial B2B	D
GLBA	E
HIPAA	E/D
FERPA	D
FCRA	D
DPPA	D

E Entity-level exemption D Data-level exemption ⊗ No exemption

CONSUMER RIGHTS	
Access	✓
Correct	✓
Delete	✓
Opt out of processing for ...	Targeted advertising/cross-contextual behavioral advertising
	Sale of personal data
	Profiling
Portability	☑

✓ Applies to all personal data of a consumer held by a regulated entity
☑ Applies to consumer-provided data only

SENSITIVE INFORMATION	
Recognized categories of sensitive information:	✓
→ Racial or ethnic origin	
→ Religious beliefs	
→ Mental or physical health data e.g., conditions, diagnoses, treatments	
→ Sexual orientation/sexuality	
→ Citizenship or immigration status	
→ Genetic or biometric data for purposes of uniquely identifying an individual	
→ Children's data	
→ Precise geolocation	

New Hampshire Data Privacy Act

SB 255

Enacted: 16 Mar. 2023

Effective: 1 Jan. 2025

New Hampshire was the fourth state to give rulemaking authority to state officials, although, due to a subsequent amendment, those provisions did not come into effect. When SB 255-FN was originally signed on 6 March 2024, it included provisions for the New Hampshire Secretary of State to establish privacy notice standards and procedures for consumers to exercise their rights. A subsequent bill signed on 19 July 2024, HB 1220-FN, modified those provisions so as to eliminate the RSA 507-H rulemaking provisions, leaving just three states – California, Colorado and New Jersey – that grant rulemaking authority to a state agency.

APPLICABILITY THRESHOLDS		
Does business in the state of New Hampshire	AND	controls or processes the personal data of 35,000 or more unique consumers
		OR controls or processes the personal data of 10,000 or more unique consumers and derives more than 25% of its revenue from the sale of personal data

KEY DEFINITIONS	
Consumer	An individual who is a resident of New Hampshire.
	"Does not include an individual acting in a commercial or employment context."
Controller	"An individual who, or legal entity that, alone or jointly with others determines the purpose and means of processing personal data."
Processor	"An individual who, or legal entity that, processes personal data on behalf of a controller."
Third party	"An individual or legal entity, such as a public authority, agency, or body, other than the consumer, controller, or processor, or an affiliate of the processor or the controller."
Personal data	"Any information that is linked or reasonably linkable to an identified or identifiable individual."
	"Does not include de-identified data or publicly available information."
Sale	"The exchange of personal data for monetary or other valuable consideration by the controller to a third party."
	Does not include the disclosure of personal data: → To a processor that processes personal data on behalf of the controller. → To a third party for purposes of providing a product or service requested by the consumer. → To a controller's affiliate. → When the consumer directs the controller to disclose the personal data or intentionally uses the controller to interact with a third party. → That the consumer intentionally made available to the general public via a channel of mass media, and did not restrict to a specific audience. → To a third party as part of a merger, acquisition, bankruptcy or other transaction.
Child	The same meaning as provided in COPPA, which designates a child as someone under 13 years of age.

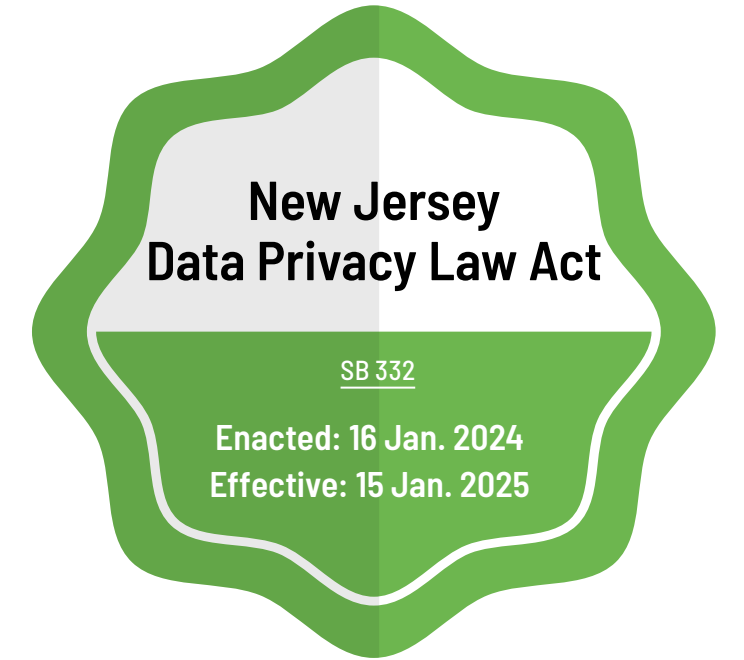
EXEMPTIONS	
Government	E
Nonprofits	E
Higher education	E
National securities associations	E
Employee/commercial B2B	D
GLBA	E/D
HIPAA	D
FERPA	D
FCRA	D
DPPA	D

