

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.

US State Comprehensive Privacy Laws Report

2024 LEGISLATIVE SESSION




Table of contents

What's inside?

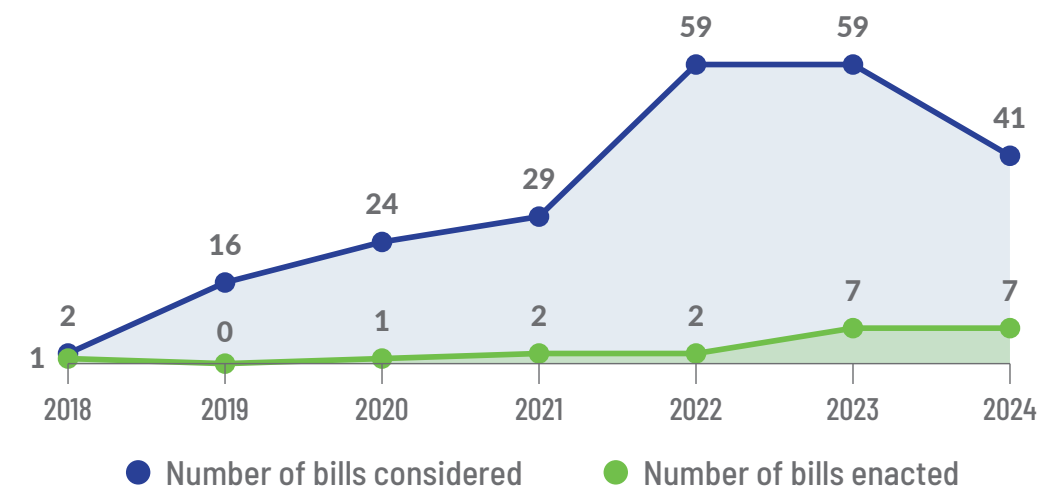
Overview	3
Scope.....	6
Exemptions.....	10
Consumer rights	13
Business obligations	16
Sensitive information	19
Rulemaking.....	23
Enforcement.....	24
Snapshots of Comprehensive US State Privacy Laws	26
Contacts	46

Overview

Keeping pace with US state privacy legislation

While 2024 may have matched the previous year with seven new comprehensive privacy laws enacted, its variety of legislative approaches has thrown the state legislative landscape into flux. Prior to this year, comprehensive privacy legislation was relatively uniform with marginal deviations in areas like jurisdictional thresholds and definitions of sensitive personal data. The qualitative differences between the new U.S. state privacy laws and their predecessors are even more apparent than the increase in the quantity of the laws. In response to continued technological innovation and maturing approaches to privacy, state lawmakers have taken U.S. state privacy lawmaking in new directions this year. All seven of the bills enacted so far in 2024 have introduced provisions meant to address privacy harms in unique ways that present new compliance challenges for privacy professionals to overcome.

The growth of US state privacy legislation



Minnesota, for example, introduced a new set of consumer rights to address potential harms caused by profiling. As is typical of other bills based on the unpassed Washington Privacy Act, it gives consumers the ability to opt out of processing personal data for certain profiling but goes further in affording the right to contest the result of profiling, including to be informed of actions that could have been taken to secure a different decision.

Or look to the Rhode Island Data Transparency and Privacy Protection Act, the most recent bill passed in 2024. Like Oregon and Minnesota's comprehensive privacy laws, it requires disclosing the list of specific third parties — as opposed to just the categories of third parties — to which a business has disclosed a consumer's personal data upon request. Rhode Island takes this a step further, requiring a business disclose the third parties to which it "may sell" personally identifiable information.

Other laws enacted in 2024 have their own twists, from Maryland's data minimization framework to New Jersey's requirement of a general notice when using certain tracking technologies. Vermont, via House Bill 121, came close to enabling a private right of action until it was thwarted by a gubernatorial veto. Indeed, part of Gov. Phill Scott's, R-Vt., justification for the veto was to avoid Vermont becoming "a national outlier."

In total, 19 enacted U.S. state privacy laws 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.

