4A's State Data Privacy Laws Comparison

	Virginia Consumer Data Protection Act ("VCDPA") [Link] [Amendment- H.B. 381] [Amendment- S. 534]	California Consumer Privacy Act ("CCPA") [Link]	California Privacy Rights Act ("CPRA") [Link]	Colorado Privacy Act ("CPA") [Link]	Connecticut Data Privacy Act ("CTDPA") [Link]
Key Dates	**Operative:** Jan. 1, 2023	**Operative:** Jan. 1, 2020 **Enforcement:** July 1, 2020	**Effective:** Dec. 16, 2020 Most provisions not operative until Jan. 1, 2023, excluding regulations provisions and those establishing California Privacy Protection Agency **Enforcement:** July 1, 2023 **Final Regulations 1:** Finalized 3/29/23 [Link]	**Effective:** July 1, 2023 **Cure Sunset Date:** Jan. 1, 2025 **AG Rule Promulgation Deadline:** Jan. 1, 2025 (begin) **Universal Opt-out Mechanism:** Before July 1, 2023 **Final Regulations:** Finalized March 2023 [Link]	**Effective:** July 1, 2023 **Cure Sunset Date:** Jan. 1, 2025 **Universal Opt-out Mechanism:** Jan. 1, 2025
Covered Entities and Exceptions	Applies to persons that conduct business in Virginia or produce products or services that are targeted to Virginia residents and that: -Control or process personal data of at least 100,000 consumers annually -Control or process personal data of at least 25,000 consumers and derive at least 50% of gross revenue from the sale of personal data. Exemptions: Does not apply to state government entities, non-profits, higher ed institutions, financial institutions, or businesses subject to HIPPA. There are 14 categories of exempt information and data, including protected health information under HIPPA, and other health-related information, data regulated by the Family Educational Rights and Privacy Act, the Fair Credit Reporting Act, and others. VCDPA does not apply to individuals "acting in a commercial or employment context"—meaning employee and business-to-business data appear to fall outside the law's scope. Classifies political organizations and certain 501(c)(4) organizations as "nonprofit organizations," and thus, exempt them from the VCDPA.	Applies to for-profit entities doing business in California that collects or processes consumers' personal information and meets one or more of these thresholds: -Annual gross revenues in >$25,000,000 -Annually buys, receives, sells, or shares the personal information of ≥50,000 consumers, households or devices -Derives ≥50% of its annual revenues from selling consumers' personal information. Exemptions: Businesses can collect, use, retain, sell, or disclose deidentified or aggregate consumer information. Businesses can collect, sell, or share personal information if every aspect of that commercial conduct takes place wholly outside of California.	Applies to for-profit entities doing business in California that collects or processes consumers' personal information and meets one or more of these thresholds: -Annual gross revenues in >$25,000,000 in the preceding calendar year. -Annually buys, receives, sells, or shares the personal information of ≥100,000 consumers or households. -Derives ≥50% of its annual revenues from selling or sharing consumers' personal information. Exceptions: Businesses can collect, use, retain, sell, share, or disclose deidentified or aggregate consumer information. Businesses can collect, sell, or share personal information if every aspect of that commercial conduct takes place wholly outside of California.	Applies to a controller that conducts business in Colorado or produces or delivers commercial products or services that are intentionally targeted to residents of Colorado; and -Controls or process the personal data of ≥100,000 consumers or households -Derives ≥50% of its annual revenues from selling or sharing consumers' personal information. Exceptions: Does not apply to financial institutions or affiliates subject to the Gramm-Leach-Billey Act. It does not apply to various other types of data including health care information, certain activities undertaken by a consumer reporting agency, data regulated by COPPA, data maintained for employment purposes, data maintained by higher education institutions, etc.	Applies to entities that: Conduct business in Connecticut or produce products or services targeted to Connecticut residents and that during the preceding calendar year, either: -Controlled or processed the personal data of at least 100,000 consumers, excluding personal data controlled or processed solely for the purpose of completing payment transactions. -Controlled or processed the personal data of at least 25,000 consumers and derived over 25% of their gross revenue from the sale of personal data. Exemptions: The law also exempts certain types of entities and data from its requirements including six types of entities, irrespective of whether the data collected and processed would otherwise be subject to the law, are exempt from the law including state and local governments, Nonprofits, Higher education institutions, national securities associations registered under the Securities Exchange Act of 1934, financial institutions and data subject to the Gramm-Leach-Bliley Act, and covered entities and business associates as defined by the Health Insurance Portability and Accountability Act. The law contains 16 categories of exempted data, including specific information regulated by HIPAA, the Fair Credit Reporting Act, the Driver's Privacy Protection Act, the Family Educational Rights and Privacy Act, the Farm Credit Act, and the Airline Deregulation Act. Specific employee and job applicant data are also exempt. Excludes any deidentified data or publicly available information. "Publicly available information" means "information that (A) is lawfully made available through … government records or widely distributed media, and (B) a controller has a reasonable basis to believe a consumer has lawfully made available to the general public."
Notice	In a privacy policy on businesses' website	At or before point of data collection; in a privacy policy. CCPA expressly requires businesses to include the use of cookies/pixels and other tracking technology in its notice to consumers	At or before point of data collection; in a privacy policy	In a privacy policy on businesses' website	In a privacy policy on a business' website. Clear and conspicious link to a webpage for opting out of sale or targeted advertising.
Targeting Advertising and Key Definitions	"Targeted advertising" means displaying advertisements to a consumer where the advertisement is selected based on personal data obtained from that consumer's activities over time and across nonaffiliated websites or online applications to predict such consumer's preferences or interests. Definition excludes ads based on a consumer's activities within the controller's own websites and apps, as well as (1) ads based on activities on the controller's affiliated websites; (2) ads based on the context of a consumer's search query or visit to a website or app; (3) ads displayed in response to a request for information or feedback; and (4) the processing of personal data solely for measuring or reporting ad performance, frequency, or reach. Personal information definition excludes any deidentified data or publicly available information. Personal information concerning employees and B2B contacts are also excluded. "Sale" is limited to an exchange of personal information for monetary consideration only.	"Personal information collected for commercial purposes." "Commercial purposes" means to advance a person's commercial or economic interests, such as by inducing another person to buy, rent, lease, join, subscribe to, provide, or exchange products, goods, property, information, or services, or enabling or effecting, directly or indirectly, a commercial transaction. "Commercial purposes" do not include for the purpose of engaging in speech that state or federal courts have recognized as noncommercial speech, including political speech and journalism.	"Cross-context behavioral advertising" means the targeting of advertising to a consumer based on the consumer's personal information obtained from the consumer's activity across businesses, distinctly branded websites, applications, or services, other than the business, distinctly-branded website, application, or service with which the consumer intentionally interacts. Personal information definition excludes deidentified data or publicly available information. Personal information concerning employees and B2B contacts are NOT excluded.	Includes advertising based on data "inferred" from consumers' online activity across non-affiliated websites and not just personal data "obtained" from such activity. Therefore, any advertising targeted to consumers based on profiles developed from consumers' online activity—even if not based on the actual data itself—would be "targeted advertising" under the Colorado law. "Targeted Advertising" means displaying to a consumer and advertisement that is selected based on personal data obtained or inferred over time from the consumer's activities across non-affiliated websites, applications, or online services to predict consumer preferences or interests . The law defines the "sale of personal data" as "the exchange of personal data for monetary or other valuable consideration by the controller to a third party." Personal information definition excludes any deidentified data or publicly available information. Personal information concerning employees and B2B contacts are also excluded.	"Targeted advertising" means displaying advertisements to a consumer where the advertisement is selected based on personal data obtained or inferred from that consumer's activities over time and across nonaffiliated Internet web sites or online applications to predict such consumer's preferences or interests. "Targeted advertising" does not include (A) advertisements based on activities within a controller's own Internet web sites or online applications, (B) advertisements based on the context of a consumer's current search query, visit to an Internet web site or online application, (C) advertisements directed to a consumer in response to the consumer's request for information or feedback, or (D) processing personal data solely to measure or report advertising frequency, performance or reach. The law defines the "sale of personal data" as "the exchange of personal data for monetary or other valuable consideration by the controller to a third party." Personal information definition excludes any deidentified data or publicly available information. Personal information concerning employees and B2B contacts are also excluded.
