U.S. State Comprehensive Consumer Data Privacy Law Comparison

Prepared by Foley's Cybersecurity & Data Privacy Team

FOLEY

FOLEY & LARDNER LLP

FOLEY & LARDNER LLP

U.S. State Comprehensive Consumer Data Privacy Law Comparison

Since the passage of the California Consumer Privacy Act (CCPA) in 2018, other U.S. states have followed suit by enacting comprehensive consumer data privacy laws in rapid succession. While these state consumer privacy laws tend to have similar themes and address comparable topics, there are also important differences among them — meaning a one-size-fits-all data privacy program will not suffice. Given that the federal government has yet to pass a comprehensive consumer data privacy law, organizations must ensure they comply with the law of each applicable state and monitor this rapidly evolving regulatory environment.

For a summary comparison of enacted state consumer data privacy laws, download Foley's U.S. State Comprehensive Consumer Data Privacy Law Comparison chart. This chart addresses state comprehensive data privacy laws enacted as of October 1, 2025, and should be used for informational purposes only because this chart does not cover every aspect of each law.

Without limitation, this chart does not cover:

- State data privacy laws specific to only a particular type of data, such as the Washington My Health My Data Act
- All entity-level or data-level exemptions
- Contents of the privacy notice
- Procedures for responding to consumer rights requests
- Specific obligations when engaging service providers or other third parties
- Compliance obligations for service providers or other third parties
- Universal opt-out requirements
- Financial incentives
- Discrimination prohibitions

For more information about U.S. state comprehensive consumer data privacy laws or other data privacy matters, please contact a senior member of Foley's Technology Transactions, Cybersecurity, and Privacy Practice.

Current as of October 1, 2025

This chart is updated quarterly. To ensure you always refer to the most up-to-date version, please access the chart via Foley's website: www.foley.com/state-consumer-data-privacy-laws.

CHART KEY:

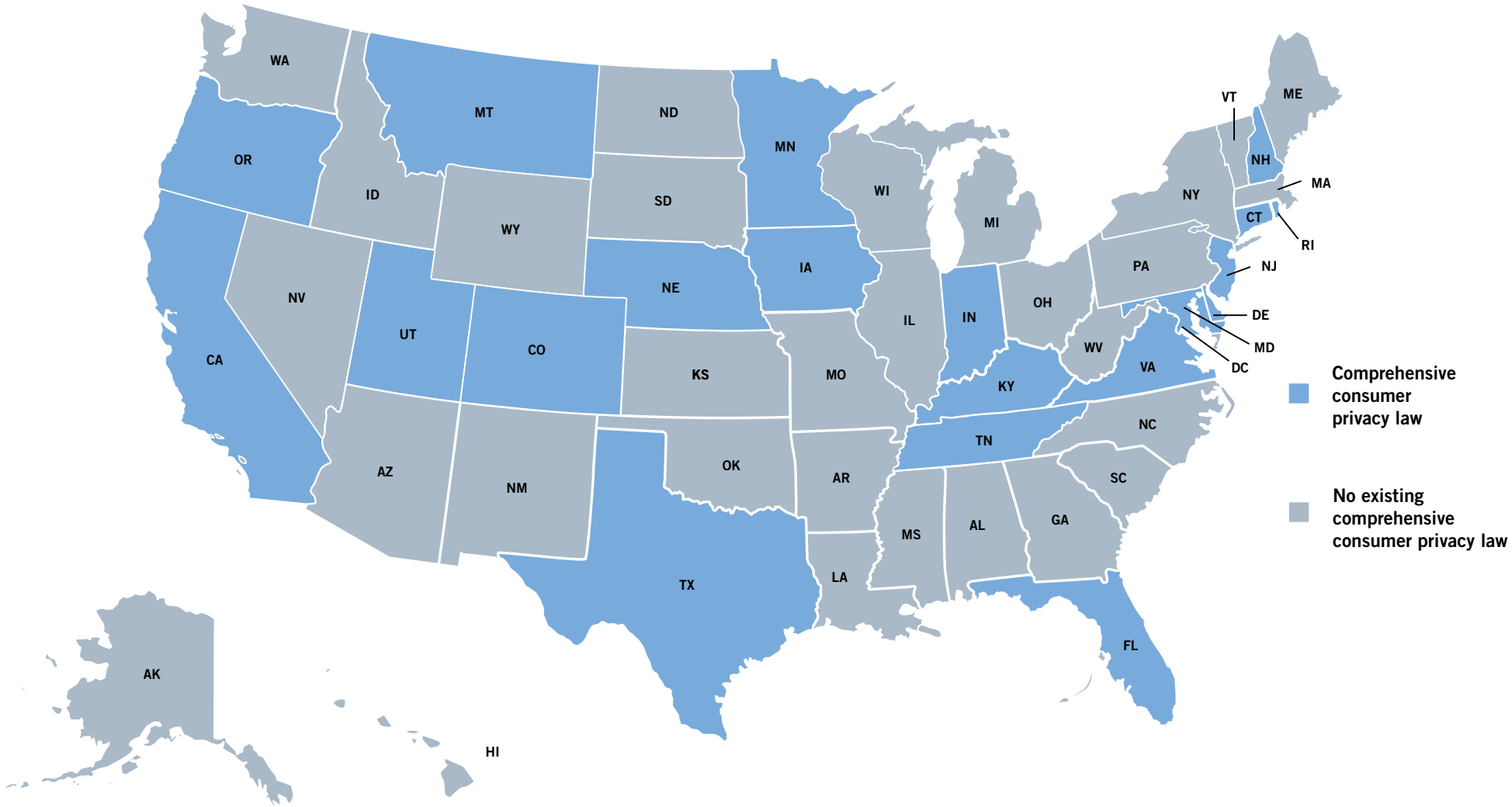
L	–	Limited
S	–	Obtain opt-in consent for processing for sale or sharing of personal data
SD	–	Sensitive data
D	–	Mental or physical health diagnosis
CD	–	Mental or physical health condition or diagnosis
MCTD	–	Mental or physical health medical history, condition, treatment, or diagnosis
EL	–	Entity-level exemption for covered entities and business associates as defined by HIPAA
DL	–	Data-level exemption for health care information collected by a covered entity or business associate to the extent they are treating data as protected health information as defined by HIPAA