Enactment and effective dates of comprehensive US state privacy laws

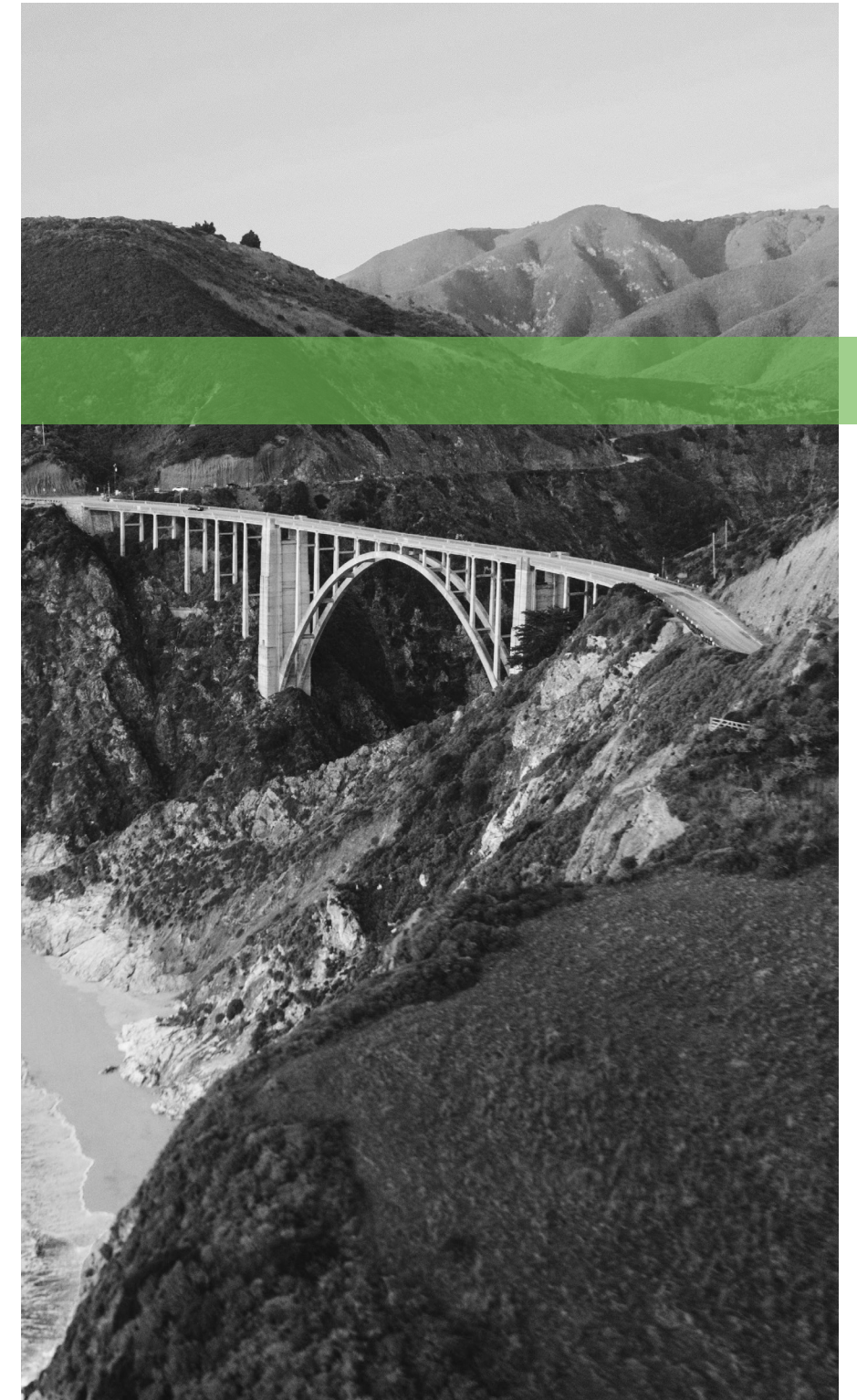
STATE PRIVACY LAW	DATE OF PASSAGE	DATE OF ENFORCEMENT
California Consumer Privacy Act	28 June 2018	1 Jan. 2020
California Privacy Rights Act	3 Nov. 2020	9 Feb. 2024
Virginia Consumer Data Protection Act	2 March 2021	1 Jan. 2023
Colorado Privacy Act	7 July 2021	1 July 2023
Connecticut Data Privacy Act	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 Senate Bill 332	16 Jan. 2024	15 Jan. 2025
New Hampshire Senate Bill 255	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 addition, longer standing bills have been amended this year, adding creases and technicolor to the patchwork. The Colorado Privacy Act now categorizes neural data as sensitive. The Virginia Consumer Data Protection Act added new protections for children. And California made numerous amendments to the California Consumer Privacy Act.

Meanwhile, the rapidly shifting landscape of state privacy adds to the pressure on federal legislators to pass a comprehensive privacy law. Though another such bipartisan effort was undertaken in 2024 via the American Privacy Rights Act — building upon the momentum generated by the American Data Privacy and Protection Act of 2023 — Congress has yet to reach a consensus that would both satisfy calls to preempt the patchwork of state laws and provide stronger protections for consumers in the form of a PRA.

By the same token, the ongoing debate at the federal level has influenced new legislation at the state level. Maryland and Minnesota's privacy laws, for example, both include provisions that are reflective of those in APRA. With the proliferation of state approaches, a federal law that would preempt them all will undoubtedly continue to meet resistance from maturing state privacy regulators, much like the APRA was formally opposed by the [California Privacy Protection Agency](#).

All told, there is much to support the argument that 2024 has been one of the most active years for comprehensive U.S. state privacy legislation tracking. Indeed, 2024 may become the year in which the most U.S. privacy laws are enacted. Regardless of the results of the 2024 legislative session, the topography of the 2025 privacy law landscape will likely feature equitable peaks, valleys and contours that privacy pros will need to traverse.



