PILLAR LEGAL

New U.S. State Privacy Laws in the Pipeline for 2024

U.S. TECH LAW UPDATE[1]

January 24, 2024

By: Greg Pilarowski | Alexandra Ashbrook

In an era defined by rapid digital evolution, U.S. states are ramping up their efforts to protect citizens' personal information. Following the landmark California Consumer Privacy Act in 2018, as amended by the California Privacy Rights Act in 2020, a handful of states enacted their own privacy legislation. In 2023, data privacy laws in Virginia, Colorado, Connecticut, and Utah took effect, and many other states passed similar legislation for implementation over the next few years.[2] Starting in 2024, companies will be required to comply with new state-level data privacy laws.

While the number of states implementing data protections continues growing, the U.S. still lacks a comprehensive data privacy law at the federal level. The American Data Privacy and Protection Act was approved by the Committee on Energy and Commerce on July 20, 2022, by a wide margin, but failed to advance to the House or Senate floors for a full vote.[3] Negotiations for a revised version of the bill are underway, but its future is uncertain.[4] Several other comprehensive data privacy laws were introduced at the federal level in 2023, including the Data Care Act and the Online Privacy Act.[5] However, passage of a federal privacy law is complicated by competing priorities and agendas.

Lack of a single data privacy bill applicable across the U.S. means companies must scramble to comply with a patchwork of laws, posing a challenge to those which operate nationwide. While fears of completely disparate privacy requirements across the states have yet to materialize, companies' compliance burden continues to increase as each new state-level data privacy law is passed. One approach that may lessen this burden is looking to the "highest standards" across all active state-level data privacy laws and implementing them, instead of attempting to comply with lower standards in one state, and higher ones in another.

This legal update provides a summary of the five new data privacy laws (including Utah) poised to take effect in 2024. In addition, it identifies the "highest standards" for key data

---

[1] This U.S. Tech Law Update is provided by Pillar Legal, P.C. (the "Firm") as a service to clients and other readers. The information contained in this publication should not be construed as legal advice, and use of this memorandum does not create an attorney - client relationship between the reader and the Firm. In addition, the information has not been updated since the date first set forth above and may be required to be updated or customized for particular facts and circumstances. This U.S. Tech Law Update may be considered "Attorney Advertising" under applicable law. Questions regarding the matters discussed in this publication may be directed to the Firm at the following contact details: +1-925-930-3932 (San Francisco Bay Area office), +86-21-5876-0206 (Shanghai office), email: info@pillarlegalpc.com. Firm website: www.pillarlegalpc.com.

[2] Melissa Griffins Paulk, *US Data Privacy Landscape in the First Half of 2023*, NATIONAL LAW REVIEW (Jun. 6. 2023).

[3] Steve Adler, *Revised American Data Privacy and Protection Act Due to be Released*, THE HIPAA JOURNAL (Apr. 14, 2023).

[4] *Id*.

[5] Muge Fazlioglu, *U.S. privacy legislation in 2023: Something old, something new?*, IAPP (Jul. 26, 2023).

privacy compliance requirements through 2024. Finally, this article contains a charted overview of all U.S. state-level data privacy laws effective through 2024.

I. New U.S. State Privacy Laws Effective in 2024

In 2024, five new data privacy laws will become effective: Utah, Florida, Oregon, Texas, and Montana. Each are briefly discussed below. Please see Section III (U.S. State Privacy Laws in Effect for 2024) for more information on each current and incoming state privacy law.

A. Utah

Utah's Consumer Privacy Act (the "Utah Privacy Law") took effect on December 31, 2023—just before the new year.[6] The Utah Privacy Law is largely similar to other state-level data privacy laws, but contains certain exclusions uncommon to privacy laws generally. For example, the Utah Privacy Law does not give Utah consumers the right to correct inaccurate or incomplete data, nor the right to opt-out of profiling and automated decision making. In addition, it does not require data controllers to conduct data privacy impact assessments.