FOLEY

FOLEY & LARDNER LLP

U.S. States With a Comprehensive Consumer Privacy Law

Enacted As of October 1, 2025



				Scope		Protected Data
State	**Statute**	**Regulations?**	**Effective Date**	**Protected Individuals**	**Regulated Entities**	**Definition of Personal Data/Information**
California	California Consumer Privacy Act (CPRA), *Calif. Civ. Code § 1798.100*	Yes (additional regulations are forthcoming)	January 1, 2023	California *resident*	For-profit entities that (1) do business in California and (2) meet any one of the following: ■ Had annual gross revenue in excess of **US$26.625m in the preceding calendar year;** *or* ■ Annually buy, sell, or share "personal information" of ≥ **100,000** California residents or households; or ■ Derive **50% or more of annual revenue from selling or sharing** California residents' "personal information."	"Personal information": Information that identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household.
Colorado	Colorado Privacy Act (CPA), *Colo. Rev. Stat. 6-1-1301*	Yes	■ July 1, 2023 (general data privacy act provisions) ■ July 1, 2025 (amendments related to biometric data and biometric identifiers) ■ October 1, 2025 (amendments related to data protection for a minor's online activity)	Colorado *resident*	Entities that (1) do business in Colorado *or* produce or deliver commercial products or services intentionally targeted to Colorado residents, *and* (2) **control or process** the "personal data" of: ■ ≥ **100,000** Colorado residents during a calendar year; *or* ■ ≥ **25,000** Colorado residents *and* derive **revenue or receives a discount on the price of goods or services from the sale** of "personal data."[1]	"Personal data": Information that is linked or reasonably linkable to an identified or identifiable individual.

1 CPA's biometric identifier and minors' data requirements apply more broadly.

				Scope		Protected Data
State	**Statute**	**Regulations?**	**Effective Date**	**Protected Individuals**	**Regulated Entities**	**Definition of Personal Data/Information**
Connecticut	Connecticut Data Privacy Act (CTDPA), *Conn. Gen. Stat. Ann. 42-515*	No (none expected)	■ July 1, 2023 (general data privacy act provisions and provisions related to consumer health data) ■ July 1, 2024 (provisions related to social media entity's obligations with minors' data) ■ October 1, 2024 (provisions related to children's data and online dating platforms)	Connecticut *resident*	For-profit entities that (1) do business in Connecticut *or* produce products or services targeted to Connecticut residents, *and* (2) during the prior calendar year **control or process** the "personal data" of: ■ ≥ **100,000** Connecticut residents, excluding "personal data" controlled or processed solely to complete a payment transaction; *or* ■ ≥ **25,000** Connecticut residents *and* derive **over 25% of their gross revenue from the sale** of "personal data." Effective July 1, 2026: For-profit entities that (1) do business in Connecticut *or* produce products or services targeted to Connecticut residents, *and* (2) during the prior calendar year: ■ Control or process the "personal data" of ≥ **35,000** Connecticut residents, excluding personal data controlled or processed solely to complete a payment transaction; ■ Control or process **sensitive data** concerning Connecticut residents, unless such data is processed solely for the purposes of completing a payment transaction; *or* ■ Offer consumers' personal data **for sale** in trade or commerce.	"Personal data": Any information that is linked or reasonably linkable to an identified or identifiable individual.
Delaware	Delaware Personal Data Privacy Act (DPDPA), *6 Del. C. §§ 12D-101*	No (none expected)	January 1, 2025	Delaware *resident*	Entities that (1) do business in Delaware *or* produce products or services targeted to Delaware residents, *and* (2) during the prior calendar year **control or process** the "personal data" of: ■ ≥ **35,000** Delaware residents, excluding "personal data" controlled or processed solely to complete a payment transaction; *or* ■ ≥ **10,000** consumers *and* derive **more than 20% of their gross revenue from the sale** of "personal data."	"Personal data": Any information that is linked or reasonably linkable to an identified or identifiable individual.

				Scope		Protected Data
State	**Statute**	**Regulations?**	**Effective Date**	**Protected Individuals**	**Regulated Entities**	**Definition of Personal Data/Information**
Florida	Florida Digital Bill of Rights (FDBR), *Fla. Stat. § 501.701*	Yes	July 1, 2024 (Florida Digital Bill of Rights)	Florida *resident*	For-profit entities that (1) do business in Florida, (2) collect "personal data" about Florida residents, (3) have over US$1bn in global annual revenue, *and* (4) meet any one of the following: ■ Derive 50% of global gross annual revenue from the sale of advertisements online; *or* ■ Operate a consumer smart speaker and voice command service with an integrated virtual assistant connected to a cloud computing service that uses hands-free verbal activation; *or* ■ Operate an app store or digital distribution platform with at least 250,000 different software applications for consumers to download and install.	"Personal data": Any information, including sensitive data, that is linked or reasonably linkable to an identified or identifiable individual.
Indiana	Indiana Consumer Data Protection Act (Ind. CDPA), *Ind. Code 24-15*	No (none expected)	January 1, 2026	Indiana *resident*	Entities that (1) conduct business in Indiana *or* (2) produce products or services targeted at Indiana residents that: ■ Control or process "personal data" of at least **100,000** Indiana consumers; *or* ■ Control or process "personal data" of at least **25,000** Indiana consumers *and* derive **more than 50% of gross revenue from the sale** of "personal data."	"Personal data": Any information that is linked or reasonably linkable to an identifiable individual.
Iowa	Iowa Consumer Data Protection Act (Iowa CDPA), *Iowa Code Ann. 715D*	No (none expected)	January 1, 2025	Iowa *resident*	For-profit entities that (1) conduct business in Iowa *or* (2) produce products or services targeted to Iowa residents that: ■ Control or process "personal data" of at least **100,000** consumers; *or* ■ Control or process "personal data" of at least **25,000** consumers *and* derive over **50% of gross revenue from the sale** of "personal data."	"Personal data": Any information that is linked or reasonably linkable to an identified or identifiable natural person.
Kentucky	Kentucky Consumer Data Protection Act (KCDPA), *Ky. Rev. Stat. § 367.3611*	No (none expected)	January 1, 2026	Kentucky *resident*	Persons that (1) conduct business in Kentucky or produce products or services that are targeted to residents of Kentucky, *and* (2) during a calendar year control or process personal data of: ■ ≥ **100,000** consumers; or ■ ≥ **25,000** consumers and derive **over 50% of gross revenue from the sale** of "personal data."	"Personal data": Any information that is linked or reasonably linkable to an identified or identifiable natural person.