Consumer Rights	**Right to Know** whether a controller is processing the consumer's personal data. **Right to Acces**s personal data processed by a controller (45 days) **Right to Correct** **Right to Delete**; allows consumer to request deletion of all personal data collected about the consumer **Right to Data Portability** **Right to Opt Out** of targeted advertising, the sale of personal data or profiling **Right to Non-discrimination**	**Right to Know**: what personal info is collected **Right to Access**: Accessibility to all personal information (45 days) **Right to Know** if Personal Information is Sold **Right to Delete:** subject to certain exceptions **Right to Data Portability** **Right to Opt Out** of Sale	**Right to Know:** What information is being collected **Right to Access:** Personal Information (45 days) **Right to Know** what Personal information is sold or shared and to Whom **Right to Correct** **Right to Delete; limited to data that the consumer has provided to the controller, not all data.** **Right to Data Portability** **Right to Opt Out** of Sale or Sharing: Includes "cross-context behavioral advertising" a separately defined term **Right to Non-Discrimination** Note: CPRA generally expands or modifies existing CCPA rights	**Right to Access:** Access to confirm whether a controller is processing personal data concerning the consumer and to access such data (45 days) **Right to Correction** **Right to Data Portability** (twice a year) **Right to Revokation of Consent** of data processing [Rulemaking] **Right to Delete:** Allows consumer to request deletion of all personal data collected about the consumer **Right to Opt Out** of targeted advertising, the sale of personal data, or profiling Opt-out requests need not to be authenticated (per rulemaking).	**Right to Know** whether a controller is processing the consumer's personal data. **Right to Access** personal data processed by a controller (45 days) **Right to Correction** **Right to Delete:** Allows consumer to request deletion of all personal data collected about the consumer **Right to Data Portability** **Right to Revokation of Consent of data processing** **Right to opt out** of targeted advertising, the sale of personal data or profiling
Appeals Process	Yes, within 60 days	No	No	Yes, 45 days to respond	Yes, within 60 days
Data Protection Assessments (DPA)	Yes. Writing DPAs required for each of the following processing activities involving personal data including: 1) Targeted advertising 2) Sale of personal data 3) Profiling in certain circumstances 4) Sensitive data 5) Processing activities that present a heightened risk of harm. AG may request and evaluate a DPA for compliance.	See CPRA.	Yes. Provides for regulations requiring businesses whose processing of consumers' information presents significant risk to consumers' privacy or security to: 1) Perform annual cybersecurity audit 2) Submit risk assessment for processing information to the CPPA, including whether the processing involves sensitive personal information, and identifying and weighing the benefits resulting from the processing against the potential risks, with the goal of restricting or prohibiting the processing if the privacy risks to the consumer outweigh the benefits of processing for the consumer, business, and the public.	Yes. DPAs are required when conducting processing activities that present a heightened risk of harm. This heightened risk of hard includes: 1) Targeted advertising where profiling presents a risk of A) unfair or deceptive treatment, or unlawful or disparate impact on consumers; B) Financial or physical injury; C) Other substantial injury. 2) Selling personal information 3) Processing sensitive data DPAs must be made available to AG upon request. AG can then evaluate DPA for compliance. There is a three-year retention requirement for DPAs.	Yes. DPAs are required for each of the following processing activities involving personal data including: 1) Processing data for the purposes of targeted advertising. 2) Selling personal data. 3) Processing personal data for the purposes of profiling, where such profiling presents a reasonably foreseeable risk of substantial injury to consumers. 4) Processing sensitive data. AG may request and evaluate a DPA for compliance.
Enforcement	AG General Investigative and Enforcement Authority. Virginia JCOTS Consumer Data Protection Act Workgroup is developing recommendations for clean-up bill and enforcement.	AG General Enforcement.	AG Enforcement Administrative Enforcement (California Privacy Protection Agency) Enforcement	AG Enforcement and District Attorneys Enforcement	AG General Investigative and Enforcement Authority.
Private Right of Action	No	Yes, but limited to certain types of data breaches. California consumers can initiate a private right of action when their "nonencrypted and nonredacted personal information" is "subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures."[4] This private right of action includes the availability of statutory damages and is unlike most data breach and privacy laws, which require proof of actual harm and do not allow for statutory damages.	See CCPA	No	No
Cure Period	Yes. 30 Days after notice from AG.	Yes. 30 Days to cure alleged non-compliance. Businesses can seek guidance from AG on compliance.	Yes. 30 days to cure alleged non-compliance.	Yes. 60 days to cure alleged violation prior to Jan. 1, 2025. Cure period sunsets on Jan. 1, 2025	Yes. 60 days to cure alleged violation. Sunsets on Jan. 1, 2025.

4A's State Data Privacy Laws Comparison

	Virginia Consumer Data Protection Act ("CDPA") [Link] [Amendment: H.B. 381] [Amendment: S. 534]	California Consumer Privacy Act ("CCPA") [Link]	California Privacy Rights Act ("CPRA") [Link]	Colorado Privacy Act ("CPA") [Link]	Connecticut Data Privacy Act ("CTDPA") [Link]
Penalties	Up to $7,500 per violation; AG may recover reasonable expenses incurred including attorney fees.	$7,500 per intentional violation; <$2,500 per unintentional violation to be recovered in a civil action brought by AG. For PRA, consumers may recover injunctive or declaratory relief and damages in an amount >$100 to $750 per consumer per incident or actual damages, whichever is greater.	<$2,500 per unintentional violation or $7,500 per intentional violation or violations involving minor consumers to be assessed and recovered in a civil action brought by AG. <$2,500 per unintentional violation or $7,500 per intentional violation or violations involving the personal information of consumers, the business, service provider, contractors, or other persons under 16 years of age in an enforcement action brought by CPPA.	Violations of CPA constitute deceptive trade practices and therefore are subject to a $20,000 per violation fine pursuant to the Colorado Consumer Protection Act.	Violations of the CTDPA will constitute an unfair trade practice, which carries civil penalties of up to $5,000 per willful violation.
Opt-in vs. Opt-out	Right to opt out for targeted advertising, sales, and profiling for legal or similarly significant effects. Opt-in consent for the collection or processing of certain sensitive categories of personal data, such as racial origin or citizenship status, and geolocation data.	Right to opt-out of selling personal data only; must include opt-out link on website. Explicit definition of sensitive personal data was not included in the CCPA.	Right to opt-out of the sale and sharing of their personal information; businesses must include opt-out link on website; CPRA does not require opt-out requests to be verified. In other words, a California resident will not have to prove their identity to opt out of the sale of their personal data, for targeted advertising, or for certain types of profiling. Opt-in for minors under 16. Parental opt-in for minors under 13. Personal information is data that reveals a customer's government-issued identification number, financial account information and account login credentials, precise geolocation information, the contents of an email or text messages, genetic data, racial or ethnic origin, religious beliefs, biometrics data, health data, and data concerning sex life or sexual orientation; or Is used for the purpose of inferring characteristics about a consumer.	Right to opt-out of processing of personal data concerning the consumer for purposes of targeted advertising, the sale of personal data, or profiling. Opt-in for processing of sensitive data. Colorado does not treat precise geolocation data as "sensitive" data. The CPA does not recognize the validity of consent obtained through dark patterns. Opt out requests need not to be authenticated (via rulemaking).	Right to opt-out of processing of personal data concerning the consumer for purposes of targeted advertising and the sale of personal data. Opt-in for processing of sensitive data or profiling in furtherance of solely automated decisions that produce legal or similarly significant effects concerning the consumer. The CT bill also does not require opt-out requests to be verified. A CT resident will not have to prove their identity to opt out of the sale of their personal data, for targeted advertising, or for certain types of profiling. Opt-in for targeted advertising or sale of PI of children ages 13-17.
Universal Opt Out Mechanisms	No	See CPRA.	Yes. UOOM signals must be recognized. CPRA requires that an opt-out signal not be the default setting (i.e. a consumer must instead be required to affirmatively select the opt-out option) in order for it to be covered under the law.	Yes. Law requires the Attorney General to establish technical specifications for a universal targeted advertising and sale opt-out (e.g., global privacy control) by July 1, 2023, which controllers must honor starting July 1, 2024. Technical specifications for applicable universal opt-out mechanisms are spelled out in the CPA regulations. Colorado Department of Law will maintain a public list of opt-out mechanisms that satisfy those specifications, and will update it regularly. Requires that an opt-out signal not be the default setting (i.e. a consumer must instead be required to affirmatively select the opt-out option) in order for it to be covered under the law.	Yes. Beginning Jan. 1, 2025, controllers must recognize universal "opt-out preference signal[s]" indicating a consumer's intent to opt out of targeted advertising and sales, which will trump any conflicting controller-specific privacy setting. Requires that an opt-out signal not be the default setting (i.e. a consumer must instead be required to affirmatively select the opt-out option) in order for it to be covered under the law. Opt out requests need not be authenticated since the harms associated with an unauthenticated access request, for example, do not apply to a request that opts a consumer out of targeted advertising, sales, or profiling.
Portability	Yes; Right to portability is limited to personal data that the controller receives from the consumer.	Yes	Yes	Yes; Right to portability is not limited to personal data that the controller receives from the consumer. Consumers have the right to receive in a portable format any personal data that the controller has collected about the consumer. Right to portability limited to twice per year.	Yes; Consumers have the right to "obtain a copy of the consumer's personal data processed by the controller, in a portable and, to the extent technically feasible, readily usable format that allows the consumer to transmit the data to another controller without hindrance, where the processing is carried out by automated means, provided such controller shall not be required to reveal any trade secret."