B. Florida

Florida's Digital Bill of Rights (the "Florida Privacy Law") takes effect on July 1, 2024.[7] Under the Florida Privacy Law, "personal data" is defined broadly as any information that is linked or reasonably linkable to an identified or identifiable individual. The Florida Privacy Law imposes familiar data privacy obligations on data controllers, such as limiting personal data collection, establishing data security practices, and providing consumers with easy-to-understand policies outlining the controller's data privacy practices. It also grants Florida residents familiar rights, such as the right to delete their data and the right to opt-out of sensitive personal data processing, targeted advertising, and profiling. However, unlike other data privacy laws, the Florida Privacy Law applies only to large tech companies such as Google, Amazon, and Apple. Furthermore, it will require search engines to disclose whether political ideology influences search results, and bans government-mandated content moderation on social media.[8]

C. Oregon

Oregon's Consumer Data Privacy Law (the "Oregon Privacy Law") takes effect on July 1, 2024.[9] The Oregon Privacy Law is one of the strongest data privacy bills passed at the state-level to date, borrowing significantly from Colorado's and Connecticut's privacy laws and adding unique provisions, some of which are discussed more below.

- *Device Data Covered.*[10] While other data privacy bills cover personal data that is linkable to a particular individual or consumer, the Oregon Privacy Law also captures device data. Device data, such as an IP address or ad tag, is the data generated by an individual's

[6] Bebe Vanek, *What Utah's new data privacy protection laws mean for you*, UNIVERSITY OF UTAH (Jul. 10, 2023).
[7] Skye Witley, *DeSantis Takes Swing at Big Tech in New Florida Privacy Law*, BLOOMBERG LAW (Jun. 6, 2023).
[8] *Id.*
[9] Sarah Bruno, *Oregon passes comprehensive privacy law*, REUTERS (Aug. 11, 2023).
[10] Oregon Consumer Data Privacy Law, S.B. 619, 82nd Oregon Legislative Assembly (2023), Section 1(13)(a).

electronic device. Device data is sometimes used to analyze consumer behaviors. The law defines "personal data" as "data . . . that is linked to . . . a consumer *or to a device* that identifies . . . one or more consumers in a household." The Oregon legislature in its drafting comments stated it sought to close an obvious loophole present in many other data privacy laws, which could arguably exclude device data from their scope.[11]

- *Expansion of Sensitive Personal Information Definition*.[12] The Oregon Privacy Law includes an individual's "status as transgender or nonbinary" in its definition of sensitive personal data, meaning that collection and use of such personal data will require additional compliance procedures.
- *Additional Consumer Rights*.[13] The Oregon Privacy Law provides Oregon residents with the right to access a list of specific third parties that the controller has disclosed personal data to generally or disclosed a specific resident's personal data to. Other active data privacy laws only require data controllers to disclose categories of third parties personal data is shared with, not specific entities.

D. Texas

Texas' Data and Privacy Security Act (the "Texas Privacy Law") takes effect on July 1, 2024.[14] While many provisions of the Texas Privacy Law largely track other state-level data privacy laws, there are some notable differences. First, the Texas Privacy Law does not apply to small businesses as defined by the U.S. Small Business Administration, an organization that applies varying business size standards across different industries.[15] In addition, the Texas Privacy Law will require data controllers that engage in sensitive personal data sales or biometric data sales to provide the following notices to consumers in their privacy policies:[16]

"NOTICE: We may sell your sensitive personal data."

"NOTICE: We may sell your biometric personal data."

E. Montana

Montana's Consumer Data Privacy Act (the "Montana Privacy Law") takes effect on October 1, 2024.[17] Similar to Florida's law, personal data is broadly defined under the Montana Privacy Act to capture any personal data reasonably linkable to an identifiable individual. The Montana Privacy Act gives many similar rights to Montana residents as other state-level data privacy laws. Notable however is the requirement that data controllers obtain a consumer's prior consent to process sensitive personal data.[18] This requirement contrasts with California's approach, which allows controllers to process sensitive personal data unless a consumer opts out.

---

[11] See the Oregon legislature's drafting comments on the OCDPL here.
[12] Oregon Consumer Data Privacy Law, S.B. 619, 82nd Oregon Legislative Assembly (2023), Section 1(18)(a)(A).
[13] Oregon Consumer Data Privacy Law, S.B. 619, 82nd Oregon Legislative Assembly (2023), Section 3(1)(a)(B).
[14] Matt Stringer, *New Texas Data and Privacy Security Act Aims to Increase Protections for Online User Data*, THE TEXAN (Jun. 19, 2023).
[15] Texas Data and Privacy Security Act, H.B. No. 4, 88th Leg. Sess. (2023), Section 541.002(a)(3). What entities qualify as a "small" business varies by industry. You can read more about the Small Business Association's size standards here.
[16] Texas Data and Privacy Security Act, H.B. No. 4, 88th Leg. Sess. (2023), Section 541.102(b), (c).
[17] Tiffany Stecker, *Montana Joins State Data Privacy Patchwork as Governor Signs Law*, BLOOMBERG LAW (May 22, 2023).
[18] Consumer Data Privacy Act, S.B. 0384, 68th Legislature (2023), Section 8(2)(b).