E Entity-level exemption D Data-level exemption

CONSUMER RIGHTS		
Access		✓
Correct		✓
Delete		✓
Opt out of processing for ...	Targeted advertising/cross-contextual behavioral advertising	✓
	Sale of personal data	✓
	Profiling	✓
Portability		✓

✓ Applies to all personal data of a consumer held by a regulated entity

SENSITIVE INFORMATION	
Recognized categories of sensitive information:	✓
→ Racial or ethnic origin	
→ Religious beliefs	
→ Mental or physical health data e.g., conditions, diagnoses, treatments	
→ Sexual orientation/sexuality	
→ Sex life	
→ Citizenship or immigration status	
→ Genetic or biometric data for purposes of uniquely identifying an individual	
→ Children's data	



New Jersey's privacy law notably authorizes the state's director of the Division of Consumer Affairs to promulgate regulations, making it the third state to do so. It further joined California as the only other state to include financial information as a new category of sensitive data and to require data protection assessments prior to processing. With two amendment bills under consideration with requirements around de-identification and an exemption around detecting and preventing fraud, New Jersey may yet see a change to its privacy law in 2025.

APPLICABILITY THRESHOLDS		
Does business in the state of New Jersey	AND	controls or processes the personal data of 100,000 or more unique consumers
		OR controls or processes the personal data of 25,000 or more unique consumers and derives any revenue or discount on the price of any goods or services from the sale of personal data

KEY DEFINITIONS	
Consumer	An identified person who is a resident of New Jersey "acting only in an individual or household context."
	Does not include a person "acting in a commercial or employment context."
Controller	"An individual, or legal entity that, alone or jointly with others determines the purpose and means of processing personal data."
Processor	"A person, private entity, public entity, agency, or other entity that processes personal data on behalf of the controller."
Third party	"A person, private entity, public entity, agency, or entity other than the consumer, controller, or affiliate or processor of the controller."
Personal data	"Any information that is linked or reasonably linkable to an identified or identifiable person."
	"Does not include de-identified data or publicly available information."
Sale	"The sharing, disclosing, or transferring of personal data for monetary or other valuable consideration by the controller to a third party."
	Does not include the disclosure of personal data: → To a processor that processes the personal data on the controller's behalf. → To a third party for purposes of providing a product or service requested by the consumer. → To the controller's affiliate. → That the consumer intentionally made available to the general public through a mass media channel and did not restrict to a specific audience. → To a third party as part of a merger or acquisition.
Child	The same meaning as provided in COPPA, which designates a child as someone under 13 years of age.

EXEMPTIONS	
Government	E
Nonprofits	⊗
Higher education	⊗
National securities associations	⊗
Employee/commercial B2B	D*
GLBA	E
HIPAA	D
FERPA	⊗
FCRA	D
DPPA	D

E Entity-level exemption D Data-level exemption ⊗ No exemption

*Note: New Jersey's law exempts employee/commercial data insofar as its definition of consumer excludes people "acting in a commercial or employment context." However, the law does not incorporate a broader, clearer employee/B2B data exemption like those found in other state privacy laws.

CONSUMER RIGHTS	
Access	✓
Correct	✓
Delete	✓
Opt out of processing for ...	Targeted advertising/cross-contextual behavioral advertising
	Sale of personal data
	Profiling
Portability	✓

✓ Applies to all personal data of a consumer held by a regulated entity

SENSITIVE INFORMATION	
Recognized categories of sensitive information:	✓
→ Racial or ethnic origin	
→ Religious beliefs	
→ Mental or physical health data e.g., conditions, diagnoses, treatments	
→ Sexual orientation/sexuality	
→ Sex life	
→ Status as transgender or nonbinary	
→ Citizenship or immigration status	
→ Genetic or biometric data for purposes of uniquely identifying an individual	
→ Children's data	
→ Precise geolocation	
→ Finance-related information	