Processor Compliance and Contractual Requirements	Processors are required to follow a controller's instructions and assist the controller in meeting its obligations. VCDPA requires controllers to establish a contractual relationship with their processors. The contract must provide not only instructions for processing the data but also a description of the nature and purpose of processing, the type of data to be processed, the duration of processing, and the rights and obligations of both parties. It is important that the controller and the processor share expectations and develop a common view of the relevant processing. Controllers and processors must comply with the verifiable parental consent requirements of the Children's Online Privacy Protection Act (15 U.S.C. § 6501 et seq.) and shall be deemed compliant with any obligation to obtain parental consent. Additional processor requirements to be addressed in the contract include: -Ensuring that each person processing personal data is subject to a duty of confidentiality with respect to the data; -Deleting or returning all personal data to the controller at the end of the contract; -Demonstrating compliance with all CDPA and contractual requirements; -Allowing, and cooperating with, reasonable audits, assessments, and other reviews by the controller or designated assessor; -Engaging subcontracted processors only through written contracts that require the subcontractor to meet the same standards as the processor with respect to the personal data; and -Committing not to attempt re-identification of any de-identified data, and taking reasonable measures to prevent such re-identification.	Does not include designation of "controllers" or "processors". Instead places obligations on "businesses", "service providers" and "third parties "Service Provider" includes requirement that there be a contract that prohibits the service provider from using the personal information for any purpose other than for the specific contractual purpose or using the personal information for a different commercial purpose. "Third Party" is defined in the negative as a person who is not a business that collects personal information or subject to service-provider type contractual requirements, including those that prohibit the person from: 1. Selling or sharing personal information 2. Using personal information for any purpose other than for the business purpose specified in the contract. 3. Using personal information outside the direct business relationship. 4. Combining the personal information with other personal information, subject to certain exceptions.	Does not include designation of "controllers" or "processors". Instead places obligations on "businesses", "service providers" and "third parties. Contractual Requirements: A business that collects a consumer's personal information and sells it to or share it with a third party or discloses it to a service provider or contractor for a business purpose is required to enter into an agreement with the third party, service provider or contractor that includes specific terms. "Service Provider" includes requirement that there be a contract that prohibits the service provider from using the personal information for any purpose other than for the specific contractual purpose or using the personal information for a different commercial purpose. "Third Party" is defined in the negative as a person who is not a business that collects personal information or subject to service-provider type contractual requirements. Contractors and Service Providers must enter into contract that prohibit: 1. Selling the personal information. 2. Using the personal information for any purpose other than specified in the contract. 3. Using the information outside of the business relationship. 4. Combining the personal information with other personal information, subject to certain exceptions. 5. For contractors, includes a certification it understands the restrictions. 6. Permits a business to monitor for compliance. A business that discloses personal information to a service provider shall not be liable under this title if the service provider receiving the personal information uses it in violation of the restrictions set forth in the title, provided that, at the time of disclosing the personal information, the business does not have actual knowledge, or reason to believe, that the service provider intends to commit such a violation. A service provider shall likewise not be liable under this title for the obligations of a business for which it provides services as set forth in this title.	Processors are required to adhere to the instructions of the controller and assist the controller in meeting its obligations by: 1. Taking appropriate measures to assist in consumer requests to exercise their rights. 2. Helping meet the controller's security obligations for breach notification and system security 3. Providing information to the controller necessary to enable the controller necessary to enable the controller to conduct and document any data protection assessments required. Additionally, processing by a processor must be governed by a binding contract between the processor and the controller that sets out: 1. Instructions, including the nature and purpose of the processing, to which the processor is bound. 2. The duration of processing and the type of personal data subject to the processing. 3. The requirement that each person processing the personal data is subject to a duty of confidentiality with respect to the data. 4. The requirement that a contractor may only use a subcontractor pursuant to a contract requiring the subcontractor to meet the processor's obligations with respect to the data. The processor must also provide the controller with an opportunity to object. 5. The allocation of responsibility between the controller and the processor for maintaining technical and organization measures to ensure appropriate security. 6. Whether the controller requires the processor to return or delete all personal data to the controller at the end of the provision of services, unless that retention. 7.That the processor share make all information necessary to demonstrate compliance with this law available to the controller. 8. The processor shall allow for, and contribute to, reasonable audits and inspections by controller or auditor.. Controllers must provide an effective means by which a consumer may revoke consent for the processing of personal data (bestowed via rulemaking).	The CTDPA places affirmative obligations on Processors, such as those related to compliance with a Controller's instructions and the implementation of security controls to safeguard personal data from unauthorized use. It requires Controllers and Processors to execute written agreements that contain certain data protection clauses, which must address, among other things, the nature and purpose of data processing, the limited manner in which the Processor can use the personal data, confidentiality, and compliance assessments. The CTDPA also requires these Controller-to-Processor contracts to include clauses requiring the Processor to, at the end of the data processing services, delete or return the personal data in its custody, unless retention is required by law. In addition, the CTDPA mandates written contracts between Processors and subcontractors that require the subcontractor to meet the Processor's obligations with respect to personal data. Controllers must provide an effective means by which a consumer may revoke consent for the processing of personal data.

4A's State Data Privacy Laws Comparison

	Indiana Consumer Data Protection Act ("INCDPA") [Link]	Iowa Data Privacy Act ("IDPA") [Link]	Montana Privacy Law (SB 384) [Link]	Tennessee Information Protection Act ("TIPA") [Link]	Florida Digital Bill of Rights ("FDBR") [Link]
Key Dates	**Effective:** January 1, 2026 **Cure Sunset Date:** None	**Effective:** January 1, 2025 **Cure Sunset Date:** None	**Effective:** October 1, 2024 **Cure Sunset Date:** April 1, 2026 **Universal Opt-Out Mechanism:** January 1, 2026	**Effective**: July 1, 2025 **Cure Sunset Date:** None	**Effective:** July 1, 2024 **Cure Sunset Date:** None
Covered Entities and Exceptions	Applies to a person that conducts business in Indiana or produces products or services that are targeted to residents of Indiana and that during a calendar year: (1) Controls or processes personal data of at least one hundred thousand (100,000) consumers who are Indiana residents; or (2) Controls or processes personal data of at least twenty-five thousand (25,000) consumers who are Indiana residents and derive more than fifty percent (50%) of gross revenue from the sale of personal data SB 5's protections would apply to residents of Indiana who act for a personal, family or household purpose, with express exemption for individuals acting in a commercial or employment context. The bill also contains a number of exemptions, including exceptions for financial institutions, affiliates, and data subject to Title V of the Gramm-Leach-Bliley Act, covered entities and business associates under the Health Insurance Portability and Accountability Act of 1996, nonprofit organizations and institutions of higher education.	Controllers and processors who "conduct business in" Iowa or that "produce products or services that are targeted to residents" (Sec. 2(1)) Must exceed small business exceptions by satisfying 1 of 2 thresholds: - Control or process the personal data of at least 100,000 consumers - Derive over 50% of the entity's gross revenue from the sale of personal data and controlling or processing personal data of at least 25,000 consumers (Sec. 2(1)) Exceptions: The law exempts certain types of data and entities, including publicly available data, de-identified data, and data subject to the Health Insurance Portability and Accountability Act, the Driver's Privacy Protection Act, and the Family Education Rights and Privacy Act. The SF 262 also includes broad entity-based exemptions for entities and businesses covered by the Fair Credit Reporting Act and the Gramm-Leach-Bliley Act, as well as non-profit entities, higher education institutions, tribes, and government bodies.	Applies to controllers that: -Produce products or services targeted to Montana residents and that process or control the personal data of 50,000 or more Montana residents; or -Derives more than 25% of gross revenue from sale of personal data + control or process personal data of not less than 25,000 consumers. Exceptions: The law exempts certain types of data and entities, including publicly available data, de-identified data, and data subject to the Health Insurance Portability and Accountability Act, the Driver's Privacy Protection Act, and the Family Education Rights and Privacy Act. The law also includes broad entity-based exemptions for entities and businesses covered by the Fair Credit Reporting Act and the Gramm-Leach-Bliley Act, as well as non-profit entities, higher education institutions, tribes, and government bodies.	Applies to people conducting business in Tennessee or producing products or services that are targeted to residents of Tennessee and that either: -Control or process personal information of at least 100,000 consumers during a calendar year; or -Control or process personal information of at least 25,000 consumers and derive more than 50 percent of their gross revenue from the sale of personal information. Contains exemptions for governmental entities, financial institutions governed by the Gramm-Leach-Bliley Act, businesses subject to the federal Health Insurance Portability and Privacy Act (HIPAA), nonprofit organizations, and institutions of higher education. The TIPA also exempts certain types of data, such as protected health information under HIPAA, personal information regulated by the Family Educational Rights and Privacy Act, and data processed or maintained in the course of employment. The TIPA also exempts the use of personal information for certain specific purposes, such as compliance with law, preventing fraud or injury to others and defending legal claims.	FDBR appllies controllers that gross more than $1 billion a year and 1) make at least 50% of their revenue from the sale of advertisements online; 2) operate an app store or digital distribution platform that offers at least 250,000 different software applications for consumers to download and install; or 3) operate 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. FDBR's provision requiring consumer consent before selling sensitive data or processing the sensitive data of a known child applies to any for-profit entity that conducts business in Florida and collects personal data. A business can be covered by the Act even if it neither does business in Florida nor targets goods and services to residents in Florida. It is sufficient if the business produces a product or service "used by" Florida residents and the business processes or sells personal data. Exceptions exist for financial institutions and data subject to GLBA, covered entities and business associates under HIPAA's privacy and security rules, non-profits, and other specified entities and data. FDBR expressly does not restrict an entity's use of personal information for certain purposes, such as responding to a subpoena, complying with the law, defending against a legal claim, prevention of fraud, harassment, identity theft and other illegal activity, and specified internal purposes. One section sets requirements that all businesses (for profit businesses conducting business in Florida who collect personal data about consumers, without a revenue threshold) must follow. Under Section 501.715, all businesses must obtain prior consent from a consumer before selling that consumer's sensitive data. Further, if a business sells sensitive data, it must include a very specific notice on its website.
Notice	In "a reasonably accessible, clear, and meaningful privacy notice"	In "a reasonably accessible, clear, and meaningful privacy notice." Must provide notice prior to processing a consumer's sensitive data.	In "a reasonably accessible, clear, and meaningful privacy notice."	In a "reasonably accessible, clear and meaningful privacy notice".	In a "reasonably accessible, clear and meaningful privacy notice".