II. "Highest Standard" Approach to US Data Privacy Compliance

Due to the lack of comprehensive privacy legislation at the federal level, businesses must navigate compliance with a patchwork of state-level privacy laws. This can be difficult in the digital era when consumers across the U.S. may access a business' products or services in states where the business does not have a physical presence, subjecting the business to that state's privacy laws. Instead of implementing a different privacy approach in each state where a business has customers, businesses should consider adopting the highest standards of currently-enacted privacy laws. Note, however, that each state's privacy laws contain unique differences, necessitating a thorough understanding of each state's data privacy laws for full compliance. To help companies navigate the patchwork, the below table identifies the highest standards in 2024 for certain key US privacy law requirements.

Key Requirement	"Highest Standard" in 2024
Privacy Notice The business must provide notice to consumers about the business' personal data privacy practices. While specific obligations vary from state-to-state, most states at the minimum require disclosures regarding the personal data collected by the business, why the business collects such personal data, and what personal data the business shares and with whom. In 2024, Oregon[19] and California[20] will set the highest standards for privacy notice disclosures.	Businesses must disclose: • A list of the categories of personal data (including sensitive personal data) the company collected in the preceding 12 months (California requires reference to the categories set forth in the CCPA or CPRA); • The categories of sources from which the data is collected; • The business or commercial purpose for collecting, selling, or sharing personal data for each category; • The categories of personal data that the business shares with third parties; • The categories of third parties to whom the business discloses personal data; • The length of time the business intends to retain each category of personal data, or the criteria used to determine that period; • Specific descriptions of all user rights; • A clear description of any processing of personal data in which the business engages for the purpose of targeted advertising or profiling the consumer in furtherance of decisions that may produce legal effects or effects of similar significance, and a procedure by which the consumer may opt-out of this type of processing; and • If a business buys, receives, sells, or shares personal data of 10M+ California consumers in a calendar year, metrics regarding the number of requests to know, delete, and opt-out received, complied with, or denied, median or mean response days, and denials by reason.

[19] *See* Oregon SB 619 § 5(4) (2023) for Oregon's privacy policy requirements.
[20] *See* Cal. Civ. Code § 1798.130(B)(5) for California's privacy policy requirements.

Key Requirement	"Highest Standard" in 2024
Purpose Limitation Businesses cannot use personal data beyond those specific purposes made known to the consumer at the time of collection. In the event the business seeks to use previously collected personal data for another purpose, generally the business must receive a second consent from the consumer for that new purpose. While implied in most state-level privacy laws, certain states such as Montana and Colorado explicitly require businesses to obtain a new consent.[21]	Businesses are prohibited from processing personal data for purposes that are not reasonably necessary to or compatible with the disclosed purposes for which the personal data is processed as disclosed to the consumer unless the business obtains a second consent from the consumer.
Reasonable Data Security Businesses are generally required to take appropriate and proportional measures to safeguard consumer data privacy, confidentiality, and integrity. This principle requires implementing security procedures and practices that are commensurate with the sensitivity of the data being processed, and may include measures such as encryption, access controls, regular security assessments, and adoption of privacy-by-design principles. Most state laws do not prescribe specific data security measures, instead opting for flexibility in light of the evolution of data security best practices. However, California's Attorney General has set a bare minimum, setting the highest standard for 2024.	In 2016, the California Attorney General set the CIS Critical Security Controls as "a minimum level of information security that all organizations that collect or maintain personal information should meet." Further, failing to implement the controls constitutes a lack of "reasonable security."[22]

[21] *See* Montana SB 384 § 7(2)(a); *see also* Colorado SB 21-190 § 6-1-1308 (4).
[22] Kamala D. Harris, Attorney General, *California Data Breach Report*, CALIFORNIA DEPARTMENT OF JUSTICE (Feb. 2016).