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 criterion, then it must usually 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 and the other based on its sale 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

Regarding the threshold for the processing of residents' personal data, there are five different levels found across all U.S. state privacy laws:

- Nebraska and Texas have no threshold.
- 35,000 or more unique consumers in Delaware, Maryland, New Hampshire and Rhode Island.
- 50,000 or more unique consumers in Montana.
- 100,000 or more unique consumers in California, Colorado, New Jersey, Connecticut, Minnesota, Oregon, Indiana, Iowa, Kentucky, 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. Most states fall somewhere between a raw threshold of 35,000 and 100,000 or more unique

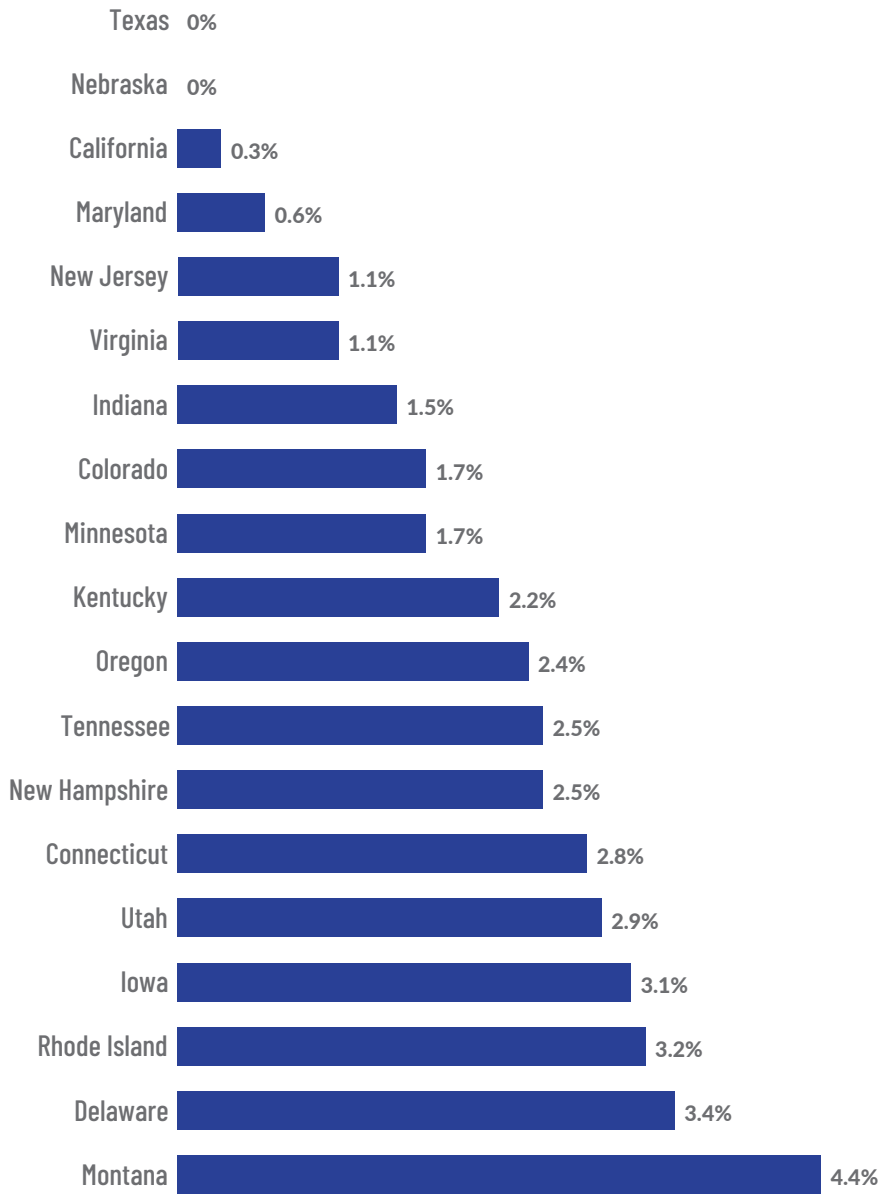
consumers. In terms of raw numbers, Tennessee is at the other end of the spectrum, putting the threshold of personal data processing at 175,000 or more unique customers. But, if adjusted by state population, Montana has the highest threshold by far.

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 following chart 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 the processing of personal data.

For example, while Maryland and Delaware both require an entity to process the data of 35,000 or more consumers, Maryland's threshold is much lower, as this equates to just about 0.6% of the population of Maryland compared to about 3.4% 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 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, with one component related to the volume of data processing/control, which is similar in nature to but typically lower than the previously listed thresholds, and the other component related to the percentage of revenue an entity obtains from the sale of personal data overall. Roughly in descending order of strictness, an entity must:

- Engage in any processing of personal data or any sale of personal data in Nebraska and Texas.
- 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 in Colorado and New Jersey.
- 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 Delaware, Maryland and Rhode Island.
- 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 in New Hampshire.
- 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 in Connecticut, Minnesota, Montana and Oregon.

- Derive 50% or more of its revenues from the sale of personal data in California.
- 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 in Indiana, Iowa, Kentucky, Tennessee, Utah and Virginia.

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. Colorado and New Jersey set some of the second lowest thresholds. In these two states, processing the personal data of 25,000 or more unique consumers and generating any revenue or discount on the price of any goods or services from the sale of personal data is sufficient to trigger applicability of its law. The largest group of states require entities 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 for this threshold to be met.