Targeting Advertising and Key Definitions	Targeted advertising is defined as displaying ads that are selected based on the consumer's activities over time and across nonaffiliated websites; Sale of personal data is defined as the exchange of personal data for monetary consideration; Notably, S.B. 5 limits its definition of "profiling" to "solely automated processing." Personal information definition excludes any deidentified data or publicly available information. Personal information concerning employees and B2B contacts are also excluded.	"Targeted advertising" means displaying advertisements to a consumer where the advertisement is selected based on personal data obtained from that consumer's activities over time and across nonaffiliated websites or online applications to predict such consumer's preferences or interests. "Targeted advertising" does not include the following: a. Advertisements based on activities within a controller's own or affiliated websites or online applications. b. Advertisements based on the context of a consumer's current search query, visit to a website, or online application. c. Advertisements directed to a consumer in response to the consumer's request for information or feedback. d. Processing personal data solely for measuring or reporting advertising performance, reach, or frequency. "Sale of personal information" is defined as the exchange of personal data for monetary consideration. Personal information definition excludes any deidentified data or publicly available information. Personal information concerning employees and B2B contacts are also excluded.	Defines the "sale" of personal data as encompassing transfers for both monetary and "other valuable consideration," which means that more activities will fall under the scope of the "sale" of personal data and permit consumers to opt out of those sales. "Personal Data" in the MCDPA is "information that is linked or reasonably linkable to an identified or identifiable individual." Personal information definition excludes any deidentified data or publicly available information. Personal information concerning employees and B2B contacts are also excluded. "Sensitive data" is considered personal data that includes information such as racial/ethnic origin, religious beliefs, mental or physical health diagnosis, information about a person's sex life, sexual orientation, citizenship or immigration status, genetic or biometric information used to uniquely identify an individual, personal data collected from a known child (under the age of 13) and precise geolocation (location within a radius of 1,750 feet). Under the MCDPA, a controller may not process (including collection) sensitive data without obtaining the consumer's consent or, in the case of a child, complying with COPPA. "Targeted advertising" means displaying advertisements to a consumer in which the advertisement is selected based on personal data obtained or inferred from that consumer's activities over time and across nonaffiliated internet websites or online applications to predict the consumer's preferences or interests.	"Personal information" in the TIPA is "information that is linked or reasonably linkable to an identified or identifiable individual." It excludes, however, deidentified data, aggregate data and publicly available data. Personal information concerning employees and B2B contacts are also excluded. "Sale of personal information" means the exchange of personal information for monetary consideration or other valuable consideration by the controller to a third party. "Sensitive data" is considered personal information that includes information such as racial/ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, citizenship or immigration status, genetic or biometric information used to uniquely identify an individual, personal information collected from a known child (under the age of 13) and precise geolocation (location within a radius of 1,750 feet). "Targeted advertising" means displaying to a consumer an advertisement that is selected based on personal information obtained from that consumer's activities over time and across nonaffiliated websites or online applications to predict the consumer's preferences or interests.	"Personal Data" is information that is linked or reasonably linkable to an identified or identifiable individual or a device linked to that individual." Personal information concerning employees and B2B contacts are also excluded. The Act only excludes deidentified or publicly available information from the definition of personal data. De-identified data is data that is not reasonably linkable to an individual or a device linked to that individual. "Sensitive data" means a category of personal data which includes personal data revealing an individual's racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status, Genetic or biometric data processed for the purpose of uniquely identifying an individual. Personal data collected from a known child and precise geolocation data. "Sale" is defined as the sharing, disclosure, or transfer of personal data for "monetary or other valuable consideration."Definition lacks common exceptions, such as transfers as part of a merger or acquisition. "Search engine" is defined as "technology and systems that use algorithms to sift through and index vast third-party websites and content on the Internet in response to search queries entered by a user" but excludes licensees who don't have control over the search algorithm, the index from which results are generated, or the ranking order in which the results are provided. "Substantial harm or privacy risk" to include: mental health disorders; addictive behaviors; physical violence, online bullying and harassment; sexual exploitation; the promotion and marketing or tobacco, gambling, alcohol, or narcotic drugs; and predatory, unfair, or deceptive marketing practices or other financial harms. "Targeted advertising" is defined as displaying advertisements to a consumer based on personal data "obtained from that consumer's activities over time and across affiliated and nonaffiliated websites or online applications to predict the consumer's preferences or interests." Does not exempt first-party data from opt-out rights -meaning information collected from affiliated sites and apps.
Consumer Rights	**Right to Know** whether a controller is processing the consumer's personal data. **Right to Access** personal data processed by a controller (45 days) **Right to Correction** **Right to Delete:** Allows consumer to request deletion of all personal data provided by or about the consumer **Right to Data Portability** **Right to Opt Out** of targeted advertising, the sale of personal data or profiling	**Right to Know:** what personal info is being collected and whether a controller is processing their personal data **Right to Access:** Access the personal data that a controller processes about them **Right to Deletion:** Provides consumers a narrow deletion right that applies only to personal data that the consumer provided to the controller. **Right to Portability:** Ability to obtain a copy of their personal data in a format that is portable, readily usable, and allows the consumer to transmit the data to another controller without impediment; and **Right to Opt Out:** Allows consumer the option to out the sale of personal data. Consumers, in their requests, must specify the right they intend to exercise. Excludes data that is pseudonymized or publicly available.	**Right to Know** whether a controller is processing the consumer's personal data. **Right to Access** personal data processed by a controller (45 days) **Right to Correction** **Right to Delete:** Allows consumer to request deletion of all personal data collected about the consumer **Right to Data Portability** **Right to Revocation of Consen**t of data processing **Right to opt ou**t of targeted advertising, the sale of personal data or profiling Companies do not need to include pseudonymous data (under certain circumstances) when responding to consumer requests under the MCDPA. Opt-out requests need not to be authenticated.	**Right to Know** whether a controller is processing the consumer's personal data. **Right to Access** personal data processed by a controller **Right to Correction** **Right to Delete**: Allows consumer to request deletion of all personal data provided by or about the consumer **Right to Data Portability** **Right to Opt Out** of targeted advertising, the sale of personal data or profiling Excludes data that is pseudonymized or publicly available.	**Right to Know** whether a controller is processing the consumer's personal data. **Right to Access** personal data processed by a controller **Right to Correction** **Right to Delete:** Allows consumer to request deletion of all personal data provided by or about the consumer **Right to Data Portability** **Right to Opt Out** of targeted advertising, the sale of personal data or profiling
Appeals Process	Yes, 60 days to respond	Yes.	Yes, 60 days to respond	Yes. 60 days to respond.	Yes. 60 days to respond.
Data Protection Assessments (DPA)	Yes. Controllers must conduct and document a DPA for each of the following processing activities involving personal data: (1) the processing of personal data for purposes of targeted advertising; (2) the sale of personal data; (3) the processing of personal data for purposes of profiling, if such profiling presents certain reasonably foreseeable risks; (4) the processing of sensitive data; and (5) any processing activities involving personal data that present a heightened risk of harm to consumers.	None	Yes. For processing activities created or generated after January 1, 2025, controllers must comply with data protection assessment requirements. Controllers must conduct and document a DPA for each of the following processing activities involving personal data: (1) the processing of personal data for purposes of targeted advertising; (2) the sale of personal data; (3) the processing of personal data for purposes of profiling, if such profiling presents certain reasonably foreseeable risks; (4) the processing of sensitive data; and (5) any processing activities involving personal data that present a heightened risk of harm to consumers.	Yes. TIPA requires that data protection assessments be conducted for applicable processing activities created or generated on or after July 1, 2024, but there is no requirement to conduct an assessment prior to TIPA's effective date of January 1, 2025. Controllers must conduct and document a DPA for each of the following processing activities involving personal data: (1) the processing of personal data for purposes of targeted advertising; (2) the sale of personal data; (3) the processing of personal data for purposes of profiling, if such profiling presents certain reasonably foreseeable risks; (4) the processing of sensitive data; and (5) any processing activities involving personal data that present a heightened risk of harm to consumers. TIPA allows for the use of impact assessments done under other state laws to count towards the requirements of the TIPA and does not require retroactive impact assessments for processing activities occurring prior to the effective date of the law.	No. However, FDBR places a burden of proof on online platforms to demonstrate that processing personal information does not violate any of the law's prohibitions. Covered platforms may therefore ultimately need to conduct a DPA or similar assessment to meet this burden of proof.
Enforcement	AG Enforcement	AG Enforcement	AG Enforcement	AG Enforcement; Affirmative Defense: In the event of an allegation of violation of TIPA, a controller or processor has an affirmative defense if it creates, maintains, and complies with a written privacy program that conforms to the National Institute of Standards and Technology (NIST) privacy framework entitled "A Tool for Improving Privacy through Enterprise Risk Management Version 1.0" or "other documented policies, standards, and procedures designed to safeguard consumer privacy." If the NIST or a comparable privacy framework publishes a subsequent revision to its privacy framework, a controller or processor shall reasonably conform its privacy program to the revised framework no later than two years after the publication date stated in the subsequent version.	AG Enforcement
Private Right of Action	No	No	No	No	No
Cure Period	Yes. 30 days to cure alleged non-compliance.	Yes.	Yes. 60 days to cure alleged violation. Requires the AG's office to provide a controller with a notice of violation and an opportunity to cure, but only until April 1, 2026, when that right to cure sunsets.	Yes. 60 days to cure alleged violation No cure sunset.	Yes. 45 days to cure alleged violation. No cure sunset.

4A's State Data Privacy Laws Comparison

	Indiana Consumer Data Protection Act ("INCDPA") [Link]	Iowa Data Privacy Act ("IDPA") [Link]	Montana Privacy Law (SB 384) [Link]	Tennessee Information Protection Act ("TIPA") [Link]	Florida Digital Bill of Rights ("FDBR") [Link]
Penalties	$7,500 per violation	$7,500 per violation	N/A; doesn't specify caps for monetary penalties	$7,500 in civil penalties for each violation of the law (in situations where a company fails to remedy the violation within the statutory cure period), as well as attorney's fees and investigative costs. Treble damages may be awarded for willful or knowing violations.	Civil penalties up to $50,000 per violation. Civil penalties may also be tripled if the violation involves a Florida consumer who is known to be a child, is based on the failure to delete data or correct personal information after receiving a request when an exception does not apply, or is based on continuing to sell or share a consumer's personal data after the consumer chooses to opt out.