Key Requirement	"Highest Standard" in 2024
Notices for Sensitive or Biometric Personal Data Use and Sales Most states recognize the collection and processing of sensitive and/or biometric personal data incurs increased risks to consumers. Under a principle of transparency, some states require additional disclosures to consumers where sensitive or biometric personal data is used for certain purposes or sold. Texas and California will set the standards in 2024 with notice requirements related to sensitive and biometric personal data use and sales.	Where a business engages in sensitive personal data sales or biometric data sales, it must provide a notice to consumers of these practices. The notice must state "**NOTICE: We may sell your sensitive personal data**" or "**NOTICE: We may sell your biometric personal data**," as applicable.[23] California requires a link which has the words "**Limit the Use of My Sensitive Personal Information**" to be made available for consumers. The link must allow consumers to restrict the business' use of their sensitive personal data to the limited purposes listed below.[24] This requirement is not applicable to businesses that do not use sensitive personal data to infer characteristics about a consumer and businesses that only use sensitive personal data for the limited purposes set forth in California's privacy law, including:[25] • The uses necessary to perform the services or provide the goods reasonably expected by an average consumer who requests those goods or services; • To prevent, detect, and investigate security incidents that compromise the availability, authenticity, integrity, or confidentiality of stored or transmitted personal data; • To resist malicious, deceptive, fraudulent, or illegal actions directed at the business and to prosecute those responsible; • To ensure the physical safety of natural persons; • For short-term, transient use, including but not limited to non-personalized advertising; • To perform services on behalf of the business (e.g., for maintaining or servicing accounts, providing customer service, or processing orders); • To verify or maintain the quality or safety of a product, service, or device that is owned, manufactured, manufactured for, or controlled by the business; and • To improve, upgrade, or enhance the business' service or device.
Universal Opt-Out Mechanism Recognition Universal opt-out mechanisms are extensions through which users can set their opt-out preferences across websites and browsers. In 2024, California, Colorado, Montana, Oregon, and	Businesses must recognize universal opt-out mechanisms as a valid means to opt out of targeted advertising ad data sales. California's Attorney General references the Global Privacy Control ("GPC") as the leading opt-out mechanism meeting California's standards. The GPC can be set at the browser level for some browsers or through browser extensions. Read more about current universal opt-out mechanisms here.

[23] *See* Tex. Bus. & Com. Code § 541.102(b) and (c).
[24] *See* Cal. Civ. Code § 1798.121.
[25] *See* CCPA Regulations, 11 CCR § 7027(m).

Key Requirement	"Highest Standard" in 2024
Texas will require entities collecting personal data to recognize universal opt-out mechanisms, if applicable.	
Opt-Out Rights for Data Sales, Cross-Context Behavioral and Targeted Advertising, and Profiling "Opt-out" consent requires a consumer to take action to stop the business' collection, use, or sharing of their personal data. Under this approach, a business may assume that users consent to a business' processing activities unless they, for example, uncheck a checkbox that is checked by default, or click a button or link. The following states allow consumers to opt-out of **data sales:** California, Colorado, Connecticut, Utah, Virginia, Florida, Texas, Oregon, and Montana. The following states allow consumers to opt-out of **cross-context behavioral and targeted advertising**: California, Colorado, Connecticut, Utah, Virginia, Florida, Texas, Oregon, and Montana. The following states allow consumers to opt-out of **profiling** (in the furtherance of decisions that produce legal or similarly significant effects concerning the consumer): Colorado, Connecticut, Virginia, Florida, Texas, Oregon, and Montana.[26]	Businesses must provide an opt-out mechanism whereby consumers may opt out of: • Sales of their personal data; • Cross context behavioral and targeted advertising; and • Profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer.
Opt-In Default for Children/Teenagers While the personal data of children under 13 is subject to the Children's Online Privacy Protection Act ("COPPA"), many	At the minimum, businesses must ensure that their collection and processing of personal data of children and teenagers is in compliance with COPPA. Businesses must receive affirmative, opt-in consent from consumers under 16 (or their parent or guardian, where the consumer is under 13) to: • Sell their personal data;

[26] On November 27, 2023, the California Privacy Protection Agency released draft automated decision making technology ("ADMT") regulations that give consumers opt-out rights with respect to business' use of ADMT, which includes profiling. The draft regulations on ADMT also propose requirements for businesses using ADMT for decisions that tend to have significant impacts on consumers' lives (e.g., employment). *See* A New Landmark for Consumer Control Over Their Personal Information: CPPA Proposes Regulatory Framework for Automated Decision Making Technology, CALIFORNIA PRIVACY PROTECTION AGENCY (Nov. 27, 2023).