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	Delaware, Maryland and Rhode Island	New Hampshire	Montana	Colorado and New Jersey	Connecticut, Minnesota and Oregon	Indiana, Iowa, Kentucky, Utah and Virginia	California	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
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	≥ 35,000 consumers	≥ 50,000 consumers	≥ 100,000 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	> 10,000 consumers	≥ 10,000 consumers	≥ 25,000 consumers	≥ 25,000 consumers	> 25,000 consumers	≥ 25,000 consumers	Any consumers	≥ 25,000 consumers
	— AND — PERCENT OF GROSS REVENUE DERIVED FROM SELLING PERSONAL DATA IS ...	Any	> 20%	> 25%	> 25%	Any	> 25%	> 50%	> 50%	> 50%

Note: Within each U.S. state privacy law, a consumer is generally defined as a resident of that state.

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											<div><div>E</div>Entity-level exemption</div> <div><div>D</div>Data-level exemption</div> <div><div>⊗</div>No exemption</div> <div><div>*Please see the following section on exemption nuances.</div></div>
	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	E/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	⊗*	E*	⊗	D	D	D	D	D	D	
Montana	E	E	E	E	D	E/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	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	

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 only an exemption for state bodies in the form of a data-level exemption. All of the states except Colorado, Delaware, Minnesota and New Jersey 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 is for national securities associations, i.e., the Financial Industry Regulation Authority. Just under half of the states — Colorado, Connecticut, 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 a form of 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.

Exemption nuances

- * The Colorado Privacy Act, as amended by House Bill 24-1130 on the privacy of biometric identifiers and data, 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 criminal or fraudulent acts relating to insurance or first responders responding to catastrophic events are exempt.
- * In Minnesota, nonprofits that detect insurance fraud are exempt.
- * In Minnesota, postsecondary institutions regulated by the Office of Higher Education are not required to comply until 31 July 2029.
- * The Colorado Privacy Act, as amended by HB 24-1130, applies to employers' collection and use of biometric data of employees and independent contractors.
- * Oregon's law only exempts nonprofits that try to prevent insurance fraud and journalistic nonprofits.



Consumer rights

What types of data requests can consumers make?

Each U.S. comprehensive state privacy law establishes various consumer rights, from the rights to access, correct and delete their data held by companies to the right to opt out of processing 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, and most provide all three. The sole deviations are in Indiana, where the right to correct data applies only to consumer-provided data, and in Utah, which provides no right to correction and wherein the right to delete applies only to consumer-provided data. 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

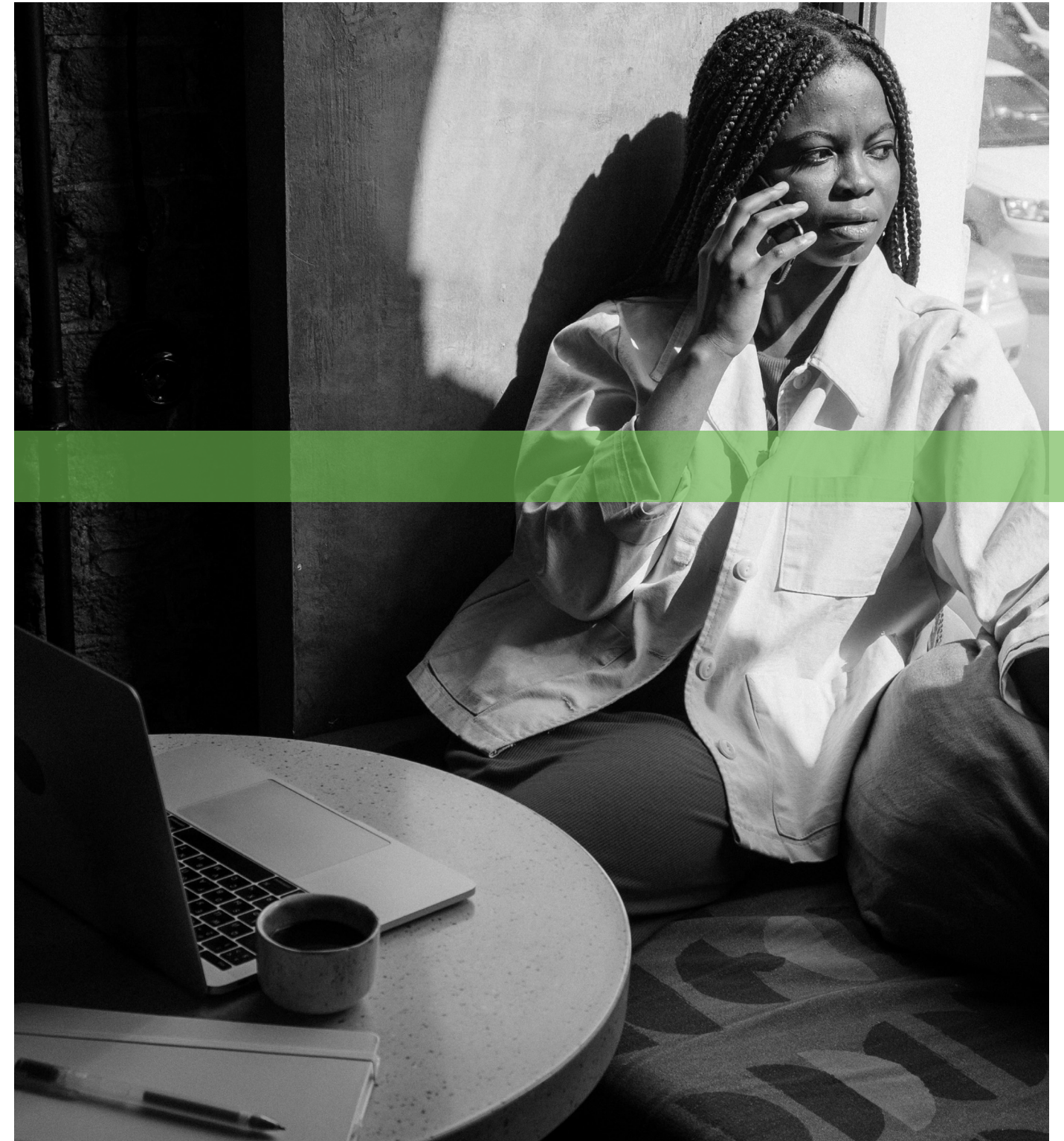
The state laws are also mostly consistent in terms of providing the right to opt out of processing for targeted or cross-contextual behavioral advertising, sale of personal data and profiling. In terms of deviations, Iowa's privacy law lacks the right to opt out of processing for targeted advertising and profiling, although it does establish the right to opt out of the sale of personal data. In addition, Utah provides no 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, the right to portability applies to any personal data of an individual held by a regulated entity. Yet, in a minority — Delaware, Indiana, Iowa, Montana, Tennessee, Texas, Utah and Virginia — the right to portability applies only to consumer-provided data.