Opt-in vs. Opt-out	Right to opt-out for the processing of their personal data for targeted advertising, profiling and selling of personal data. Opt-in for the collection of sensitive data. Sensitive data is defined to include personal data revealing racial or ethnic origin, religious beliefs, mental or physical health diagnosis made by a health care provider, sexual orientation, citizenship and immigration status; genetic and biometric data that identifies an individual; precise geolocation data; and personal data collected from a known child. A unique element of this definition is that sensitive data only includes health information to the extent a diagnosis has been made by a health care provider.	Right to opt-out of the sale of personal data. NOTE: Whether consumers have a right to opt out of targeted advertising is unclear; (right is not listed in consumer rights provision of bill, but controllers must provide means to opt out) The Iowa bill does not require that businesses obtain affirmative consent from consumers for any processing activities. -Processing sensitive data requires "clear notice and an opportunity to opt out of such processing" (Sec. 4(1))	Right to opt out of the processing of the consumer's personal data for purposes of targeted advertising or profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer. The Montana bill also does not require opt-out requests to be verified. In other words, a Montana resident will not have to prove their identity to opt out of the sale of their personal data, for targeted advertising, or for certain types of profiling. Opt out requests need not to be authenticated. For sensitive personal information, the Montana Law requires opt-in consent before a business can collect and process sensitive personal information. Opt-in rights for advertising and targeted marketing to individuals aged 13 to 16. The MCDPA does not recognize the validity of consent obtained through dark patterns.	Right to opt out of the sale of personal information, targeted advertising and profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer. . TIPA's carveout for pseudonymized information and deidentified data extends to the consumer right to opt-out of data sales, targeted advertising, and significant profiling decisions. Under the TIPA, without a consumer's opt-in consent, a controller may not process (including collection) sensitive data.	FDBR provides that consumers have a right to opt out of the collection or processing of sensitive data. Notably, controllers are separately prohibited from processing sensitive data without first obtaining consumer "consent". This diverges from other common frameworks that either require consent for processing sensitive data, or only create an opt-out right. FDBR will require all businesses (including those that do not meet FDBR revenue thresholds) to obtain consent prior to the sale of sensitive data, while also providing consumers the general right to opt-out of the sale of any personal data. Requires an opt-in for the processing of sensitive data (although the Act also provides for an opt-out right), processing of personal data for a purpose not reasonably necessary or compatible with the original purpose of the collection, the data of a known child aged 13 to 18 (through an "affirmative authorization"), and processing of data of a known child under 13 years (in compliance with COPPA). Companies that target ads based on pseudonymous data wouldn't be required to allow opt-outs, provided the pseudonymous data was stored separately from identifiable data. Right to opt out of the collection of sensitive personal data Right to opt out of the collection of personal data through a voice recognition feature. Consent requires an affirmative act. Acceptance of broad terms of use or consent obtained by dark patterns are not sufficient. Covered entities may not process the personal information of a person under 18 if they have actual knowledge or willfully disregard that processing may result in "substantial harm or privacy risk to children."
Universal Opt Out Mechanisms	No	No	Yes. Starting January 1, 2025, the MCDPA will require controllers to recognize universal opt-out mechanisms to effectuate opt-out requests for the sale of personal data and targeted advertising. MCDPA requires that an opt-out signal not be the default setting (i.e. a consumer must instead be required to affirmatively select the opt-out option) in order for it to be covered under the law. Oupt out requests need not be authenticated.	No	No
Portability	Yes; Consumers have the right to obtain a copy of the consumer's personal data processed by the controller, in a portable and, to the extent technically feasible, readily usable format such that it may be ported to another controller.	Yes; Consumers have the right to "to obtain a copy of the consumer's personal data, except as to personal data that is defined as "personal information" pursuant to section 715C.1 that is subject to security breach protection,that the consumer previously provided to the controller in a portable and, to the extent technically practicable, readily usable format that allows the consumer to transmit the data to another controller without hindrance, where the processing is carried out by automated means."	Yes; Consumers have the right to obtain a copy of the consumer's personal data processed by the controller, in a portable and, to the extent technically feasible, readily usable format such that it may be ported to another controller.	Yes. Consumers have the right to obtain a copy of the consumer's personal data. Data portability rights are limited to data the consumer previously provided. Controller must provide in a portable and, to the extent technically feasible, readily usable format such that it may be ported to another controller.	Yes. Consumers have the right to obtain a copy of the consumer's personal data. Data portability rights are limited to data the consumer previously provided. Controller must provide in a portable and, to the extent technically feasible, readily usable format such that it may be ported to another controller.
Processor Compliance and Contractual Requirements	S.B. 5 uses the terms "controller" and "processor." Under S.B 5, processors must assist controllers in meeting their obligations, including responding to consumer requests and conducting data protection impact assessments ("DPIAs"). S.B. 5 would require certain contractual terms between controllers and processors, including those requiring the processor to maintain a duty of confidentiality. A processor must adhere to the controller's instructions, including those regarding the nature, purposes, and duration of the processing, and the contract between a controller and processor must require: -Confidentiality of personal data; -Deletion or return of personal data at termination of the agreement; -Demonstration of compliance with the INCDPA upon request; -Cooperation with data protection impact assessments; and -Use of subcontractors that are subject to the same privacy requirements as processors. Requires controllers to provide a "reasonably accessible, clear, and meaningful" privacy notice to consumers that discloses the categories of personal data processed, the purpose of such processing, how consumers can exercise their rights (e.g., right to delete), categories of personal data shared with third parties, and categories of third parties with whom the data is shared. Controllers must not collect additional categories of personal data or use personal data collected for additional purposes without providing notice to consumers. Controllers may not process personal data for purposes that are neither reasonably necessary for nor compatible with the disclosed purposes for which the personal data is processed, unless the controllers obtain consumer consent.	A contract between a controller and a processor shall govern the processor's data processing procedures with respect to processing performed on behalf of the controller. Controllers have the following obligations and responsibilities: Controllers must provide consumers with a clear and accessible privacy notice that includes the categories of data the controller processes, the purpose of the processing, the categories of data that is shared with third parties and the types of third parties with whom the data is shared, a contact email address, and instructions for exercising data subject rights. If personal data is sold to third parties or used for targeted advertising, the controller must clearly and conspicuously disclose the processing, along with a means for the consumer to opt out of such sale. Transparency, purpose specification- A controller shall provide consumers with a reasonably accessible and comprehensive privacy notice that includes (1) the categories of personal data processed; (2) the purposes for which the personal data is processed; (3) how and where consumers may exercise a right; (4) the categories of personal data that the controller shares with third parties; and (5) the categories of third parties with whom the controller shares personal data; Security – A controller must maintain appropriate data security practices to protect the personal data and reduce risks of harm to the consumer relating to the processing of the data; The bill does not contain a duty to avoid secondary use, nor is there a responsibility to practice data minimization. Controllers shall provide a process for consumers to exercise their rights. Controllers have 90 days to respond to a request. Controllers can extend the period by another 45 days for good cause. While controllers must handle requests free, they may charge a fee for second or subsequent requests in a 12-month period, or if certain other circumstances apply.	Controllers must provide consumers with a clear and accessible privacy notice that includes the categories of data the controller processes, the purpose of the processing, the categories of data that is shared with third parties and the types of third parties with whom the data is shared, a contact email address, and instructions for exercising data subject rights. If personal data is sold to third parties or used for targeted advertising, the controller must clearly and conspicuously disclose the processing, along with a means for the consumer to opt out of such sale. Under the MCDPA, controllers must: -Limit the purpose of processing personal data to that which is reasonably necessary and proportional; Take steps to implement reasonable safeguards for the personal data within their control; -Refrain from discriminating against consumers for exercising their rights and from processing personal data in violation of federal laws that prohibit discrimination; -Ensure contracts control relationships with their processors (note: the law itself details the minimum necessary provisions of these contracts). Contracts between controllers and processors must set out instructions for processing data, the nature and purpose of processing, the types of data being processed, the duration of processing, and the rights and obligations of the respective parties. The contract must also establish the processor's obligations to ensure that processing is conducted subject to a duty of confidentiality, to delete or return personal data at the end of the provision of services at the controller's direction, and to require subcontractors to meet all obligations of the processor with respect to the data. -Data security: Controllers must adopt administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data. While the act doesn't prescribe specific measures, they should be appropriate considering the volume and nature of the data. Controllers must provide an effective means by which a consumer may revoke consent for the processing of personal data.	Under the TIPA, controllers must: -Limit the purpose of processing personal information to that which is reasonably necessary and proportional; -Take steps to implement reasonable safeguards for the personal information within their control; -Refrain from discriminating against consumers for exercising their rights and from processing personal information in violation of federal laws that prohibit discrimination; -Be transparent in their reasonably accessible, clear and meaningful privacy notice that includes the categories of data the controller processes, the purpose of the processing, the categories of data that is shared with third parties and the types of third parties with whom the data is shared, a contact email address, and instructions for exercising data subject rights. If personal data is sold to third parties or used for targeted advertising, the controller must clearly and conspicuously disclose the processing, along with a means for the consumer to opt out of such sale. -Ensure contracts control relationships with their processors. The contract is binding and must clearly set forth instructions for processing data, the nature and purpose of processing, the type of data subject to processing, the duration of processing, and the rights and obligations of both parties and includes specific requirements that the processor must follow in regard to how personal information is handled. TIPA requires controllers and processors to create, maintain and comply with a written privacy program and creates a safe harbor for businesses whose privacy program reasonably conforms with the National Institute of Standards and Technology (NIST) privacy framework. When a subsequent revision of the NIST privacy framework is published, businesses have one year to update their privacy program to conform to the revised framework.	Controllers and processors will have new responsibilities including creating retention schedules and disclosure obligations for the sale of sensitive or biometric data. The controller's contract with the vendor must include: -Clear instructions for processing data; -the nature and purpose of processing; -the type of data subject to processing; -the duration of processing; -the rights and obligations of both parties; -a requirement that the processor ensure that each person processing personal data is subject to a duty of confidentiality with respect to the data; -a requirement that the processor delete or return all personal data to the controller as requested after the provision of the service is completed, unless retention of the personal data is required by law; -a requirement that the processor make available to the controller, upon reasonable request, all information in the processor's possession necessary to demonstrate the processor's compliance with this part; -a requirement that the processor allow, and cooperate with, reasonable assessments by the controller or the controller's designated assessor; and -a requirement that the processor engage any subcontractor pursuant to a written contract that requires the subcontractor to meet the requirements of the processor with respect to the personal data. -If the processors engage an independent assessor to conduct an assessment of the processor's policies and technical and organizational measures under the Act, the processor shall provide the assessor's report to the controller upon request. Businesses regulated under FDBR that utilize voice or face recognition, or have video or audio features in devices, will be subject to heightened restrictions for data collected through these services, regardless of whether the device can identify an individual. If a controller sells sensitive or biometric data, they must provide the following notice: "NOTICE: This website may sell your [sensitive and/or biometric] personal data and/or biometric personal data." If the controller discloses pseudonymous data to the processor, it must engage in reasonable oversight to monitor compliance with any contractual commitments to which the data or information is subject and must take appropriate steps to address any breach of the contractual commitments.