Key Requirement	"Highest Standard" in 2024
states have varying requirements when it comes to teenagers' personal data. California was first to set the standard for the maximum age necessitating receipt of opt-in consent by a business for data sales at 16 years old.[27] However, privacy laws such as the one in Connecticut goes beyond California's by requiring opt-in consent for not only the sale of personal data, but also for targeted advertising.[28] In addition, certain privacy laws such as Colorado's requires parent or guardian consent to process sensitive personal data of a consumer under 13.[29]	• To process their personal data for targeted advertising; and • To process their sensitive personal data (if under 13). Most state privacy laws do not set forth standards for how businesses may receive and verify parental consent. However, Virginia's privacy law specifies that businesses that comply with verifiable parental consent requirements under COPPA will be compliant with Virginia's privacy law requirements.[30]
Opt-In for Sensitive Personal Data Processing[31] "Opt-in" consent requires consumers to take affirmative action before a business can collect or use their personal data. The opt-in mechanism is generally considered the most secure method of obtaining user consent, as it ensures that users have voluntarily agreed to a particular data processing activity. Opt-in consent is typically obtained by requiring users to check an empty "I Agree" checkbox or button. While some states like California, Florida, and Utah require a covered business to provide an opportunity for consumers to opt *out* of processing sensitive personal data, others such as Colorado, Connecticut, Montana, Texas, and Virginia require a covered business to provide consumers with clear notice and receive consumer opt-in consent to process sensitive personal data.	Businesses must receive opt-in consent in order to process a consumer's sensitive personal data. Valid opt-in consent requires the following characteristics:[32] • Clear affirmative action, conduct, or statements indicating acceptance; • Freely given, meaning it can be refused or revoked at any time without penalty; • Specific, and uncoupled from consents for unrelated purposes; • Informed, meaning that the consumer was provided a clear notice regarding the requested consent and the processing; and • Unambiguous, and not obtained through a "dark pattern" (i.e., an interface that impairs user autonomy, decision-making, or choice). Various states such as Colorado, Connecticut, Texas, Montana, and Oregon, identify some or all of the following methods as **insufficient** for obtaining a consumer's opt-in consent: • Inaction; • Acceptance of general or broad terms containing descriptions of data processing and other unrelated terms; • Hovering over, muting, pausing, or closing a piece of content; • Agreement obtained through dark patterns.

[27] *See* Cal. Civ. Code § 1798.120(c).
[28] *See* Conn. Gen. Stat. § 42-522 6(a)(7).
[29] *See* Colorado SB 21-190 § 6-1-1308(7).
[30] *See* Va. Code § 59.1-576(D).
[31] To read more about sensitive personal data processing under US state privacy laws, *see* Zachary S. *Schapiro, Update: Processing Sensitive Personal Information under U.S. State Privacy Laws, THE NATIONAL LAW REVIEW (Sept.* 12, 2023).
[32] *See, e.g.,* 4 Colo. Code Regs. § 904-3-7.03.

Key Requirement	"Highest Standard" in 2024
	If a consumer withdraws their consent, Colorado requires businesses to either delete sensitive personal data or permanently anonymize it.[33]

Data Protection Impact Assessment
 	
Data Protection Impact Assessments ("DPIAs"), sometimes called privacy impact assessments and/or data protection assessments, are internal documents detailing the business' data collection and processing activities to help businesses analyze, identify, and minimize data protection risks. Conducting a DPIA involves evaluating potential risks to consumers' privacy posed by a business' activities and implementing measures to mitigate such risks.
 	
California and Utah do not require covered businesses to conduct a DPIA.[34] Others (including Virginia, Colorado, Connecticut, Florida, Oregon, Texas, and Montana) do require covered businesses to conduct DPIAs where the business engages in data processing activities that could result in heightened privacy risks to consumers.
	Businesses must conduct a DPIA prior to engaging in the following types of personal data processing that present a heightened risk of harm to a consumer:[35]
	• Processing of sensitive personal data;
	• Processing personal data for purposes of targeted advertising or profiling;
	• Processing personal data for purposes of profiling where this presents a reasonably foreseeable risk of:
	  ○ Injury to the consumer;
	  ○ Unfair or deceptive or unlawful disparate impact on consumers,
	  ○ Intrusion upon the seclusion of consumers;
	  ○ Other financial, reputational, or physical harms.
	• Selling personal data; and
	• Any other processing activity that may present a heightened risk of harm to consumers.