Oregon Consumer Privacy Act

OREGON SB 619
AMENDED BY HB 2008 AND HB 3875

Enacted: 23 June 2022
Effective: 1 July 2024

Oregon staked its claim on one side of a long but niche debate among policymakers by requiring controllers to, upon request by a consumer, disclose the list of specific third parties to which they have disclosed the consumer's personal data. Most states only require disclosure of the categories of third parties to which covered entities disclose data. Oregon regulators have highlighted this unique provision as at the vanguard of privacy law, but it may create operational challenges in an increasingly complicated and connected information ecosystem.

APPLICABILITY THRESHOLDS		
Does business in the state of Oregon	AND	controls or processes the personal data of 100,000 or more unique consumers
		OR controls or processes the personal data of 25,000 or more unique consumers and derives more than 25% of its revenue from the sale of personal data

KEY DEFINITIONS	
Consumer	A natural person who resides in Oregon.
	Does not include an individual acting in an employment or commercial context
Controller	"A person that, alone or jointly with another person, determines the purposes and means for processing personal data."
Processor	"A person that processes personal data on behalf of a controller."
Third party	"A person, a public corporation, including the Oregon Health and Science University and the Oregon State Bar, or a public body, other than a consumer, a controller, a processor or an affiliate of a controller or processor."
Personal data	"Data, derived data or any unique identifier that is linked to or is reasonably linkable to a consumer or to a device that identifies, is linked to or is reasonably linkable to one or more consumers in a household."
	"Does not include deidentified data or data that is lawfully available through federal, state or local government records or through widely distributed media; or a controller reasonably has understood to have been lawfully made available to the public by a consumer."
Sale	"A controller's act of exchanging personal data with a third party for money or other valuable consideration or, as appropriate, the completion of such an exchange."
	Does not include the disclosure of personal data: → To a processor. → To a controller's affiliate or to a third party for the purpose of enabling the controller to provide a product or service requested by a consumer. → To a third party as part of a merger or acquisition → When a consumer directs a controller to disclose the personal data or interact with one or more third parties. → Intentionally disclosed by the consumer to the public by means of mass media, if the disclosure is not restricted by a specific audience.
Child	"An individual under the age of 13."

EXEMPTIONS	
Government	E
Nonprofits	⊗*
Higher education	⊗
National securities associations	⊗
Employee/commercial B2B	D
GLBA	D
HIPAA	D
FERPA	D
FCRA	D
DPPA	D

E Entity-level exemption D Data-level exemption ⊗ No exemption

*Note: Oregon's law only exempts nonprofits that try to prevent insurance fraud and journalistic nonprofits.

CONSUMER RIGHTS		
Access		✓
Correct		✓
Delete		✓
Opt out of processing for ...	Targeted advertising/cross-contextual behavioral advertising	✓
	Sale of personal data	✓
	Profiling	✓
Portability		✓

✓ Applies to all personal data of a consumer held by a regulated entity

SENSITIVE INFORMATION	
Recognized categories of sensitive information:	✓
→ Racial or ethnic origin	
→ National origin	
→ Religious beliefs	
→ Mental or physical health data e.g., conditions, diagnoses, treatments	
→ Sexual orientation/sexuality	
→ Status as transgender or nonbinary	
→ Citizenship or immigration status	
→ Genetic or biometric data	
→ Children's data	
→ Precise geolocation	
→ Status as a victim of crime	

Rhode Island Data Transparency and Privacy Protection Act

H 7787

Enacted: 25 June 2024

Effective: 1 Jan. 2026

Rhode Island's privacy law broke cleanly from the Washington Privacy Act model in building on the existing requirement that entities must disclose to consumers the specific third parties to whom it sells personal data. In another U.S. state privacy law first, a controller must also disclose the third parties to whom a consumer may sell personally identifiable information – a separate, undefined term apart from personal data.