				Scope		Protected Data
State	**Statute**	**Regulations?**	**Effective Date**	**Protected Individuals**	**Regulated Entities**	**Definition of Personal Data/Information**
Maryland	Maryland Online Data Privacy Act (MODPA), *Md. Code, Com. Law § 14-4701*	No (none expected)	October 1, 2025	Maryland *resident*	A person that (1) conducts business in Maryland or provides products or services that are targeted to residents of Maryland, *and* (2) during the preceding calendar year controlled or processed the "personal data" of: ■ ≥ **35,000** consumers, excluding personal data controlled or processed for the purpose of completing a payment transaction; or ■ ≥ **10,000** consumers and derived **more than 20% of gross revenue from the sale** of "personal data."	"Personal data": Any information that is linked or can be reasonably linked to an identified or identifiable consumer.
Minnesota	Minnesota Consumer Data Privacy Act (MNCDPA), *Minn. Stat. § 325M*	No (none expected)	July 31, 2025 (general data privacy act provisions) July 31, 2029 (provisions related to postsecondary institutions regulated by the Office of Higher Education)	Minnesota *resident*	Legal entities that (1) conduct business in Minnesota or produce products or services that are targeted to residents of Minnesota, *and* (2) satisfy one or more of the following: ■ During a calendar year, control or process personal data of **100,000** or more consumers, excluding personal data controlled or processed for the purpose of completing a payment transaction; or ■ Derive over **25% of gross revenue from the sale** of "personal data" and process or control personal data of **25,000** consumers or more.	"Personal data": Any information that is linked or reasonably linkable to an identified or identifiable natural person.
Montana	Montana Consumer Data Privacy Act (Mont. CDPA), *Mont. Code Ann. § 30-14-2801*	No (none expected)	October 1, 2024	Montana *resident*	Persons that (1) conduct business in Montana *or* produce products or services targeted to Montana residents, *and* (2) **control or process** the "personal data" of: ■ ≥ **25,000** Montana residents, excluding "personal data" controlled or processed only for the purpose of completing a payment transaction; *or* ■ ≥ **15,000** Montana residents *and* derive **over 25% of gross revenue from the sale** of "personal data." For sections related to minors: Persons that conduct business in Montana or deliver commercial products or services that are **intentionally targeted** to minors under the age of 18 in Montana.	"Personal data": Any information that is linked or reasonably linkable to an identified or identifiable individual.

				Scope		Protected Data
State	**Statute**	**Regulations?**	**Effective Date**	**Protected Individuals**	**Regulated Entities**	**Definition of Personal Data/Information**
Nebraska	Nebraska Data Privacy Act (NDPA), *Neb. Rev. Stat. § 87-1101*	No (none expected)	January 1, 2025	Nebraska *resident*	A person that: ■ Conducts business in Nebraska *or* produces a product or service consumed by residents of Nebraska; ■ Processes or engages in the sale of personal data; and ■ Is not a small business as determined under the federal Small Business Act.[2]	"Personal data": Information, including sensitive data, that is linked or reasonably linkable to an identified or identifiable individual and includes pseudonymous data when the data is used by a controller or processor in conjunction with additional information that reasonably links the data to an identified or identifiable individual.
New Hampshire	New Hampshire Privacy Act (NHPA), *N.H. Rev. Stat. Ann. § 507-H*	No (the secretary of state has the authority to establish privacy notice standards)	January 1, 2025	New Hampshire *resident*	Entities that (1) conduct business in New Hampshire or produce products or services that are targeted to New Hampshire residents, *and* (2) during a one-year period **control or process** the "personal data" of: ■ ≥ **35,000** unique consumers, excluding personal data controlled or processed solely for the purpose of payment transactions; or ■ ≥ **10,000** unique consumers and derive **more than 25% of gross revenue from the sale** of "personal data."	"Personal data": Any information that is linked or reasonably linkable to an identified or identifiable individual.
New Jersey	New Jersey Data Privacy Act (NJDPA), *N.J. Rev. Stat. § 56:8-166.4*	No (the Division of Consumer Affairs has the authority to promulgate rules and regulations; the Division states that regulations are forthcoming in 2025)	January 15, 2025	New Jersey *resident*	Entities that (1) conduct business in New Jersey *or* produce products or services that are targeted to New Jersey residents, *and* (2) during the calendar year **control or process** the "personal data" of: ■ ≥ **100,000** New Jersey residents, excluding data controlled or processed solely for the purpose of completing a payment transaction; *or* ■ ≥ **25,000** New Jersey residents *and* derive revenue or receive a discount on the price of any good or services from the sale of "personal data."	"Personal data": Any information that is linked or reasonably linkable to an identified or identifiable person.

2 However, a small business may not engage in the sale of sensitive data without prior consent of the consumer. *See* Nebraska Data Privacy Act, §§ 3(1)(c), 18(1).

				Scope		Protected Data
State	**Statute**	**Regulations?**	**Effective Date**	**Protected Individuals**	**Regulated Entities**	**Definition of Personal Data/Information**
Oregon	Oregon Consumer Privacy Act (OCPA), *Or. Rev. Stat. § 646A.570*	No (none expected)	■ July 1, 2024 (for-profit entities) – The requirement to recognize and honor the sale of data opt-out signals is not enforceable until January 1, 2026 ■ July 1, 2025 (501(c)(3) entities)	Oregon *resident*	Entities that (1) conduct business in Oregon *or* that provide products or services to Oregon residents, *and* (2) during a calendar year **control or process** the "personal data" of: ■ ≥ **100,000** Oregon consumers, excluding data controlled or processed solely for the purpose of completing a payment transaction; *or* ■ ≥ **25,000** Oregon consumers *and* derive **more than 25% of gross revenue from the sale** of "personal data."	"Personal data": Data, derived data, or any unique identifier that is linked to or reasonably linkable to one or more consumers or to a device that identifies, is linked to, or is reasonably linkable to one or more consumers in a household.
Rhode Island	Rhode Island Data Transparency and Privacy Protection Act (RITPPA), *6 R.I. Gen. Laws § 6-48.1*	No (none expected)	January 1, 2026	Rhode Island *resident*	For-profit entities that (1) conduct business in Rhode Island *or* produce products or services that are targeted to Rhode Island residents, *and* (2) during the preceding calendar year **control or process** the "personal data" of: ■ ≥ **35,000** Rhode Island customers, excluding data controlled or processed solely for the purpose of completing a payment transaction; *or* ■ ≥ **10,000** Rhode Island customers *and* derived **more than 20% of gross revenue from the sale** of "personal data."	"Personal data": Any information that is linked or reasonably linkable to an identified or identifiable individual.
Tennessee	Tennessee Information Protection Act (TIPA), *Tenn. Code Ann. 47-18-3301*	No (none expected)	July 1, 2025	Tennessee *resident*	For-profit entities that (1) conduct business in Tennessee *or* produce products or services targeted to Tennessee residents, (2) exceed **US$25m in revenue**, *and* (3) **control or process** the "personal information" of: ■ ≥ **175,000** Tennessee consumers during a calendar year; *or* ■ ≥ **25,000** Tennessee consumers *and* derive **more than 50% of gross revenue from the sale** of "personal information."	"Personal information": Any information that is linked or reasonably linkable to an identified or identifiable natural person.