Data Processing Agreements with Third Parties
 	
A Data Processing Agreement ("DPA") is a contract between a business and a third-party that processes personal data collected by the business on behalf of the business.
 	
Most states with consumer data privacy laws require businesses to enter into binding DPAs that set forth the parties' obligations when a business engages with a third party to process personal
	When engaging a third party to process personal data on behalf of a business, the business must enter into a binding DPA with such third party which specifies:[36]
	• The business' explicit processing instructions;
	• The nature and purpose of the processing;
	• The types of personal data to be processed;
	• The duration of the processing;
	• A description of the rights and obligations of both parties; and
	• Requirements that the third party:
	  ○ Complies with applicable privacy regulations;
	  ○ Keeps all personal data confidential;

[33] *See,* 4 Colo. Code Regs. § 904-3-7.07(E)(1).
[34] California's privacy laws do not currently require DPIAs. However, the California Privacy Protection Agency is authorized to establish regulations requiring businesses whose personal information processing presents a significant risk to consumers' privacy or security to regularly submit risk assessments to the agency.
[35] *See, e.g.,* Oregon SB 619-B § 8(1)(a) and (b).
[36] *See, e.g.*, Va. Code Ann. § 59.1-579(B); *see also* Oregon SB 619-B § 6(1) and (2); *see also* Cal. Civ. Code § 1798.100(d), 1798.140(j), (ag) and Cal. Code Regs. Tit. 11, § 7051.

Key Requirement	"Highest Standard" in 2024
data on behalf of the business. Moreover, many mandate specific provisions, as set forth in the adjacent column.	○ Limits the use of personal data to that explicitly identified in the DPA; ○ Returns or destroys all personal data when the services end or at the business' direction; ○ Makes available all information necessary to demonstrate compliance with its data protection obligations; ○ Allows the business to conduct reasonable assessments or arrange for annual independent audits of the third party's data protection policies and support measures; ○ Only engages a subcontractor under a written contract that requires such subcontractor to meet the third party's data protection obligations; ○ Provides the business the opportunity to object before the third party engages with any subcontractor and stop and remediate any unauthorized use of personal data; ○ Assists the business with the business' privacy obligations; and ○ Notifies the business if the third party can no longer meet its data privacy obligations.
Consumer Rights Recognition Various consumer data privacy laws grant consumers certain rights over their personal data. These typically include rights to access, correction, deletion, and portability. However, some states also grant consumers additional rights. Most states grant consumers most (if not all) of the rights set forth in the adjacent column.	Businesses must recognize and comply with the following consumer rights: • Know and access; • Deletion; • Data portability; • Correction; • Opt-out of: ○ Processing; ○ Personal data sales; ○ Sharing personal data for cross context behavioral or targeted advertising; ○ Sharing personal data for the purposes of profiling in furtherance of solely automated decisions that produce legal or similarly significant effects concerning the consumer; and ○ The use of automated decision making. • Opt-in to sensitive personal data processing; and • Nondiscrimination for exercising a consumer's enumerated data privacy rights.

III. U.S. State Privacy Laws in Effect for 2024

State	Privacy Law	Effective	Applicability	Penalties
Currently Active U.S. State Consumer Data Privacy Laws				
Nevada (NV)[37]	Nevada Privacy of Information Collected on the Internet from Consumers Act, as amended by SB-260	Oct. 1, 2019 (NPICICA) Oct. 1, 2021 (SB-260)	• Data brokers; and Commercial internet website or online service operators that collect or maintain covered information on NV consumers.	Up to $5,000 per violation.
California (CA)	California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020	Jan. 1, 2020 (CCPA) Jan. 1, 2023 (CPRA)	Business that collect the personal information of CA consumers or households that meet one of the following: • Annual gross revenues exceeding $25,000,000; • Annually buys, sells, or shares personal information of 100,000+ CA consumers/households; or • Derives 50% or more of revenues from selling or sharing personal information.	Up to $2,500 for each violation and $7,500 for each intentional violation. Automatic $7,000 fine for violations involving minors. Statutory damages from $100 to $750 per violation.
Virginia (VA)	Virginia Consumer Data Protection Act	Jan. 1, 2023	Persons or entities that conduct business in VA or target VA residents that process/control the personal data of either: • 100,000+ VA consumers; or 25,000+ VA consumers and derive greater than 50% of revenues from personal data sales.	Up to $7,500 per violation and reasonable expenses, including attorney's fees.
Colorado (CO)	Colorado Privacy Act	Jul. 1, 2023	Businesses that conduct business in CO or target CO residents that control/process personal data of either: • 100,000+ CO consumers; or • 25,000+ CO consumers and derive revenues from selling personal data.	Up to $20,000 per violation. Increased to $50,000 for violations involving an elderly person.