APPLICABILITY THRESHOLDS		
Does business in the state of Rhode Island	AND	controls or processes the personal data of 35,000 or more unique consumers
		OR controls or processes the personal data of 10,000 or more unique consumers and derives more than 20% of its revenue from the sale of personal data

KEY DEFINITIONS	
Consumer	An individual residing in Rhode Island "acting in an individual or household context."
	Does not include an individual acting in a commercial or employment context.
Controller	"An individual who, alone or jointly with others, determines the purpose and means of the processing of personal data."
Processor	"An individual who, or legal entity that, processes personal data on behalf of the controller."
Third party	"An individual or legal entity, such as a public authority, agency, or body other than the consumer, controller, processor, or an affiliate of the processor or the controller."
Personal data	"Any information that is linked or reasonably linkable to an identified or identifiable natural person."
	"Does not include de-identified data or publicly available information."
Sale	"The exchange of personal data for monetary or other valuable consideration by the controller to a third party."
	Does not include the disclosure of personal data: → To a processor that processes the personal data on the controller's behalf. → To a third party for purposes of providing a product or service requested by the consumer. → To the controller's affiliate. → When the consumer directs the controller to disclose the personal data or intentionally uses the controller to interact with a third party. → That the consumer intentionally made available to the general public through a mass media channel and did not restrict to a specific audience. → To a third party as part of a merger or acquisition.
Child	The same meaning as provided in the Children's Online Privacy Protection Rule, which designates a child as someone under 13 years of age.

EXEMPTIONS	
Government	E
Nonprofits	E
Higher education	E
National securities associations	E
Employee/commercial B2B	D
GLBA	E/D
HIPAA	D
FERPA	D
FCRA	D
DPPA	D

E Entity-level exemption D Data-level exemption

CONSUMER RIGHTS		
Access		✓
Correct		✓
Delete		✓
Opt out of processing for ...	Targeted advertising/cross-contextual behavioral advertising	✓
	Sale of personal data	✓
	Profiling	✓
Portability		✓

✓ Applies to all personal data of a consumer held by a regulated entity

SENSITIVE INFORMATION	
Recognized categories of sensitive information:	✓
→ Racial or ethnic origin	
→ Religious beliefs	
→ Mental or physical health data e.g., conditions, diagnoses, treatments	
→ Sexual orientation/sexuality	
→ Sex life	
→ Citizenship or immigration status	
→ Children's data	
→ Precise geolocation	
→ Genetic or biometric data for purposes of uniquely identifying an individual	

Tennessee Information Protection Act

TENN. PUB. CH. NO 408 §§ 47-18-3201

Enacted: 19 March 2023
Effective: 1 July 2025

While Tennessee largely followed the well-worn path of its predecessors in setting out consumer rights and business obligations, it became an outlier in several respects. For one, it sets the highest raw applicability threshold for the control/processing of personal data at 175,000 or more unique consumers. Although, once adjusted for the state's population, this threshold falls squarely in the middle of the pack. Tennessee also introduced a unique enforcement provision, connecting compliance with its law to demonstrate adoption of the National Institute of Standards and Technology's Privacy Framework. Along with Utah, Tennessee is the only other state to set an independent revenue threshold: only entities making USD25 million or more in annual revenue may be covered.

APPLICABILITY THRESHOLDS		
Does business in the state of Tennessee	AND	controls or processes the personal data of 175,000 or more unique consumers
		OR controls or processes the personal data of 25,000 or more unique consumers and derives more than 50% of its revenue from the sale of personal data

KEY DEFINITIONS	
Consumer	A natural person who is a resident of Tennessee "acting only in a personal context."
	"Does not include a natural person acting in an employment or commercial context."
Controller	"The natural or legal person that, alone or jointly with others, determines the purpose and means of processing personal information."
Processor	"A natural or legal entity that processes personal information on behalf of a controller."
Third party	"A natural or legal person, public authority, agency, or body other than the consumer, controller, processor, or an affiliate of the processor or the controller."
Personal data	"Information that is linked or reasonably linkable to an identified or identifiable natural person."
	"Does not include publicly available information or de-identified or aggregate consumer information."
Sale	"The exchange of personal information for valuable monetary consideration by the controller to a third party."
	Does not include the disclosure of personal data:
	→ To a processor that processes the personal data on the controller's behalf.
	→ To a third party for purposes of providing a product or service requested by a consumer.
	→ To the controller's affiliate.
	→ That the consumer intentionally made available to the general public through a mass media channel and did not restrict to a specific audience.
	→ When the consumer directs the controller to disclose the personal data or intentionally uses the controller to interact with a third party
	→ To a third party as part of a merger or acquisition.
Child	"A natural person younger than 13 years of age."