				Scope		Protected Data
State	**Statute**	**Regulations?**	**Effective Date**	**Protected Individuals**	**Regulated Entities**	**Definition of Personal Data/Information**
Texas	Texas Data Privacy and Security Act (TDPSA), *Texas Bus. & Comm. Code 541.001*	No (none expected)	July 1, 2024	Texas *resident*	For-profit entities that (1) conduct business in Texas *or* produce a product or service consumed by Texas residents, (2) process or engage in the sale of "personal data," *and* (3) is not a small business as defined by the U.S. Small Business Administration.[3]	"Personal data": Any information, including sensitive data, that is linked or reasonably linkable to an identified or identifiable individual. Pseudonymous data is included when the data is used in conjunction with additional information that reasonably links the data to an identified or identifiable individual.
Utah	Utah Consumer Privacy Act (UCPA), *Utah Code Ann. 13-61-101*	No (none expected)	December 31, 2023	Utah *resident*	For-profit entities that (1) do business in Utah *or* produce a product or service targeted to Utah residents, (2) have annual revenue of **US$25m** or more, *and* (3) **control or process** the "personal data" of: ■ ≥ **100,000** Utah residents during a calendar year; *or* ■ ≥ **25,000** Utah residents *and* derive **over 50% of their gross revenue from the sale** of "personal data."	"Personal data": Information that is linked or reasonably linkable to an identified individual or an identifiable individual.
Virginia	Virginia Consumer Data Protection Act (VCDPA), *Va. Code 59.1-575*	No (none expected)	January 1, 2023	Virginia *resident*	For-profit entities that (1) do business in Virginia *or* produce products or services targeted to Virginia residents, *and* (2) **control or process** the "personal data" of: ■ ≥ **100,000** Virginia residents during a calendar year; *or* ■ ≥ **25,000** Virginia residents *and* derive **more than 50% of gross revenue from the sale** of "personal data."	"Personal data": Any information that is linked or reasonably linkable to an identified or identifiable natural person.

3 However, a small business may not engage in the sale of sensitive data without receiving prior consent from the consumer.

	Key Exempted Entities							Key Protected Data (PI) Exceptions										
State	Public sector	Nonprofits	Organizations subject to GLBA (financial institutions and affiliates)	HIPAA-covered entities/ business associates	Higher education institutions	National securities associations	State insurance producers	De-identified data	Publicly available data	Aggregate data	B2B data	Employment data	DPPA-covered data	FCRA-covered data	FERPA-covered data	GLBA-covered data	HIPAA-covered data	Emergency contact data
California	X	X[4]		DL				X	X	X			X	X		X	X	
Colorado	L[5]		X	DL[6]	L[7]	X		X	X		X	X[8]	X	X	X	X	X	
Connecticut	X[9]	X	L[10]	EL	X	X	X	X	X		X	X	X	X	X	X	X	
Delaware	X	L[11]	X	L, DL[12]		X		X	X		X	X	X	X	X	X	X	X
Florida	X	X	X	EL	X			X	X	X	X	X	X	X	X		X	X[13]
Indiana	X	X[14]	X	EL	X			X	X	X	X	X	X	X	X		X	
Iowa	X	X	X	EL[15]	X			X	X	X	X	X	X	X	X	X	X	
Kentucky	X	X	X	EL, DL[16]	X			X	X		X	X	X	X	X	X	X	X
Maryland	X	L[17]	X	DL		X		X	X		X	X	X	X	X	X	X	X

4 Based on the CPRA's definition of a "business," a nonprofit can fall within scope of the law. The CPRA defines a "business" as an entity that owns or is owned by a business as defined under the CPRA. As such, a nonprofit organization that is owned by a business entity that meets the CPRA revenue threshold or a nonprofit that owns a for-profit entity that meets the CPRA revenue threshold will likely be subject to the CPRA. *See* Cal. Civil Code § 1798.140(d)(2). Further, the CPRA applies to joint ventures. Under the CPRA, a business is a joint venture when each business entity has at least 40% interest. *See* Cal. Civil Code § 1798.140(d)(3).

5 Exemption is limited and only applies if data is used for noncommercial purposes.

6 Solely to the extent the covered entity or business associate maintains the information in the same manner as HIPAA-protected health information or other exempt information.

7 Exemption is limited and only applies to information maintained by postsecondary institutions.

8 The CPA regulates employer processing of biometric identifiers of employees/prospective employees and when employers may require consent to process as a condition of employment. *See* Colo. Rev. Stat. § 6-1-1314.

9 The CTDPA specifies that it also does not apply to any candidate committee, national committee, party committee, or political committee, as such terms are defined by Connecticut law. *See* Conn. Pub. Act. 25-113 § 7(a)(4) (effective July 1, 2026).

10 Limited to (A) banks and credit unions, any any affiliate or subsidiary, that is (i) only and directly engaged in financial activities as described in 12 U.S.C. § 1843(k), (ii) regulated and examined by the Department of Banking or an applicable federal bank regulatory agency, and (iii) has established a program to comply with all applicable requirements established by such regulators concerning personal data; or (B) an agent, broker-dealer, investment advisor, or investment advisor agent (as such terms are defined by state law) who is regulated by the Department of Banking or SEC. *See id.* at (a)(11)-(12).

11 Exemption is limited to nonprofit organizations "dedicated exclusively to preventing and addressing insurance crime" and nonprofit organizations that provide services to victims of child abuse, domestic violence, human trafficking, sexual assault, violent felony, or stalking. *See* Del. HB 154 § 12D-103(b)(3) & (c)(13).

12 Information is exempt "to the extent it is used for public health, community health, or population health activities and purposes, as authorized by HIPAA, when provided by or to a covered entity or when provided by or to a business associate pursuant to a business associate agreement with a covered entity." *See* Del. HB 154 § 12D-103(c)(6).