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...		Profiling	Portability	Limit the use and disclosure of sensitive personal information
				Targeted advertising/cross-contextual behavioral advertising	Sale of personal data			
California	✓	✓	✓	✓	✓	✓	✓	✓
Colorado	✓	✓	✓	✓	✓	✓	✓	✗
Connecticut	✓	✓	✓	✓	✓	✓	✓	✗
Delaware	✓	✓	✓	✓	✓	✓	✓	✗
Indiana	✓	✓	✓	✓	✓	✓	✓	✗
Iowa	✓	✗	✓	✗	✓	✗	✓	✗
Kentucky	✓	✓	✓	✓	✓	✓	✓	✗
Maryland	✓	✓	✓	✓	✓	✓	✓	✗
Minnesota	✓	✓	✓	✓	✓	✓	✓	✗
Montana	✓	✓	✓	✓	✓	✓	✓	✗
Nebraska	✓	✓	✓	✓	✓	✓	✓	✗
New Hampshire	✓	✓	✓	✓	✓	✓	✓	✗
New Jersey	✓	✓	✓	✓	✓	✓	✓	✗
Oregon	✓	✓	✓	✓	✓	✓	✓	✗
Rhode Island	✓	✓	✓	✓	✓	✓	✓	✗
Tennessee	✓	✓	✓	✓	✓	✓	✓	✗
Texas	✓	✓	✓	✓	✓	✓	✓	✗
Utah	✓	✗	✓	✓	✓	✗	✓	✗
Virginia	✓	✓	✓	✓	✓	✓	✓	✗

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

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



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 personal data to be used for 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.





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 stringent 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.

Data protection assessments

Data protection assessments are required by most U.S. state privacy laws for any processing activities that involve a "heighted 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 currently required in California and Colorado, albeit limited in Colorado to the attorney general's [Universal Opt-Out Shortlist](#). Beginning in January 2025, recognition of universal opt-out mechanisms will also be required in Delaware, Montana, Nebraska and Texas. By July 2025, it will be 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 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, and 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:

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

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 in California.

- Status as transgender or nonbinary in Delaware, Maryland, New Jersey and Oregon.
- Genetic or biometric data in Delaware, Maryland, New Hampshire and Oregon, though other state laws may apply.
- Consumer health data in California, Connecticut and Maryland, though other state laws may apply.
- Status as victim of a crime in Oregon and Connecticut.
- Finance-related information in California and New Jersey.
- Biological or neural data in California and Colorado.

In addition to those listed above, California uniquely recognizes a few additional categories of information as sensitive, including Social Security numbers, driver's licenses, state identification cards or passport numbers; union membership; and contents of a consumer's mail, email and text messages unless the business is the intended recipient of the communication.