EXEMPTIONS	
Government	E
Nonprofits	E
Higher education	E
National securities associations	⊗
Employee/commercial B2B	D
GLBA	E/D
HIPAA	E/D
FERPA	D
FCRA	D
DPPA	D

E Entity-level exemption D Data-level exemption ⊗ No exemption

CONSUMER RIGHTS	
Access	✓
Correct	✓
Delete	✓
Opt out of processing for ...	Targeted advertising/cross-contextual behavioral advertising
	Sale of personal data
	Profiling
Portability	☑

✓ Applies to all personal data of a consumer held by a regulated entity
☑ Applies to consumer-provided data only

SENSITIVE INFORMATION	
Recognized categories of sensitive information:	✓
→ Racial or ethnic origin	
→ Religious beliefs	
→ Mental or physical health data e.g., conditions, diagnoses, treatments	
→ Sexual orientation/sexuality	
→ Citizenship or immigration status	
→ Genetic or biometric data for purposes of uniquely identifying an individual	
→ Children's data	
→ Precise geolocation	

Enacted: 18 June 2023
Effective: 1 July 2024

Does business in the state of Texas	AND	controls or processes the personal data of any consumers
		OR engages in any sale of personal data

EXEMPTIONS	
Government	E
Nonprofits	E
Higher education	E
National securities associations	⊗
Employee/commercial B2B	D
GLBA	E/D
HIPAA	E/D
FERPA	D
FCRA	D
DPPA	D

Access	
Correct	
Delete	
Opt out of processing for ...	Targeted advertising/cross-contextual behavioral advertising 
	Sale of personal data 
	Profiling 
Portability	

 Applies to consumer-provided data only

- Racial or ethnic origin
- Religious beliefs
- Mental or physical health data e.g., conditions, diagnoses, treatments
- Sexual orientation/sexuality
- Citizenship or immigration status
- Genetic or biometric data for purposes of uniquely identifying an individual
- Children's data
- Precise geolocation

Utah Consumer Privacy Act

UTAH CODE § 13-61-101, ET SEQ.
AMENDED BY HB 418

Enacted: 24 March 2022
Effective: 31 Dec. 2023

The fourth state to pass a comprehensive privacy law, Utah draws heavily from two of its direct predecessors, the Virginia Consumer Data Protection Act and the Colorado Privacy Act. Having one of the highest raw applicability thresholds and lacking a couple of standard consumer rights, i.e., the rights to correct and to opt out of data processing for the purposes of profiling, Utah's law took one of the most business-friendly approaches to consumer privacy. Along with Tennessee, Utah is the only other state to set an independent revenue threshold: only entities making USD25 million or more in annual revenue may be covered.

APPLICABILITY THRESHOLDS		
Does business in the state of Utah	AND	controls or processes the personal data of 100,000 or more unique consumers
		OR controls or processes the personal data of 25,000 or more unique consumers and derives more than 50% of its revenue from the sale of personal data.

KEY DEFINITIONS	
Consumer	"An individual who is a resident of the state acting in an individual or household context."
	"Does not include an individual acting in an employment or commercial context."
Controller	"A person doing business in the state who determines the purposes for which and the means by which personal data are processed, regardless of whether the person makes the determination alone or with others."
Processor	"A person that processes personal data on behalf of a controller."
Third party	"A person other than the consumer, controller, or processor; or an affiliate or contractor of the controller or the processor."
Personal data	"Information that is linked or reasonably linkable to an identified individual or an identifiable individual."
	"Does not include deidentified data, aggregated data, or publicly available information."
Sale	"The exchange of personal data for monetary consideration by a controller to a third party."
	Does not include the disclosure of personal data: → To a processor who processes the personal data on behalf of the controller. → To a controller's affiliate. → To a third party if the purpose is consistent with a consumer's reasonable expectation, considering the context of the data collection. → When a consumer directs a controller to disclose the personal data or interact with one or more third parties. → To a third party for the purpose of providing a product or service requested by the consumer or a parent or legal guardian of a child.
Child	"An individual younger than 13 years old."