13 Data processed or maintained as the emergency contact information of an individual used for emergency contact purposes is exempt. *See* Fla. Stat. § 501.704(17).

14 "Nonprofit organizations" means any organization exempt from taxation under Section 501(c)(3), 501(c)(6), or 501(c)(19) of the Internal Revenue Code. *See* Ind. SB 5 Sec. 18.

15 Solely to the extent the information (i) originates from and is intermingled to be indistinguishable from, or (ii) is treated in the same manner as, other exempt information.

16 Exemption applies to (i) HIPAA-covered entities and business associates; (ii) HIPAA-protected health information; (iii) information collected by a HIPAA-covered entity health care provider that maintains protected health information in accordance with HIPAA; and (iv) information included in a HIPAA limited data set to the extent used, disclosed, and maintained as specified in HIPAA. *See* Ky. H.B. 473, 2025 Reg. Sess. § 1(3)(i)-(j) (effective January 1, 2026).

17 Exemption is limited to a nonprofit controller that "processes or shares personal data solely for the purposes of assisting: law enforcement agencies in investigating criminal or fraudulent acts relating to insurance; or first responders in responding to catastrophic events." *See* Md. SB 541 § 14-4603(A)(4).

FOLEY & LARDNER LLP

	Key Exempted Entities							Key Protected Data (PI) Exceptions										
State	Public sector	Nonprofits	Organizations subject to GLBA (financial institutions and affiliates)	HIPAA-covered entities/ business associates	Higher education institutions	National securities associations	State insurance producers	De-identified data	Publicly available data	Aggregate data	B2B data	Employment data	DPPA-covered data	FCRA-covered data	FERPA-covered data	GLBA-covered data	HIPAA-covered data	Emergency contact data
Minnesota	X	L[18]	L[19]	DL[20]			X	X	X		X	X	X	X	X	X	X	X[21]
Montana	X	L[22]	L[23]	EL	X	X	X	X	X		X	X	X	X	X	X	X	
Nebraska	X	X	X	EL	X			X	X		X	X	X	X	X	X	X	X
New Hampshire	X	X	X	EL	X	X		X	X		X	X	X	X	X	X	X	X
New Jersey	X		X	DL			X	X	X		X	X	X[24]	X		X	X	
Oregon	X	L[25]	L[26]	DL			X	X	X		X	X	X	X	X	X	X	X
Rhode Island	X	X	X	EL	X	X		X	X	X	X	X	X	X	X	X	X	L[27]
Tennessee	X	X	X	EL	X		X[28]	X	X	X	X	X	X	X	X	X	X	X
Texas	X	X	X	EL	X			X	X		X	X	X	X	X	X	X	X
Utah	X	X	X	EL	X			X	X	X	X	X	X	X	X	X	X	
Virginia	X	X	X	EL	X			X	X		X	X	X	X	X	X	X	

18 Exemption is limited to a "nonprofit organization that is established to detect and prevent fraudulent acts in connection with insurance." *See* Minnesota Consumer Data Privacy Act, § 325M.(12)(2)(a)(20).
19 Limited to "a state or federally chartered bank or credit union, or an affiliate or subsidiary that is principally engaged in financial activities, as described in" 12 U.S.C. § 1843(k). *See* Minnesota Consumer Data Privacy Act, § 325M.12(2)(a)(16).
20 Solely to the extent the information originates from, and intermingles to be indistinguishable with, any HIPAA-protected health information maintained by the covered entity or business associate. *See* Minnesota Consumer Data Privacy Act, § 325O.12(2)(a)(5).
21 Solely to the extent collected or maintained in the course of an individual acting as a job applicant to or an employee, owner, director, officer, medical staff member, or contractor of a business. *See* Minnesota Consumer Data Privacy Act, § 325M.12(2)(a)(13)(ii).
22 Exemption is limited to a "nonprofit organization that is established to detect and prevent fraudulent acts in connection with insurance." *See* Mont. S.B., 297, 69th Leg. § 4(1)(b) (effective October 1, 2025).
23 Limited to "a state or federally chartered bank or credit union, or an affiliate or subsidiary that is principally engaged in financial activities, as described in" 12 U.S.C. § 1843(k). *See id.* at (1)(e)-(f).
24 Excepts "the sale of a consumer's personal data by the New Jersey Motor Vehicle Commission that is permitted by" the federal DPPA. *See* New Jersey Data Privacy Act § 10(e).
25 Exemption is limited and only applies to a nonprofit organization that is established to detect and prevent fraudulent acts in connection with insurance or that provides programming to radio or television services. *See* Ore. SB 619 § 2(r) and (s)(C).
26 Only "financial institutions" as defined under Ore. Rev. Stat. § 706.008 or a financial institution's affiliate or subsidiary that is only and directly engaged in financial activities are subject to a full exemption. *See* Ore. SB 619 § 2(l).
27 Solely to the extent that the data is processed or maintained in the course of an individual applying to, employed by, or acting as an agent or independent contractor of a controller, processor, or third party. *See* R.I. SB 2500A § 6-48.1-3(e)(15).
28 TIPA does not apply to Title 56 licensed insurance companies. *See* Tenn. Stat. § 47-18-3210(a)(3).

	Consumer Rights							Sale of Personal Data	Business Obligations				Obtain Opt-in Consent for Processing		
State	To know/access	To data portability	To erasure/ deletion	To rectify/ correct	To opt out of sale	To opt out of processing for cross-contextual behavioral/ targeted advertising	To opt out of profiling	"Sales" include disclosures for other valuable consideration	Provide a privacy notice	Third-party agreement with processors	Avoid dark patterns to obtain consumer consent	Conduct risk assessments	Sensitive information	PI of minors (under age listed)	Other
California	X	X	X	X	X	X	X[29]	X	X[30]	X	X	X[31]	X[32]	S/16	X[33]
Colorado	X[34]	X	X	X	X	X	X	X	X[35]	X	X	X[36]	X	18[37]	X[38]
Connecticut	X[39]	X	X	X	X[40]	X	X[41]	X	X	X	X	X[42]	X	13	X[43]
Delaware	X	X	X	X	X	X	X	X	X	X		X	X	13	X[44]
Florida	X	X	X	X	X	X	X	X	X[45]	X	X	X	X	13	X[46]
Indiana	X	L[47]	X	L[48]	X	X	X		X	X		X	X	13	