Recognized categories of sensitive information across U.S. 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	Medical history, treatments or diagnoses	Sexual orientation/ sexuality	Sex life	Status as transgender or nonbinary	Personal data of known child	
California	✓	✗	✓	✓	✓	✓	✓	✗	✓	✓	✗	✗	✓ Recognized as a category of sensitive information
Colorado	✓	✗	✓	✓	✗	✗	✓	✗	✓	✓	✗	✓	
Connecticut	✓	✗	✓	✓	✗	✓	✓	✗	✓	✓	✗	✓	✗ Not recognized as a category of sensitive information
Delaware	✓	✗	✓	✓	✗	✗	✓	✗	✓	✓	✓	✓	
Indiana	✓	✗	✓	✓	✗	✗	✓	✗	✓	✗	✗	✓	
Iowa	✓	✗	✓	✓	✗	✗	✓	✗	✓	✗	✗	✓	
Kentucky	✓	✗	✓	✓	✗	✗	✓	✗	✓	✗	✗	✓	
Maryland	✓	✓	✓	✓	✗	✓	✗	✗	✓	✓	✓	✓	
Minnesota	✓	✗	✓	✓	✗	✗	✓	✗	✓	✗	✗	✓	
Montana	✓	✗	✓	✓	✗	✗	✓	✗	✓	✓	✗	✓	
Nebraska	✓	✗	✓	✓	✗	✗	✓	✗	✓	✗	✗	✓	
New Hampshire	✓	✗	✓	✓	✗	✗	✓	✗	✓	✓	✗	✓	
New Jersey	✓	✗	✓	✓	✗	✗	✓	✗	✓	✓	✓	✓	
Oregon	✓	✓	✓	✓	✗	✗	✓	✗	✓	✗	✓	✓	
Rhode Island	✓	✗	✓	✓	✗	✗	✓	✗	✓	✓	✗	✓	
Tennessee	✓	✗	✓	✓	✗	✗	✓	✗	✓	✗	✗	✓	
Texas	✓	✗	✓	✓	✗	✗	✓	✗	✓	✗	✗	✓	
Utah	✓	✗	✓	✓	✗	✗	✓	✓	✓	✗	✗	✗	
Virginia	✓	✗	✓	✓	✗	✗	✓	✗	✓	✗	✗	✓	

Recognized categories of sensitive information across U.S. state privacy laws, *continued*

	Genetic or biometric data for purposes of uniquely identifying an individual	Genetic or biometric data	Biological data, including 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

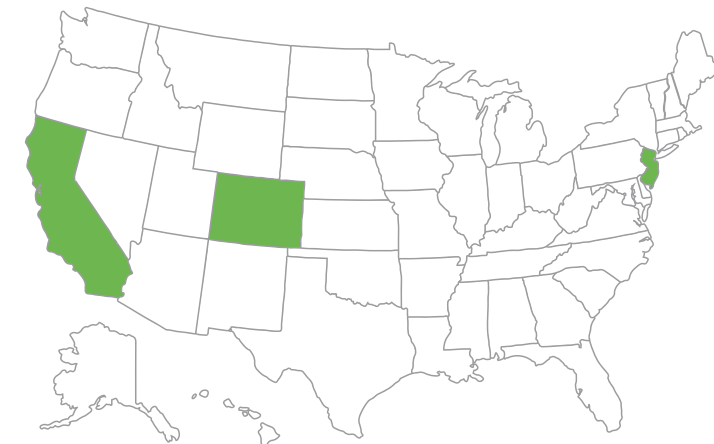
Three states — Colorado, California and New Jersey — give rulemaking authority to a state agency.

In Colorado, the attorney general's office released the finalized Colorado Privacy Act Rules 1 July 2023 to implement the Colorado Privacy Act.

Only California has a dedicated enforcement agency, the CPPA, for the promulgation of rulemaking. The enforcement date of the new CCPA Regulations was pushed to March 2024, and other required rulemakings remain in progress.

New Jersey's law, effective 15 Jan. 2025, grants rulemaking authority to its director of the Division of Consumer Affairs in the Department of Law and Public Safety and does not require promulgation by any stated deadline.

States with rulemaking authority



Enforcement

How are US privacy laws being enforced?

Privacy-related enforcement and compliance activities have also picked up in 2024 across the states. Indeed, this year has seen the largest privacy-related fine in any state to date with the Texas attorney general's [settlement](#) with Meta for USD1.4 billion due to allegations of unauthorized capture of biometric data. The prior record was set by the USD390 million settlement obtained by 40 state attorneys general against Google in 2022. Although this lawsuit was brought under Texas's Capture or Use of Biometric Identifier Act and predated the newly effective Texas Data Privacy and Security Act, it shows the breadth of enforcement tools that state regulators now have at their disposal — and are willing to use — to enforce consumer privacy rights.

Largest privacy-related fines brought forward by states, 2022 to 2024



This year has also been notable for bringing about the second and third public CCPA enforcement settlements. In June, a joint investigation between the California attorney general and the Los Angeles City Attorney's Office led to a USD500,000 [settlement](#) with a mobile game developer that allegedly collected and shared children's data without parental consent. And, in February, a food delivery platform agreed to pay USD375,000 due to [allegations](#) that it sold the personal information of its consumers without providing notice or the opportunity to opt out.

As they have stepped 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. After announcing the enforcement of the Colorado Privacy Act by mailing a [series of letters](#) to businesses educating them on their various legal obligations last year, the Colorado attorney general provided targeted [guidance](#) on the Global Privacy Control this year. Moreover, in April 2024, the CPPA issued its first [enforcement advisory](#), which focused on applying data minimization to consumer requests. This 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.