4A's State Data Privacy Laws Comparison

	Texas Data Privacy and Security Act ("TDPSA") [Link]	Utah Consumer Privacy Act ("UCPA") [Link]	Oregon Consumer Privacy Act ("OCPA") [Link]	Delaware Personal Data Privacy Act ("DPDPA") [Link]	New Jersey Data Privacy Act ("NJDPA") [Link]
Key Dates	**Effective:** March 1, 2024 **Cure Sunset Date:** None **Universal Opt Out Mechanism:** January 1, 2024	**Effective:** March 24, 2022 **Enforcement:** December 31, 2023 **Cure Sunset Date:** None	**Effective:** July 1, 2024; July 1, 2025 [non-profits] **Cure Sunset Date:** January 1, 2026 **Universal Opt Out Mechanism:** January 1, 2026	**Effective:** January 1, 2025 **Cure Sunset Date:** December 31, 2025 **Universal Opt Out Mechanism:** January 1, 2026	**Effective:** January 1, 2025 **Cure Sunset Date:** July 16, 2026 **Universal Opt Out Mechanism:** July 1, 2025
Covered Entities and Exceptions	The scope of the Texas bill is drawn somewhat differently, and more broadly, than existing state privacy laws. Unlike those laws, which generally apply to businesses that exceed certain revenue or data processing thresholds, the Texas bill applies to corporations and people who 1) Conduct business in Texas or produce a product or service consumed by Texas residents; 2) Process personal data of Texas residents; and 3) Are not a small business as defined by the U.S. Small Business Administration (SBA). The Texas bill has no data-processing volume threshold. While the SBA currently defines a small business as one having 500 or fewer employees, this definition may be subject to adjustment, and there are myriad exceptions to the current SBA definition. The law's prohibition against selling sensitive data without consent applies to all businesses that operate in Texas, regardless of size. The bill features a familiar list of exceptions and exemptions. It does not apply to state agencies, nonprofit organizations, higher education institutions, or entities governed by the Health Information Portability and Accountability Act (HIPAA) or the Gramm-Leach-Bliley Act. The bill only protects consumers acting in an individual or household capacity, and therefore it's not applicable to employment or business-to-business (B2B) contexts. Publicly available information is also excluded.	Applies to business in the state of Utah or those who produces products or services targeted toward consumers who are Utah residents; and -Has an annual revenue of $25 million or more; and either -Processes or controls personal data of 100,000 or more Utah citizens or derives more than 50% of its gross revenue from processing or controlling the personal data of 25,000 or more Utah consumers. Exceptions: The law exempts certain types of data and entities, including publicly available data, de-identified data, and data subject to the Health Insurance Portability and Accountability Act, the Driver's Privacy Protection Act, and the Family Education Rights and Privacy Act. The UCPA also includes broad entity-based exemptions for entities and businesses covered by the Fair Credit Reporting Act and the Gramm-Leach-Bliley Act, as well as non-profit entities, higher education institutions, tribes, and government bodies.	OCPA applies to persons that conduct business in Oregon or that provide products or services to Oregon residents and that, during a calendar year, control or process the personal data of 100,000 or more consumers (other than personal data controlled or processed solely for the purpose of completing a payment transaction) or the personal data of 25,000 or more consumers while deriving 25% or more of the person's annual gross revenue from selling personal data. OCPA does not provide entity-level exemptions for covered entities or business associates regulated under HIPAA or financial institutions covered under the Gramm-Leach-Bliley Act ("GLBA"). Instead, the Act only creates information-level exemptions for information governed under HIPAA and GLBA (though the Act does exempt financial institutions governed under the Bank Holding Company Act). It contains an exemption for employment-related data, public corporations, state government bodies, local government bodies and special government bodies. OCPA does not exempt non-profits although it does contain limited non-profit exemptions for organizations established to detect and prevent fraudulent acts in connection with insurance and organizations that provide programming to radio or television networks.	DPDPA covers businesses that control or process personal data on more than 35,000 consumers or derive 20% of revenue from selling the data of more than 10,000 consumers. The bill contains both entity-level and data-level exemptions for GLBA financial institutions and information subject to the GLBA. It does not contain an entity-level exemption for HIPAA covered entities and business associates. The bill does contain several data-level exemptions for health data, but these are not the same as in the Connecticut law. DPDPA exempts state governmental entities; however, it states that the exemption excludes "any institution of higher education." DPDPA does not exempt non-profits. It only exempts nonprofit organizations that are "dedicated exclusively to preventing and addressing insurance crime." The bill also exempts personal data "of a victim of or witness to child abuse, domestic violence, human trafficking, sexual assault, violent felony, or stalking that is collected, processed, or maintained by a nonprofit organization that provides services to victims of or witnesses to child abuse, domestic violence, human trafficking, sexual assault, violent felony, or stalking." Delaware already has an existing online privacy law – the Delaware Online Privacy and Protection Act (DelOPPA). Although the requirements in DelOPPA are far less stringent than this new bill, entities should consider both laws when driving compliance.	NJDPA applies to data controllers conducting business in New Jersey or targeting consumers who are state residents, and that either (1) control or process the data of at least 100,000 consumers, or (2) control or process data of at least 25,000 consumers and derives revenue, or receives a discount on the price of any goods or services from the sale of personal data. NJDPA does not have a separate criteria for minimum percent of income generated by data in order to trigger applicability under the law. NJDPA does not apply to Gramm-Leach-Bliley Act-regulated entities and state-regulated insurance companies. NJDPA contains a narrow data-level (and not entity-level) HIPAA exemption, exempting PHI collected by a HIPAA covered entity or business associate. Personal information handled by a consumer reporting agency is also exempt, as is information used in connection with human subject research under federal law. NJDPA will apply to nonprofits that otherwise meet applicable standards. It contains an exemption for employment-related data, public corporations, state government bodies, local government bodies, and special government bodies. B2B data is also exempted.
Notice	In a "reasonably accessible, clear and meaningful privacy notice". Must includes information about the types of personal data they collect, how consumers can exercise their rights, and the categories of personal data shared with third parties.	In a "reasonably accessible and clear privacy notice" on businesses' website and in a notice prior to processing a consumer's sensitive data	Controllers must provide consumers with a privacy notice that describes: the categories of personal data processed (including sensitive data); purposes for said processing; how consumers may exercise their consumer data rights; specific third parties with whom the controller shares personal data; controller's contact information including identity, and email address; any processing of personal data in which the controller engages for the purpose of targeted advertising or for the purpose of profiling; and the method for consumers to submit requests. The OCPA borrows from Colorado by stating that controllers must specify in their "privacy notice . . . the express purposes for which the controller is collecting and processing personal data."	Controllers must provide consumers with a privacy notice that describes: the categories of personal data processed (including sensitive data); purposes for said processing; how consumers may exercise their consumer data rights; categories of personal data the controller shares with third parties; controller's contact information including identity, and email address; any processing of personal data in which the controller engages for the purpose of targeted advertising or for the purpose of profiling; and the method for consumers to submit requests. The DPDPA borrows from Colorado by stating that controllers must specify in their "privacy notice . . . the express purposes for which the controller is collecting and processing personal data."	NJDPA requires controllers to provide a reasonably accessible, clear and meaningful privacy notice that includes: (1) the categories of personal data processed by the controller; (2) the purposes for processing personal data; (3) the categories of third parties to whom personal data is disclosed; (4) the categories of personal data shared with third parties; (5) how consumers may exercise their privacy rights, and how to appeal a controller's decision on a privacy request; (6) how the controller notifies consumers of material changes to the privacy notice; (7) the privacy notice's effective date; and (8) an active email address or other online mechanism that consumers may use to contact the controller. NJDPA expressly requires businesses to include the use of cookies/pixels and other tracking technology in its notice to consumers.