29 The right to opt out of profiling is subject to future regulations. *See* Cal. Civ. Code § 1798.185(a)(16), (d).
30 California also requires a notice at or before the time of collection that has additional content requirements.
31 Additional regulations related to risk assessments forthcoming.
32 A business must obtain opt-in consent for processing sensitive personal information if previously limited by the consumer. *See* Cal. Civ. Code § 1798.120(d).
33 A business must obtain opt-in consent for processing upon entry into a financial incentive program. *See* Cal. Civ. Code § 1798.125(b)(3).
34 The CPA's right to access explicitly includes a consumer's right to access biometric data. *See* Colo. Rev. Stat. § 6-1-1314(5).
35 Colorado also requires a controller that controls or processes biometric identifiers to include a biometric identifier notice. *See* Colo. Rev. Stat. § 6-1-1314(2)(a)-(b), (4).
36 Controllers must additionally conduct a yearly assessment to determine whether the storage of biometric identifiers, or any personal data generated from a digital or physical photograph or an audio or video recording, is necessary and adequate. *See* 4 Colo. Code Regs. § 904-3, Rule 6.11.
37 The CPA regulates "children" (under age 13) and "minors" (under age 18) differently. A controller needs consent when they actually know or willfully disregard the fact that the consumer is a minor or when using any system design feature to significantly increase, sustain, or extend the use by a consumer who the controller actually knows or willfully disregards is a minor. *See* 4 Colo. Code Regs. § 904-3, Rule 7.03(A)(5), (6).
38 A controller that offers any online service, product, or feature must obtain opt-in consent to process the personal data of a minor (under age 18) for: (i) the purposes of targeted advertising, sale, or profiling in furtherance of decisions that produce legal or similarly significant effects; (ii) for any processing purpose other than the processing purpose that the controller disclosed at the time the controller collected the minor's personal data or that is reasonably necessary for, and compatible with, the processing purpose that the controller disclosed at the time the controller collected the minor's personal data; or (iii) for longer than is reasonably necessary to provide the online service, product, or feature, where the controller has actual knowledge, or willfully disregards, that the consumer is a minor. *See* Colo. Rev. Stat. § 6-1-1308.5.
39 The CTDPA's right to access includes a consumer's right to access any inferences about the consumer derived from their personal data and whether a controller or processor is processing such personal data for the purposes of profiling. *See* Conn. Pub. Act. 25-113 § 8(a)(1) (effective July 1, 2026).
40 Upon request of the consumer, a controller must provide a list of third parties to whom it has sold the consumer's personal data. *See id* at (a)(7).
41 If a consumer's personal data was processed for the purposes of profiling, the consumer has the right to: (i) question the result of such profiling, (ii) be informed of the reason that such profiling resulted in a certain decision, (iii) review the personal data processed for the purposes of profiling, (iv) if the profiling concerned decisions related to housing, correct any incorrect personal data processed and have the decision re-evaluated. *See id.* at (a)(6).
42 Only for processing that presents a heightened risk of harm to a consumer. Effective July 1, 2026, this includes: (1) the processing of personal data for the purposes of targeted advertising; (2) the sale of personal data; (3) the processing of personal data for the purposes of profiling in certain cases; and (4) the processing of sensitive data. *See* Conn. Pub. Act. 25-113 § 11(a).
43 A business that has actual knowledge or willfully disregards a consumer is a minor under the age of 18 is prohibited from processing personal data for the purposes of targeted advertising, any sale of personal data, or profiling, unless such processing is reasonably necessary to provide an online service, product, or feature. *See* Conn. Pub. Act. 25-113 § 9(l).
44 A controller may not process a minor's personal data for the purposes of targeted advertising without obtaining consent. *See* Del. HB 154 § 12D-106(a)(7).
45 If a controller sells sensitive data or biometric data, it must provide an additional privacy notice. If a controller sells sensitive data, it must provide the following notice: "NOTICE: This website may sell your sensitive personal data." *See* Fla. Stat. §§ 501.711 (f)(2)-(3).
46 A controller must obtain opt-in consent upon entry into a financial incentive program. *See* Fla. Stat. § 501.71(2)(c).
47 The right to data portability only applies to personal data provided by the consumer. *See* 2023 Ind. Code 24-15-3 § 1(b)(4).
48 The right to correct only applies to personal data provided by the consumer. *See* 2023 Ind. Code 24-15-3 § 1(b)(2).

	Consumer Rights							Sale of Personal Data	Business Obligations				Obtain Opt-in Consent for Processing		
State	To know/access	To data portability	To erasure/ deletion	To rectify/ correct	To opt out of sale	To opt out of processing for cross-contextual behavioral/ targeted advertising	To opt out of profiling	"Sales" include disclosures for other valuable consideration	Provide a privacy notice	Third-party agreement with processors	Avoid dark patterns to obtain consumer consent	Conduct risk assessments	Sensitive information	PI of minors (under age listed)	Other
Iowa	X	X[49]	X[50]		X[51]	X			X	X				13	
Kentucky	X	X[52]	X	X	X	X	X		X	X		X	X	13	
Maryland	X	X	X	X	X	X	X	X	X	X	X	X		13	
Minnesota	X	L[53]	X	X	X	X	X[54]	X	X	X	X	X	X	13	
Montana	X	X	X	X	X	X	X	X	X	X	X	X	X	13/18[55]	X[56]
Nebraska	X	L[57]	X	X	X	X	X	X	X	X	X	X	X	13	
New Hampshire	X	X	X	X	X	X	X	X	X	X	X	X	X	13	X[58]
New Jersey	X	X	X	X	X	X	X	X	X	X	X	X	X	13	X[59]
Oregon	X	X	X	X	X	X	X	X[60]	X	X		X	X	13	X[61]
Rhode Island	X	X	X	X	X	X	X	X	X	X	X	X	X	13	
Tennessee	X	X	X	X	X	X	X		X	X		X	X	13	
Texas	X	X	X	X	X	X	X	X	X	X	X	X	X	13	
Utah	X	X	X	X	X	X			X	X				13	
Virginia	X	X	X	X	X	X	X		X	X		X	X	13	