EXEMPTIONS	
Government	E
Nonprofits	E
Higher education	E
National securities associations	⊗
Employee/commercial B2B	D
GLBA	E/D
HIPAA	E/D
FERPA	D
FCRA	D
DPPA	D

E Entity-level exemption D Data-level exemption ⊗ No exemption

CONSUMER RIGHTS		
Access		✓
Correct		☑
Delete		☑
Opt out of processing for ...	Targeted advertising/cross-contextual behavioral advertising	✓
	Sale of personal data	✓
	Profiling	⊗
Portability		☑

✓ Applies to all personal data of a consumer held by a regulated entity
☑ Applies to consumer-provided data only ⊗ Does not apply

SENSITIVE INFORMATION	
Recognized categories of sensitive information:	✓
→ Racial or ethnic origin	
→ Religious beliefs	
→ Medical history, treatments or diagnoses	
→ Mental or physical health data e.g., conditions, diagnoses, treatments	
→ Sexual orientation/sexuality	
→ Citizenship or immigration status	
→ Genetic or biometric data for purposes of uniquely identifying an individual	
→ Precise geolocation	

Virginia Consumer Data Protection Act

VA. CODE § 59.1-575, ET SEQ.
AMENDED BY SB 854

Enacted: 2 March 2021
Effective: 1 Jan. 2023

The second state to enact comprehensive privacy legislation, Virginia helped lead privacy legislation away from the California model by enacting a bill based on the still unpassed Washington Privacy Act. With increasing variation, all comprehensive privacy laws passed since have closely followed this model. As an early law, it has already been amended, including in the 2024 session via HB 707, which increased protections for minors under the act.

APPLICABILITY THRESHOLDS		
Does business in the state of Virginia	AND	controls or processes the personal data of 100,000 or more unique consumers
		OR controls or processes the personal data of 25,000 or more unique consumers and derives more than 50% of its revenue from the sale of personal data.

KEY DEFINITIONS	
Consumer	A natural person who is a Virginia resident "acting only in an individual or household context."
	"Does not include a natural person acting in a commercial or employment context."
Controller	"The natural or legal person that, alone or jointly with others, determines the purpose and means of processing personal data."
Processor	"A natural or legal entity that processes personal data on behalf of a controller."
Third party	"A natural or legal person, public authority, agency, or body other than the consumer, controller, processor, or an affiliate of the processor or the controller."
Personal data	"Any information that is linked or reasonably linkable to an identified or identifiable individual."
	"Does not include de-identified data or publicly available information."
Sale	"The exchange of personal data for monetary consideration by the controller to a third party."
	Does not include the disclosure of personal data: → To a processor that processes personal data on behalf of the controller. → To a third party for purposes of providing a product or service requested by the consumer. → To a controller's affiliate. → That the consumer intentionally made available to the general public via a channel of mass media, and did not restrict to a specific audience. → To a third party as part of a merger, acquisition, bankruptcy or other transaction.
Child	"Any natural person younger than 13 years of age."

EXEMPTIONS	
Government	E
Nonprofits	E
Higher education	E
National securities associations	⊗
Employee/commercial B2B	D
GLBA	E/D
HIPAA	E/D
FERPA	D
FCRA	D
DPPA	D

E Entity-level exemption D Data-level exemption ⊗ No exemption

CONSUMER RIGHTS	
Access	✓
Correct	✓
Delete	✓
Opt out of processing for ...	Targeted advertising/cross-contextual behavioral advertising
	Sale of personal data
	Profiling
Portability	☑

✓ Applies to all personal data of a consumer held by a regulated entity
☑ Applies to consumer-provided data only

SENSITIVE INFORMATION	
Recognized categories of sensitive information:	✓
→ Racial or ethnic origin	
→ Religious beliefs	
→ Mental or physical health data e.g., conditions, diagnoses, treatments	
→ Sexual orientation/sexuality	
→ Citizenship or immigration status	
→ Genetic or biometric data for purposes of uniquely identifying an individual	
→ Children's data	
→ Precise geolocation	

Contacts

Connect with the team

Müge Fazlioglu, CIPP/E, CIPP/US
Principal Researcher,
Privacy Law and Policy, IAPP
muge@iapp.org

Former Westin Fellow, IAPP
Joe Jones
Director of Research
and Insights, IAPP
jjones@iapp.org

C. Kibby

For further inquiries, please reach out to research@iapp.org.

Follow the IAPP on social media



Published October 2025.

IAPP disclaims all warranties, expressed or implied, with respect to the contents of this document, including any warranties of accuracy, merchantability, or fitness for a particular purpose. Nothing herein should be construed as legal advice.

© 2025 IAPP. All rights reserved.