Targeting Advertising and Key Definitions	"Personal data" means any information, including sensitive data, that is linked or reasonably linkable to an identified or identifiable individual. The term 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. The term does not include deidentified data or publicly available information. "Sale of personal data" means the sharing, disclosing,or transferring of personal data for monetary or other valuable consideration by the controller to a third party. "Sensitive data" means a category of personal data. The term includes: (A) personal data revealing racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexuality, or citizenship or immigration status; (B) genetic or biometric data that is processed for the purpose of uniquely identifying an individual; (C) personal data collected from a known child; or D) precise geolocation data. "Targeted advertising" means displaying to a consumer an advertisement that is selected based on personal data obtained from that consumer's activities over time and across nonaffiliated websites or online applications to predict the consumer's preferences or interests.	"Sale," "sell," or "sold" means the exchange of personal data for monetary consideration by a controller to a third party. "Targeted advertising" means displaying an advertisement to a consumer where the advertisement is selected based on personal data obtained from the consumer's activities over time and across nonaffiliated websites or online applications to predict the consumer's preferences or interests. "Personal data" means information that is linked or reasonably linkable to an 162identified individual or an identifiable individual. "Sensitive data" means: 206(I) personal data that reveals: 207(A) an individual's racial or ethnic origin; 208(B) an individual's religious beliefs; 209(C) an individual's sexual orientation; 210(D) an individual's citizenship or immigration status; or 211(E) information regarding an individual's medical history, mental or physical health 212condition, or medical treatment or diagnosis by a health care professional; 213(ii) the processing of genetic personal data or biometric data, if the processing is for the 214purpose of identifying a specific individual; or 215(iii) specific geolocation data.	"Personal data" means 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. "Sale" or "sell" means the exchange of personal data for monetary or other valuable consideration by the controller with a third party. "Sensitive data" means personal data that: (A) Reveals a consumer's racial or ethnic background, national origin, religious beliefs, mental or physical condition or diagnosis, sexual orientation, status as transgender or nonbinary, status as a victim of crime or citizenship or immigration status; (B) Is a child's personal data; (C) 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; or (D) Is genetic or biometric data. "Targeted advertising" means advertising that is selected for display to a consumer on the basis of personal data obtained from the consumer's activities over time and across one or more unaffiliated websites or online applications and is used to predict the consumer's preferences or interests. The OCPA's definition of "biometric data" also is unique. Oregon's definition does not require controllers to use biometric data to identify an individual, which is required by Connecticut and the Colorado Rules. "Biometric data" means personal data generated by automatic measurements of a consumer's biological characteristics, such as the consumer's fingerprint, voiceprint, retinal pattern, iris pattern, gait or other unique biological characteristics that allow or confirm the unique identification of the consumer.	"Personal data" means any information that is linked or reasonably linkable to an identified or identifiable individual, and does not include de-identified data or publicly available information. "Sale" or "sell" means the exchange of personal data for monetary or other valuable consideration by the controller with a third party. "Sensitive data" means personal data that includes data revealing racial or ethnic origin, religious beliefs, mental or physical health condition or diagnosis (including pregnancy), sex life, sexual orientation, status as transgender or nonbinary, citizenship status, or immigration status, Genetic or biometric data Personal data of a known child, or precise geolocation data. "Targeted advertising" means displaying advertisements to a consumer where the advertisement is selected based on personal data obtained or inferred from that consumer's activities over time and across nonaffiliated Internet web sites or online applications to predict such consumer's preferences or interests. The Delaware bill also contains a definition of genetic data, which does not appear in other laws. It is defined as "any data, regardless of its format, that results from the analysis of a biological sample of an individual, or from another source enabling equivalent information to be obtained, and concerns genetic material. For purposes of this paragraph, "genetic material" includes deoxyribonucleic acids (DNA), ribonucleic acids (RNA), genes, chromosomes, alleles, genomes, alterations or modifications to DNA or RNA, single nucleotide polymorphisms (SNPs), uninterpreted data that results from analysis of the biological sample or other source, and any information extrapolated, derived, or inferred therefrom."	"Personal data" means any information that is linked or reasonably linkable to an identified or identifiable person. Personal data shall not include de-identified data or publicly available information. "Targeted advertising" means displaying advertisements to a consumer where the advertisement is selected based on personal data obtained or inferred from that consumer's activities over time and across nonaffiliated Internet web sites or online applications to predict such consumer's preferences or interests. "Biometric Data" means physical and behavioral characteristics in addition to biological characteristics; data generated by "technological processing" or "analysis"; and specific references to facial mapping, facial geometry, and facial templates. This definition is perceived to be broader than other state laws. "Sale" means the disclosure of personal data to a third party for "monetary or other valuable consideration." It does not include all of the exceptions to a sale that are found in many other privacy laws, including importantly when the consumer directs the disclosure or uses the Controller to engage with a third party. "Sensitive Data" includes (1) financial information, defined as a consumer's "account number, account log-in financial account, or credit or debit card number, in combination with any required security code, access code, or password that would permit access to a consumer's financial account"; (2) "mental or physical health condition, treatment or diagnosis"; and (3) "status as transgender or non-binary."
Consumer Rights	**Right to Know**: what personal info is being collected and whether a controller is processing their personal data **Right to Access:** Access the personal data that a controller processes about them **Right to Deletion:** Provides consumers a narrow deletion right that applies only to personal data that the consumer provided to the controller. **Right to Portability:** Ability to obtain a copy of their personal data in a format that is portable, readily usable, and allows the consumer to transmit the data to another controller without impediment; and **Right to Opt Out:** Allows consumer the option to out of the processing of their personal data if used for targeted advertising or the sale of personal data. Consumers, in their requests, must specify the right they intend to exercise. Excludes data that is pseudonymized or publicly available.	**Right to Know**: what personal info is being collected and whether a controller is processing their personal data **Right to Access:** Access the personal data that a controller processes about them **Right to Deletion:** Provides consumers a narrow deletion right that applies only to personal data that the consumer provided to the controller. **Right to Portability:** Ability to obtain a copy of their personal data in a format that is portable, readily usable, and allows the consumer to transmit the data to another controller without impediment; and **Right to Opt Out:** Allows consumer the option to out of the processing of their personal data if used for targeted advertising or the sale of personal data. Consumers, in their requests, must specify the right they intend to exercise. Excludes data that is pseudonymized or publicly available.	Right to Know: what personal info is being collected and whether a controller is processing their personal data Right to Access: Access the personal data that a controller processes about them Right to Deletion: Provides consumers a narrow deletion right that applies only to personal data that the consumer provided to the controller. Right to Portability: Ability to obtain a copy of their personal data in a format that is portable, readily usable, and allows the consumer to transmit the data to another controller without impediment; and Right to Opt Out: Allows consumer the option to out of the processing of their personal data if used for targeted advertising or the sale of personal data. Consumers, in their requests, must specify the right they intend to exercise. Pseudonymous data is not exempt from any access rights in OCPA. Opt-out requests need not be authenticated.	**Right to Know:** what personal info is being collected and whether a controller is processing their personal data **Right to Access:** Access the personal data that a controller processes about them **Right to Deletion:** Provides consumers a narrow deletion right that applies only to personal data that the consumer provided to the controller. **Right to Portability:** Ability to obtain a copy of their personal data in a format that is portable, readily usable, and allows the consumer to transmit the data to another controller without impediment; and **Right to Opt Out:** Allows consumer the option to out of the processing of their personal data if used for targeted advertising or the sale of personal data. Consumers, in their requests, must specify the right they intend to exercise. Excludes data that is pseudonymized or publicly available.	Right to Know: what personal info is being collected and whether a controller is processing their personal data Right to Access: Access the personal data that a controller processes about them Right to Deletion: Provides consumers a narrow deletion right that applies only to personal data that the consumer provided to the controller. Right to Portability: Ability to obtain a copy of their personal data in a format that is portable, readily usable, and allows the consumer to transmit the data to another controller without impediment; and Right to Opt Out: Allows consumer the option to out of the processing of their personal data if used for targeted advertising or the sale of personal data. Pseudonymous data is not exempt from any access rights in NJDPA.
Appeals Process	Yes. 60 days to respond.	No	Yes. 60 days to respond.	Yes. 60 days to respond.	Yes. 45 days to respond.
Data Protection Assessments (DPA)	"Yes. DPAs are required when conducting processing activities that present a heightened risk of harm. This heightened risk of hard includes: 1) Targeted advertising where profiling presents a risk of A) unfair or deceptive treatment, or unlawful or disparate impact on consumers; B) Financial or physical injury; C) Other substantial injury. 2) Selling personal information 3) Processing sensitive data DPAs must be made available to AG upon request. AG can then evaluate DPA for compliance.	None	Yes. DPAs are required for each of the following processing activities involving personal data including: 1) Processing data for the purposes of targeted advertising. 2) Selling personal data. 3) Processing personal data for the purposes of profiling, where such profiling presents a reasonably foreseeable risk of substantial injury to consumers. 4) Processing sensitive data. AG may request and evaluate a DPA for compliance. The OCPA contains a requirement for controllers to maintain data protection assessments for at least five years.	Yes. DPAs are required for each of the following processing activities involving personal data including: 1) Processing data for the purposes of targeted advertising. 2) Selling personal data. 3) Processing personal data for the purposes of profiling, where such profiling presents a reasonably foreseeable risk of substantial injury to consumers. 4) Processing sensitive data. The requirements shall apply to processing activities created or generated on or after six months after the law's effective date.	Yes. NJDPA requires controllers to conduct a data protection assessment before engaging in any processing that "presents a heightened risk of harm to a consumer." DPIAs must be done if the control engages in the following activities that create a "heightened risk" including: -Processing personal data for targeted advertising -Selling personal data -Processing personal data for profiling if the profiling presents a reasonably foreseeable risk of legal, deceptive, discriminatory, financial, reputational or physical harms -Processing sensitive data The required assessment must analyze the benefits of the processing to the company, consumer and public while weighing the harms and potential mitigants. NJDPA allows for the use of impact assessments done under other state laws to count toward the requirements of the NJDPA.
Enforcement	AG Enforcement	Begin with the state's Division of Consumer Protection, referred for AG Enforcement	AG Enforcement	AG Enforcement	AG Enforcement
Private Right of Action	No	No	No	No	No
Cure Period	Yes. 30 days to cure alleged violation. No cure sunset.	Yes. 30 days to cure alleged non-compliance after written notice. No cure sunset.	Yes. 60 days to cure alleged violation. Cure sunsets January 1, 2026.	Yes. 60 days to cure alleged violation. Cure sunsets December 31, 2025.	Yes. 30 days to cure alleged violation. Cure sunsets July 16, 2026.

4A's State Data Privacy Laws Comparison					
	Texas Data Privacy and Security Act ("TDPSA") [Link]	Utah Consumer Privacy Act ("UCPA") [Link]	Oregon Consumer Privacy Act ("OCPA") [Link]	Delaware Personal Data Privacy Act ("DPDPA") [Link]	New Jersey Data Privacy Act ("NJDPA") [Link]
Penalties	$7,500 per violation in civil penalties.	Actual damages to the consumer and $7,500 per violation in civil penalties.	$7,500 per violation in civil penalties.	$7,500 per violation in civil penalties.	Civil fines of up to $10,000 for the first violation and up to $20,000 for the second and subsequent violations.