49 The right to data portability only applies to personal data provided by the consumer. *See* 2023 Iowa SF 262 § 715D.3 1.c.
50 The right to delete only applies to personal data provided by the consumer. *See* 2023 Iowa SF 262 § 715D.3 1.b.
51 The sale of personal data only applies to the exchange of personal data for monetary consideration by the controller to a third party. *See* Iowa SF 262 § 715D.1. 25.
52 The right to data portability only applies to personal data provided by the consumer. *See* Kentucky Consumer Data Protection Act, § 3(2)(d).
53 The right to data portability only applies to personal data provided by the consumer. *See* Minnesota Consumer Data Privacy Act, § 325M.14(1)(e).
54 If a consumer's personal data was processed for the purposes of profiling, the consumer has the right to: (i) question the result of such profiling, (ii) be informed of the reason that such profiling resulted in a certain decision, (iii) review the personal data processed for the purposes of profiling, and (iv) correct any incorrect personal data processed and have the decision re-evaluated, if profiling is based upon inaccurate personal data. *See id.* at § 325M.14(1)(g).
55 A controller that offers an online service, product, or feature to a consumer whom the controller actually knows or willfully disregards is a minor (under age 18) may not, without consent: (i) sell the minor's data or process the minor's data for purposes of targeted advertising or profiling; (ii) process the data for any processing purpose other than the purpose disclosed at the time the controller collected the minor's personal data or that is reasonably necessary for and compatible with that processing purpose; or (iii) process the data for longer than is reasonably necessary. There are also restrictions on collecting the minor's precise geolocation. *See* Mont S.B., 297, 69th Leg. § 9(2) (effective October 1, 2025).
56 A controller must obtain opt-in consent for processing personal data for the purposes of targeted advertising, or sale, under circumstances where a controller has actual knowledge or willfully disregards that the consumer is at least 13 years of age but younger than 16 years of age. *See* Montana Consumer Data Privacy Act, § 7(2)(d).
57 The right to data portability only applies to personal data provided by the consumer. *See* Nebraska Data Privacy Act, § 7(2)(d).
58 A controller must obtain opt-in consent for processing personal data for the purposes of targeted advertising, or sale, under circumstances where a controller has actual knowledge that the consumer is at least 13 years of age but younger than 16 years of age. *See* N.H. Rev. Stat. Ann. § 507-H:6(I)(g).
59 A controller shall not process the personal data of a consumer for the purposes of targeted advertising, the sale of the consumer's personal data, or profiling in furtherance of decisions that produce legal or similarly significant effects concerning a consumer without the consumer's consent, under circumstances where a controller has actual knowledge, or willfully disregards, that the consumer is at least 13 years of age but younger than 17 years of age. *See* New Jersey Data Privacy Act, § 9(a)(7).
60 It is prohibited to sell a consumer's precise geological location data. Ore. Rev. Stat. § 646.578(2)(d)(B).
61 A controller may not sell or process the personal information of a consumer under the age of 16 for the purposes of targeted advertising or profiling in furtherance of decisions that produce legal or other significant effects. Ore. Rev. Stat. § 646A.278(2) (Updated by HB 2008-B, 2025).

	Consumer Rights Requests		Sensitive Data																		Enforcement		
State	Statutory response period (calendar days)	Extended response period (total calendar days)	Individual's status as a victim of a crime	Biometric data[62]	Children's data (under age listed)	Citizenship status	Electronic communication	Financial account information	Genetic data	Biological data	Neural data	Precise/specific geolocation data (feet)	Government ID	Health data	Race/ethnicity	Religious beliefs	Philosophical beliefs	Sex life	Sexual orientation	Status as transgender or non-binary	Union membership	Private right of action	Opportunity to cure	Fines for violations
California	45[63]	90		X	16		X	X	X		X	1,850	X	X[64]	X	X	X	X	X		X	L[65]	L[66]	Up to $2,663 per violation or up to $7,988 per intentional violation[67]
Colorado	45	90		X	18	X			X	X	X			CD	X	X		X	X				X	Up to $20,000 per violation[68]
Connecticut	45	90	X	X[69]	13	X		X	X		X	1,750	X	MCTD	X	X		X	X	X			X	Up to $5,000 for willful violations[70]
Delaware	45	90		X	13	X			X			1,750		CD	X	X		X	X	X			X[71]	Up to $10,000 per violation[72]
Florida	45	60[73]		X	18	X			X			1,750		D	X	X			X				L[74]	Up to $50,000 per violation and treble damages[75]
Indiana	45	90		X	13	X			X			1,750		D	X	X			X					Up to $7,500 per violation

62 When processed for the purpose of uniquely identifying an individual.
63 California also requires that a business provide an acknowledgement of the consumer's request within 10 business days.
64 Under the CPRA, the definition of "sensitive personal information" includes "personal information collected and analyzed concerning a consumer's health." Unlike the other state consumer privacy laws, the CPRA does not distinguish between mental and physical health. *See* Cal. Civ. Code § 1798.140(ae)(2)(B).
65 The private right of action under the CPRA is limited to security breaches. *See* Cal. Civ. Code § 1798.150.
66 Under the CPRA, the cure period for administrative actions brought by the California attorney general or California Privacy Protection Agency (CPPA) is only at the CPPA's discretion. *See* Cal. Civ. Code § 1798.199.45. For actions brought by consumers for security breaches, there is a cure period of 30 days. *See* Cal. Civ. Code § 1798.150(b).
67 Note, for actions brought by consumers for security breaches, they can recover actual damages or up to US$799, whichever is greater.
68 CPA violations constitute deceptive trade practices under Colo. Rev. Stat. § 6-1-112.
69 CTDPA treats biometric data, or information derived therefrom, as sensitive information regardless of whether the purpose of the processing of the biometric data is to uniquely identify an individual. *See* Conn. Pub. Act. 25-113 § 5(39) (Effective July 1, 2026).
70 CTDPA violations constitute unfair trade practices under Connecticut's Unfair Trade Practice Act. *See* 2022 Conn. SB 6 § 11(e); Conn. Gen. Stat. § 42-110b.
71 The general right to cure violations expires on December 31, 2025. Starting on January 1, 2026, the Department of Justice may provide an ability to cure violations but is not required to.
72 Violations of the DPDPA are considered an unlawful practice under Del. Code Tit. 6 § 2513. *See* Del. HB § 12D-111(e).
73 Within 60 days of receiving a verifiable consumer request, a controller must provide the consumer with notice that it has complied with the consumer's request. *See* Fla. Stat. § 501.706(4)
74 The cure period is at the discretion of the Department of Legal Affairs and, depending on certain factors, may grant a 45-day cure period. *See* Fla. Stat. § 501.72(2).
75 The Department of Legal Affairs can award treble damages if a violation involves a known child, a controller fails to delete or correct a consumer's personal data after receiving a verifiable consumer request or continues to sell or share a consumer's personal data after a consumer opted out of selling or sharing. *See* Fla. Stat. § 501.72(1)(a)-(c).