[37] Nevada's privacy law is limited in scope to data processing on websites or other online pages and provides consumers with fewer rights than other state data privacy laws.

State	Privacy Law	Effective	Applicability	Penalties
Connecticut (CT)	Connecticut Personal Data Privacy and Online Monitoring Act	Jul. 1, 2023	Businesses that conduct business in CT or target CT residents that control/process personal data of either: • 100,000+ CT consumers; or • 25,000+ CT consumers and derives greater than 25% of revenues from personal data sales.	Injunction, restitution, and attorneys' fees for initial violations. $5,000 per violation for willful violations.

Utah (UT)	Utah Consumer Privacy Act	Dec. 31, 2023	Business that satisfy all conditions:
			• Conduct business in UT or target UT residents;
			• $25,000,000+ in annual revenues; and
			• Control or process the personal data of:
			  ○ 100,000+ UT consumers; or
			  ○ 25,000+ UT consumers and derives greater than 50% of revenues from personal data sales.
				Actual damages to the consumer or up to $7,500 per violation.

U.S. State Consumer Data Privacy Laws Coming into Effect in 2024				

Florida (FL)	Florida Digital Bill of Rights	Jul. 1, 2024	Businesses that conduct business in FL or target FL residents and:
			• Collect personal data about FL consumers and (directly or indirectly) determine the processing purpose and means;
			• Exceed $1,000,000,000 in gross global annual revenues; and
			• Meet one of the following thresholds:
			  ○ Derives 50% or more of global revenues from the sale of ads online;
			  ○ Operates a consumer smart speaker and voice command component service with an integrated virtual assistant connected to a cloud computing service that uses hands-free verbal activation; or
			  ○ Operates an app store or a digital distribution platform that offers at least 250,000 different apps.
				$50,000 per violation, with treble damages available for:
				• Committing a violation involving a known child, including willfully disregarding the age of a minor consumer;
				• Failing to delete or correct upon consumer or controller request; or
				• Continuing to sell or share personal data after consumer opts-out.

State	Privacy Law	Effective	Applicability	Penalties
Oregon (OR)	Oregon Consumer Privacy Act	Jul. 1, 2024	Persons and entities conducting business in OR or targeting OR residents that control/process the personal data of either: ● 100,000+ OR residents (excl. data processed solely for payment transactions); or ● 25,000+ OR residents and derive greater than 25% of revenues from personal data sales.	Up to $7,500 per violation. Other equitable relief may be available, as determined by the court.
Texas (TX)	Texas Data Privacy and Security Act	Jul. 1, 2024	Persons or entities that meet all of the following conditions: ● Conduct business in TX or produce goods/services used by TX residents; ● Process or sell personal data; and ● Do not qualify as a small business under the Small Business Administration's size standards.	Up to $7,500 per violation.
Montana (MT)	Montana Consumer Data Privacy Act	Oct. 1, 2024	Businesses that conduct business in MT or target MT residents that control/process the personal data of either: • 50,000+ MT consumers (excl. data processed solely for payment transactions); or 25,000+ MT consumers and derive greater than 25% of revenues from personal data sales.	$10,000 per willful violation. Additional penalties of up to $10,000 for violations against an elderly or developmentally disabled person.[38]

[38] Subject to change. The MCDPA does not directly set a fine or penalty amount for violations. However, Section 13 of the MCDPA expresses the legislature's intent to codify the MCDPA as an integral part of Montana's Unfair Trade Practices and Consumer Protection law, and for the provisions of that law to apply to the MCDPA. Therefore, it is likely that the penalties for MCDPA violations will be those imposed for unfair trade practices under Montana's Unfair Trade Practices and Consumer Protection law, listed here.