Perhaps the most important enforcement trend in 2024 is that state attorneys general are bringing privacy lawsuits against companies based not only on alleged violations of state and federal privacy laws, but on alleged violations of state laws around consumer protection, unfair competition, false advertising, data breaches and medical confidentiality. Thus, U.S. state privacy laws have added one more tool to the enforcement toolbox of state attorneys general in seeking to protect consumers from harmful or deceptive business practices.

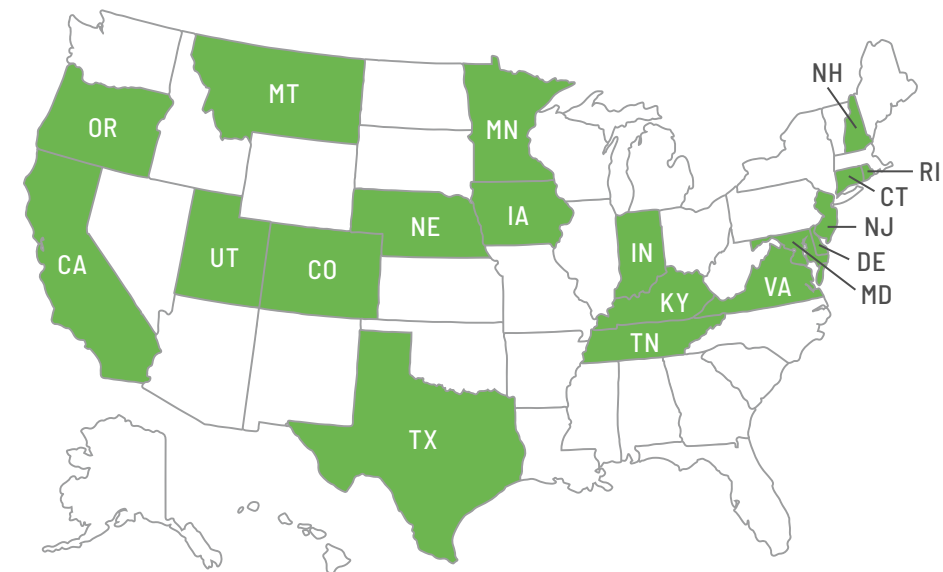


Snapshots of Comprehensive US State Privacy Laws

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. Against the WPA-inspired crowd, California remains an outlier in several important respects, such as being the only state to require notice at collection, which gives consumers the right to limit the use and disclosure of sensitive personal information. As these state-level snapshots reveal, with the passage of each new comprehensive state privacy law, the definitions, scopes and enforceability of the laws on the books undergo iterative changes.

Comprehensive US State Privacy Laws



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

CCPA, as amended
by the CPRA

CAL. CIV. CODE § 1798.100, ET SEQ

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 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 data, including neural data	

Colorado Privacy Act

COLO. REV. STAT. § 6-1-1301, ET SEQ.

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. Accounting for this flurry of activity, as well as the Colorado AI Act passed earlier this year, it will be vital to watch out for a "Denver effect" in other jurisdictions.

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.

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	
→ Personal data of known child	
→ Biological data, including neural data	

Connecticut Data Privacy Act

CONN. GEN STAT. § 42-515, ET SEQ.

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. With its scope being slightly broader than Virginia but narrower than Colorado, the Connecticut's law is notable for containing the full suite of exemptions as well as consumer rights. It also helped to reinforce the expanded boundaries for the definition of sale of data – as seen in California and Colorado – beyond pure monetary considerations to also encapsulate an exchange for "other valuable consideration."

APPLICABILITY THRESHOLDS		
Does business in the state of Connecticut	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	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	E/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	
→ Personal data of known child	
→ Precise geolocation	
→ Status as victim of crime	
→ Consumer health data	

Delaware Personal Data Privacy Act

DEL. CODE TIT. 6 § 12D-101

Enacted: 11 Sept. 2023

Effective: 1 Jan. 2025

The Delaware Personal Data Privacy does not deviate significantly from prior U.S. privacy laws. It does stand out, however, in joining only a few other states that do not provide entity-level exemptions to most nonprofit organizations and institutions of higher education.

APPLICABILITY THRESHOLDS		
Does business in the state of Delaware	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 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 included-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.

EXEMPTIONS	
Government	E
Nonprofits	⊗*
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 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."

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	
→ Personal data of known child	
→ 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

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 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 included-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.

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	
→ Personal data of known child	
→ 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.

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 Iowa 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	
→ Personal data of known child	
→ Precise geolocation	

Kentucky Consumer Data Protection Act

HB 15

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.

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	
→ Personal data of known child	
→ Precise geolocation	

Maryland Online
Data Privacy Act

SB 541

Enacted: 9 May 2024
Effective: 1 Oct. 2025

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. All told, Maryland's law may create new operational challenges for privacy pros to solve in the lead up to its effective date 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:	✓
→ 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	
→ Personal data of known child	
→ Precise geolocation	

Minnesota Consumer Data Privacy Act

HF 4757

Enacted: 24 May 2024
Effective: 31 July 2025

As the second bill 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	
→ Personal data of known child	
→ Precise geolocation	

Montana Consumer Data Privacy Act

MONT. CODE §§ 30-14-2801, ET SEQ.