	Consumer Rights Requests		Sensitive Data																			Enforcement		
State	Statutory response period (calendar days)	Extended response period (total calendar days)	Individual's status as a victim of a crime	Biometric data[76]	Children's data (under age listed)	Citizenship status	Electronic communication	Financial account information	Genetic data	Biological data	Neural data	Precise/specific geolocation data (feet)	Government ID	Health data	Race/ethnicity	Religious beliefs	Philosophical beliefs	Sex life	Sexual orientation	Status as transgender or non-binary	Union membership	Private right of action	Opportunity to cure	Fines for violations
Iowa	90	135		X	13	X			X			1,750		D	X	X			X				X	Up to $7,500 per violation
Kentucky	45	90		X	13	X			X			1,750		D	X	X			X				X	Up to $7,500 per violation
Maryland	45	90		X	13	X			X			1,750		CD	X	X		X	X	X			L[77]	Up to $10,000 per violation and up to $25,000 for subsequent violations[78]
Minnesota	45	90		X	13	X			X			X[79]		CD	X	X			X				L[80]	Up to $7,500 per violation
Montana	45	90		X	13	X			X			1,750		CD	X	X		X	X					Up to $7,500 per violation
Nebraska	45	90		X	13	X			X			1,750		D	X	X			X				X	Up to $7,500 per violation
New Hampshire	45	90		X	13	X			X			1,750		CD	X	X		X	X				L[81]	Not specified[82]
New Jersey	45	90		X	13	X		X	X			1,750		MCTD	X	X		X	X	X			L[83]	Up to $10,000 per violation and up to $20,000 for subsequent violations

76 When processed for the purpose of uniquely identifying an individual.
77 Before April 1, 2027, a controller or processor will have 60 days to cure. *See* Md. SB 541 § 14-4614(c)(1).
78 MODPA violations constitute an unfair, abusive, or deceptive trade practice under Md. Code Ann., Com. Law § 13-410. *See* Md. SB 541 § 14-4613(a)(1).
79 Specific geolocation data means "information derived from technology, including but not limited to global positioning system level latitude and longitude coordinates or other mechanisms, that directly identifies the geographic coordinates of a consumer or a device linked to a consumer with an accuracy of more than three decimal degrees of latitude and longitude or the equivalent in an alternative geographic coordinate system, or a street address derived from coordinates." *See* Minnesota Consumer Data Privacy Act, § 325M.11(w).
80 Before January 31, 2026, a controller or processor will have 30 days to cure. *See* Minnesota Consumer Data Privacy Act, § 325M.20(a).
81 Through December 31, 2025, controllers will have 60 days to cure. Beginning January 1, 2026, the attorney general may grant an opportunity to cure in accordance with a numerated list of factors. *See* N.H. Rev. Stat. Ann. § 507–H:11(II), (III).
82 A violation constitutes an unfair method of competition or any unfair or deceptive act or practice in the conduct of any trade or commerce under N.H. Rev. Stat. Ann. § 358-A:2.
83 For the first 18 months after the law's effective date, controllers will have a 30-day cure period.

	Consumer Rights Requests		Sensitive Data																			Enforcement		
State	Statutory response period (calendar days)	Extended response period (total calendar days)	Individual's status as a victim of a crime	Biometric data[75]	Children's data (under age listed)	Citizenship status	Electronic communication	Financial account information	Genetic data	Biological data	Neural data	Precise/specific geolocation data (feet)	Government ID	Health data	Race/ethnicity	Religious beliefs	Philosophical beliefs	Sex life	Sexual orientation	Status as transgender or non-binary	Union membership	Private right of action	Opportunity to cure	Fines for violations
Oregon	45	90	X	X	13	X			X			1,750[84]		CD	X	X			X	X			X[85]	Up to $7,500 per violation
Rhode Island	45	90		X	13	X			X			1,750		CD	X	X		X	X					Up to $10,000 per violation[86] Up to $100 and no more than $500 per violation for intentional disclosures of personal data
Tennessee	45	90		X	13	X			X			1,750		D	X	X			X				X	Up to $7,500 per violation and treble damages for willful or knowing violations
Texas	45	90		X	13	X			X			1,750		D	X	X		X	X				X	Up to $7,500 per violation
Utah	45	90		X		X			X			1,750		MCTD	X	X			X				X	Actual damages to affected consumers and up to $7,500 per violation
Virginia	45	90		X	13	X			X			1,750		D	X	X			X				X	Up to $7,500 per violation

84 Precise Geolocation is defined as information that accurately identifies within a radius of 1,750 feet a consumer's present or past location, or the present or past location of a device that links or is linkable to a consumer by means of technology that includes, but is not limited to, a global positioning system that provides latitude and longitude coordinates. *See* Or. Rev. Stat. § 646A.570(18)(a)(C).

85 The 30-day cure period generally sunsets on January 1, 2026, except that for certain controllers that are a noncommercial educational broadcast station (as defined in 47 U.S.C. 397), the 30-day cure period sunsets July 1, 2026. *See* O.R. SB 1121 § 5 (2025).

86 A violation constitutes a deceptive trade practice in violation of R.I. Stat. § 6-13.1. *See* R.I. SB 2500A § 6-48.1-8(a).

About Foley

Foley & Lardner LLP is a preeminent law firm that stands at the nexus of the energy, health care and life sciences, innovative technology, and manufacturing sectors. We look beyond the law to focus on the constantly evolving demands facing our clients and act as trusted business advisors to deliver creative, practical, and effective solutions. Our 1,100 lawyers across 27 offices worldwide partner on the full range of engagements from corporate counsel to IP work and litigation support, providing our clients with a one-team solution to all their needs. For nearly two centuries, Foley has maintained its commitment to the highest level of innovative legal services and to the stewardship of our people, firm, clients, and the communities we serve.

FOLEY

FOLEY & LARDNER LLP

AUSTIN | BOSTON | BRUSSELS | CHICAGO | DALLAS | DENVER | DETROIT | HOUSTON | JACKSONVILLE | LOS ANGELES | MADISON | MEXICO CITY | MIAMI | MILWAUKEE
NASHVILLE | NEW YORK | ORLANDO | RALEIGH | SACRAMENTO | SALT LAKE CITY | SAN DIEGO | SAN FRANCISCO | SILICON VALLEY | TALLAHASSEE | TAMPA | TOKYO | WASHINGTON, D.C.