Opt-in vs. Opt-out	Right to opt out of the sale of personal information, targeted advertising and profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer. TIPA has a carveout for pseudonymized information and deidentified data extends to the consumer right to opt-out of data sales, targeted advertising, and significant profiling decisions. Under the TDPSA, without a consumer's opt-in consent, a controller may not process (including collection) or sell sensitive data . The TDPSA does not recognize the validity of consent obtained through dark patterns.	Right to opt-out of the processing of their personal data if used for targeted advertising or the sale of personal data. Controllers must present a consumer with notice and an opportunity to opt out prior to processing their sensitive data.	Right to opt-out of processing of personal data concerning the consumer for purposes of targeted advertising, the sale of personal data. Opt-in for processing of sensitive data and profiling in furtherance of solely automated decisions that produce legal or similarly significant effects concerning the consumer. The OCPA also does not require opt-out requests to be verified. An OR resident will not have to prove their identity to opt out of the sale of their personal data, for targeted advertising, or for certain types of profiling. Pseudonymous data is not exempt from any access rights in OCPA., including opt-out right. Opt-in for targeted advertising or sale of PI of children ages 13-15. Opt-out requests need not to be authenticated.	Right to opt-out of processing of personal data concerning the consumer for purposes of targeted advertising, the sale of personal data, or profiling in furtherance of solely automated decisions that produce legal or similarly significant effects concerning the consumer. Opt-in for processing of sensitive data. A DE resident will not have to prove their identity to opt out of the sale of their personal data, for targeted advertising, or for certain types of profiling. Opt-in for targeted advertising or sale of PI of children ages 13-15. Requires individuals to provide opt-in consent for profiling. Delaware adds "demographic characteristics" to the list of topics covered by profiling.	The right to opt out of processing of personal data for "targeted advertising", "sale" of personal data, and "profiling" in furtherance of decisions that produce legal or similarly significant effects concerning a consumer. Opt-in for processing of "sensitive data" . Pseudonymous data is not exempt from any access rights in NJDPA, including opt-out right. Opt-in for targeted advertising or sale of PI of children ages 13-16.
Universal Opt Out Mechanisms	Yes. Effective January 1, 2025, UOOM signals must be recognized; TDPSA requires that an opt-out signal not be the default setting (i.e. a consumer must instead be required to affirmatively select the opt-out option) in order for it to be covered under the law.	No	Yes. Effective Jan. 1, 2026, OCPA also will require controllers to recognize universal opt-out mechanisms as of January 1, 2026. UOOM must not use a default setting ; it requires the consumer or authorized agent to make an affirmative, voluntary and unambiguous choice to opt out and the UOOM must be consumer-friendly.	Yes. DPDPA will require controllers to recognize universal opt-out mechanisms as of January 1, 2026. UOOM must not use a default setting ; it requires the consumer or authorized agent to make an affirmative, voluntary and unambiguous choice to opt out and the UOOM must be consumer-friendly. Attorney General's Office may publish or reference a list on its website of authorized agents. It appears this may be a reference to the Colorado Privacy Act Rules in which the Colorado Attorney General's Office states it will publish such a list.	Yes. NJPDA will require controllers to recognize universal opt-out mechanisms as of July 16, 2025. UOOM must not use a default setting; it requires the consumer or authorized agent to make an affirmative, voluntary and unambiguous choice to opt out and the UOOM must be consumer-friendly.
Portability	Yes. Consumers have the right to obtain a copy of the consumer's personal data. Data portability rights are limited to data the consumer previously provided. Controller must provide in a portable and, to the extent technically feasible, readily usable format such that it may be ported to another controller.	Yes. Consumers have the right to obtain a copy of the consumer's personal data. Data portability rights are limited to data the consumer previously provided. Controller must provide in a portable and, to the extent technically feasible, readily usable format such that it may be ported to another controller.	Yes. Consumers have the right to obtain a copy of the consumer's personal data. Data portability rights are limited to data the consumer previously provided. Controller must provide in a portable and, to the extent technically feasible, readily usable format such that it may be ported to another controller.	Yes. Consumers have the right to obtain a copy of the consumer's personal data. Data portability rights are limited to data the consumer previously provided. Controller must provide in a portable and, to the extent technically feasible, readily usable format such that it may be ported to another controller.	Yes. Consumers have the right to obtain a copy of the consumer's personal data. Data portability rights are limited to data the consumer previously provided. Controller must provide in a portable and, to the extent technically feasible, readily usable format such that it may be ported to another controller.
Processor Compliance and Contractual Requirements	The controller's contract with the vendor must include: -Clear instructions for processing data; -the nature and purpose of processing; -the type of data subject to processing; -the duration of processing; -the rights and obligations of both parties; -a requirement that the processor ensure that each person processing personal data is subject to a duty of confidentiality with respect to the data; -a requirement that the processor delete or return all personal data to the controller as requested after the provision of the service is completed, unless retention of the personal data is required by law; -a requirement that the processor make available to the controller, upon reasonable request, all information in the processor's possession necessary to demonstrate the processor's compliance with this part; -a requirement that the processor allow, and cooperate with, reasonable assessments by the controller or the controller's designated assessor; and -a requirement that the processor engage any subcontractor pursuant to a written contract that requires the subcontractor to meet the requirements of the processor with respect to the personal data. -If the processors engage an independent assessor to conduct an assessment of the processor's policies and technical and organizational measures under the Act, the processor shall provide the assessor's report to the controller upon request. If a controller sells sensitive or biometric data, they must provide the following notice: "NOTICE: This website may sell your [sensitive and/or biometric] personal data and/or biometric personal data." If the controller discloses pseudonymous data, deidentified data, or aggregate consumer information to the processor, it must engage in reasonable oversight to monitor compliance with any contractual commitments to which the data or information is subject and must take appropriate steps to address any breach of the contractual commitments.	Controllers have the following obligations and responsibilities: Transparency, purpose specification– A controller shall provide consumers with a reasonably accessible and comprehensive privacy notice that includes (1) the categories of personal data processed; (2) the purposes for which the personal data is processed; (3) how and where consumers may exercise a right; (4) the categories of personal data that the controller shares with third parties; and (5) the categories of third parties with whom the controller shares personal data; Security – A controller must maintain appropriate data security practices to protect the personal data and reduce risks of harm to the consumer relating to the processing of the data; Nondiscrimination and nonretaliation – A controller may not discriminate against a consumer for exercising a right; and Nonwaiver of consumer rights – Any provision of a contract purporting to limit or waive a consumer's right under the UCPA is void. The bill does not contain a duty to avoid secondary use nor a data minimization requirement. Controllers shall provide a process for consumers to exercise their rights.	Controllers must provide consumers with a privacy notice that describes: the categories of personal data processed (including sensitive data); purposes for said processing; how consumers may exercise their consumer data rights; categories of personal data the controller shares with third parties; specific third parties with whom the controller shares personal data; controller's contact information including identity, and email address; any processing of personal data in which the controller engages for the purpose of targeted advertising or for the purpose of profiling; and the method for consumers to submit requests. Controllers may not process personal data for purposes that are neither reasonably necessary for nor compatible with the disclosed purposes for which the personal data is processed, unless the controllers obtain consumer consent. OCPA uses the terms "controller" and "processor." Under S.B 5, processors must assist controllers in meeting their obligations, including responding to consumer requests and conducting data protection assessments. OCPA would require certain contractual terms between controllers and processors, including those requiring the processor to maintain a duty of confidentiality. A processor must adhere to the controller's instructions, including those regarding the nature, purposes, and duration of the processing, and the contract between a controller and processor must require: -Confidentiality of personal data; -Deletion or return of personal data at termination of the agreement; -Demonstration of compliance with the OCPA upon request; -Cooperation with data protection impact assessments; and -Use of subcontractors that are subject to the same privacy requirements as processors. Controllers must provide an effective means by which a consumer may revoke consent for the processing of personal data.	Controllers must provide consumers with a privacy notice that describes: the categories of personal data processed (including sensitive data); purposes for said processing; how consumers may exercise their consumer data rights; categories of personal data the controller shares with third parties; all categories of third parties with whom the controller shares personal data; controller's contact information including identity, and email address; any processing of personal data in which the controller engages for the purpose of targeted advertising or for the purpose of profiling; and the method for consumers to submit requests. Controllers may not process personal data for purposes that are neither reasonably necessary for nor compatible with the disclosed purposes for which the personal data is processed, unless the controllers obtain consumer consent. DPDPA uses the terms "controller" and "processor." Under the DPDPA, processors must assist controllers in meeting their obligations, including responding to consumer requests and conducting data protection assessments. DPDPA would require certain contractual terms between controllers and processors, including those requiring the processor to maintain a duty of confidentiality. A processor must adhere to the controller's instructions, including those regarding the nature, purposes, and duration of the processing, and the contract between a controller and processor must require: -Confidentiality of personal data; -Deletion or return of personal data at termination of the agreement; -Demonstration of compliance with the DPDPA upon request; -Cooperation with data protection impact assessments; and -Use of subcontractors that are subject to the same privacy requirements as processors. Controllers must provide an effective means by which a consumer may revoke consent for the processing of personal data.	Controllers must provide consumers with a privacy notice that describes: the categories of personal data processed (including sensitive data); purposes for said processing; how consumers may exercise their consumer data rights; categories of personal data the controller shares with third parties; all categories of third parties with whom the controller shares personal data; controller's contact information including identity, and email address; any processing of personal data in which the controller engages for the purpose of targeted advertising or for the purpose of profiling; and the method for consumers to submit requests. Under the NJDPA, processors must assist controllers in meeting their obligations, including responding to consumer requests and conducting data protection assessments. NJDPA would require certain contractual terms between controllers and processors, including those requiring the processor to maintain a duty of confidentiality. A processor must adhere to the controller's instructions, including those regarding the nature, purposes, and duration of the processing, and the contract between a controller and processor must require: -Confidentiality of personal data; -Deletion or return of personal data at termination of the agreement; -Demonstration of compliance with the NJDPA upon request; -Cooperation with data protection impact assessments; and -Use of subcontractors that are subject to the same privacy requirements as processors. Controllers must provide an effective means by which a consumer may revoke consent for the processing of personal data. Controllers may not process personal data for purposes that are neither reasonably necessary for nor compatible with the disclosed purposes for which the personal data is processed, unless the controllers obtain consumer consent.