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. While it does not stray far from any of the previously introduced pieces of U.S. state privacy legislation, it is notable for including recognitions of universal opt-out mechanisms and for setting applicability thresholds that, adjusted for its small population, make it the lowest applicability of any state privacy law.

APPLICABILITY THRESHOLDS		
Does business in the state of Montana	AND	controls or processes the personal data of 50,000 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	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	E
Higher education	E
National securities associations	E
Employee/commercial B2B	D
GLBA	E/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	
→ Personal data of known child	
→ 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

HF 4757

Enacted: 24 May 2024
Effective: 31 July 2025








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	
→ Personal data of known child	
→ Precise geolocation	

New Hampshire
SB 255

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 are longer coming into effect. When SB 255-FN was originally signed on March 6, 2024, it included provisions for the New Hampshire Secretary of State to establish how consumers may exercise their rights and privacy notice standards. HB 1220-FN, a subsequent bill signed on July 19, 2024, modified those provisions so as to eliminate the RSA 507-H rulemaking provisions, leaving just three states (CA, CO, and NJ) 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 a person 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	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	
→ Personal data of known child	

New Jersey
SB 332

SB 332

Enacted: 16 Jan. 2024
Effective: 15 Jan. 2025

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.

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	
→ Personal data of known child	
→ Precise geolocation	
→ Finance-related information	

Oregon Consumer Privacy Act

OREGON SB 619

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		controls or processes the personal data of 100,000 or more unique consumers
	AND	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	"The exchange of personal data for monetary or other valuable consideration by the controller with a third party."
	<p>Does not include the disclosure of personal data:</p> <ul style="list-style-type: none"> → 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:	
<ul style="list-style-type: none"> → 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 → Personal data of known child → 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 WPA model in building on the existing requirement that entities must disclose to consumers the specific third parties to who they sell 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

APPLICABILITY THRESHOLDS		
Does business in the state of Rhode Island		controls or processes the personal data of 35,000 or more unique consumers
	AND	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








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."
	<p>Does not include the disclosure of personal data:</p> <ul style="list-style-type: none"> → 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

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

CONSUMER RIGHTS

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
- Personal data of known child
- Consumer health data
- Precise geolocation

Tennessee Information Protection Act

TENN. PUB. CH. NO 408 §§ 47-18-3201

Enacted: 19 March 2023

Effective: 1 Jan. 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 demonstrated 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 an individual or household context.
	"Does not include a natural person acting in an employment or commercial context."
Controller	"A 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.
Child	→ 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	
→ Personal data of known child	
→ Precise geolocation	

Texas Data Privacy and Security Act

TEX. BUS. & COM. CODE §§ 541.001, ET SEQ.

Enacted: 19 March 2023
Effective: 1 Jan. 2025

When Texas became the 10th state to join the privacy law ranks, it showed some of the first signs of deviation from the long-standing Virginia model. The biggest departure marked by the Texas law was in its applicability thresholds. It was the first state — soon followed by Nebraska — to set the bar for applicability at the bare minimum of processing or engaging in the sale of any personal data. Although Texas is also one of the few states to include an exemption for small businesses, i.e., those with fewer than 500 employees, its redefinition of scope away from volume of processing or percentage of revenue generated by the sale of personal data was notable.

APPLICABILITY THRESHOLDS		
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.

KEY DEFINITIONS	
Consumer	An individual who is a resident of Texas "acting only in an individual or household context."
	"Does not include an individual acting in an employment or commercial context."
Controller	"A person that, alone or jointly with others, 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, other than the consumer, the controller, the processor, or an affiliate of the controller or processor."
Personal data	"Any information, including sensitive data, that is linked or reasonably linkable to an identified or identifiable individual."
	"Does not include deidentified 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.
	<p>Does not include the disclosure of personal data:</p> <ul style="list-style-type: none"> → 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. → To a third party as part of a merger or acquisition.
Child	"An individual 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	<input checked="" type="checkbox"/>
Correct	<input checked="" type="checkbox"/>
Delete	<input checked="" type="checkbox"/>
Opt out of processing for ...	Targeted advertising/cross-contextual behavioral advertising
	Sale of personal data
	Profiling
Portability	<input type="checkbox"/>

 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
- Sex life
- Citizenship or immigration status
- Genetic or biometric data for purposes of uniquely identifying an individual
- Personal data of known child
- Precise geolocation

Utah Consumer Privacy Act

UTAH CODE § 13-61-101, ET SEQ.

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 by the 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	
→ Mental or physical health data e.g., conditions, diagnoses, treatments	
→ Medical history, treatments or diagnoses	
→ 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.

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 WPA. 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 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	
→ Personal data of known child	
→ Precise geolocation	

Contacts

Connect with the team

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

C. Kibby
Westin Fellow, IAPP
ckibby@iapp.org

**Andrew Folks, CIPP/E,
CIPP/US, CIPM**
Former Westin Fellow, IAPP

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

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

Follow the IAPP on social media



Published October 2024.

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.

© 2024 IAPP. All rights reserved.