LEGISLATIVE/REGULATORY ALERT

**TO:** ATP Members

**FROM:** Alan Thiemann, Donna McPartland, and Will Snoeyenbos

 Han Santos, PLLC

**DATE:** May 25, 2023

**RE:** State Privacy Legislation Update

Four states have just enacted comprehensive consumer data privacy legislation, bringing to 10 the number of states that have consumer privacy laws. **Testing organizations now have more state laws to add to their list for compliance with privacy rights and to address from a contractual standpoint.**

The newest states are: Iowa Governor Kim Reynolds signed data privacy legislation into law on March 28, 2023; Indiana Governor Eric Holcomb signed privacy legislation into law on May 1, 2023; Tennessee Governor Bill Lee signed privacy legislation into law on May 11, 2023. Finally, Montana Governor Greg Gianforte signed privacy legislation on May 19, 2023.

The Iowa Act Relating to Consumer Data Protection, the Indiana Consumer Data Protection Law, the Montana Consumer Data Privacy Act, and the Tennessee Information Protection Act are generally business-friendly and share a number of similar core requirements. Key similarities and differences are discussed below.

Effective Dates

Montana: October 1, 2024

Iowa: January 1, 2025

Tennessee: July 1, 2025

Indiana: January 1, 2026

Scope and Applicability

All four laws apply to entities that either conduct business in or target the sale of products or services to state residents. Under all four laws, de-identified data that the controller has stated it will not try to re-identify is NOT included as “personal information.” Also, none of these laws define business contact information or information collected from job applicants and employees as “consumer” information.

While the language of each state law is somewhat different, the Tennessee law provides a good illustration of the definition of business contact and employee data from coverage, including when such data is processed or maintained:

(A) In the course of an individual applying to, being employed by, or acting as an agent or independent contractor of a controller, processor, or third party, to the extent that the data is collected and used within the context of that role;

(B) As the emergency contact information of an individual under this part used for emergency contact purposes; or

(C) That is necessary to retain to administer benefits for another individual relating to the employee (or agent) and used for the purposes of administering those benefits.

Indeed, a last-minute amendment to the Tennessee legislation provided that, “a natural person acting in a commercial or employment context is not a consumer for purposes of this bill.”

NOTE: Under the California Privacy Reform Act, which went into effect on January 1, 2023, business contact information and employment information are now considered "personal information."

Definition of When a Business is Covered:

A business is covered by the new consumer privacy laws when it processes:

Iowa: 100,000 Iowa consumers during a calendar year, or entities that control or process the data of at least 25,000 Iowa consumers and derive 50% of gross revenue from the sale of personal data. *There is no revenue threshold.*

Indiana: 100,000 Indiana consumers during a calendar year, or entities that control or process the data of at least 25,000 Indiana consumers and derive 50% of gross revenue from the sale of personal data. *There is no revenue threshold.*

Montana: 50,000 Montana consumers (no calendar year requirement), excluding personal data controlled or processed solely for the purpose of completing a payment transaction, or entities that control or process the personal data of 25,000 consumers and derive more than 25% of gross revenue from the sale of personal data. *There is no revenue threshold.*

Tennessee: Companies that exceed $25 million in revenue and control or process either 175,000 Tennessee consumers during a calendar year or control or process personal information of at least 25,000 consumers and derive more than 50% of gross revenue from the sale of personal information.

Consumer Data Rights

Under each of the new privacy laws, a covered business must give notice to consumers about the categories of data it processes, the purpose(s) for processing, categories of data being sold or shared, and provide consumers with information about exercising their consumer rights. A list of a consumer’s rights for each state follow:

Iowa: Right to access, right to delete, right to data portability, and right to opt out of sale of personal data. Iowa does **not** grant consumers the right to correct their personal data or opt out of the processing of their personal data for purposes of profiling. The law only grants consumers the right to opt out of the processing of their sensitive personal data.

The Iowa law requires controllers who engage in targeted advertising to "clearly and conspicuously disclose such activity, as well as the manner in which a consumer may exercise the right to opt out of such activity.”

Indiana: Right to access, right to correct, right to delete, right to data portability, right to opt out of the processing of personal data for purposes of (1) targeted advertising (2) sale of personal data; and (3) profiling. Sensitive data processing requires opt-in consent.

Montana: Right to access, right to correct, right to delete, right to data portability, right to right to opt out of the processing of personal data for purposes of (1) targeted advertising (2) sale of personal data; and (3) profiling. Sensitive data processing requires opt-in consent.

Tennessee: Right to access, right to correct, right to delete, right to data portability, and right to opt out of a controller’s selling personal information about the consumer. Sensitive data processing requires opt-in consent.

The Tennessee law also includes an additional consumer right to request that a controller who sold personal information about the consumer, or disclosed the information for a business purpose, to disclose to the consumer: (i) the categories of personal information about the consumer the business sold; (ii) the categories of third parties to which the personal information about the consumer was sold by category of personal information for each category of third parties to which the personal information was sold; and (iii) the categories of personal information about the consumer that the business disclosed for a business purpose.

Data Protection Assessments

Provisions related to whether a controller will need to conduct a data impact assessment (“DPA”) before it engages in processing activities?

Iowa: Preparation of a DPA is **not** required under the Iowa law.

Indiana: A DPA is required when (1) the personal data is processed for targeted advertising, (2) there is a sale of personal data, (3) the personal data is used for profiling and there is a reasonably foreseeable risk of harm (4 harms listed), (4) sensitive data (which includes biometric information) is processed, and (5) when any processing activities involving personal data present a heightened risk of harm to consumers.

The Indiana law allows a controller that a DPA prepared for compliance with other data privacy laws may be used to comply if the assessment has a reasonably comparable scope and effect. The DPA requirement applies to processing activities created or generated after **December 31, 2025**.

Montana: A DPA is required for each of a controller’s processing activities that present a heightened risk of harm to a consumer. Processing that presents a heightened risk of harm to a consumer includes (1) the processing of personal data for purposes of targeted advertising (2) the sale of personal data (3) the personal data is used for profiling and there is a reasonably foreseeable risk of harm (4 harms listed), and (4) processing sensitive data.

A DPA conducted for compliance with other data privacy laws may be used to comply if the assessment has a reasonably similar in scope and effect. DPAs must be created or generated after **January 1, 2025** and are not retroactive.

Tennessee: A DPA is required when (1) the personal data is processed for targeted advertising, (2) there is a sale of personal data, (3) the personal data is used for profiling and there is a reasonably foreseeable risk of harm (4 harms listed), (4) sensitive data is processed, and (5) when any processing activities involving personal data present a heightened risk of harm to consumers.

DPAs must identify and weigh the benefits that may flow, directly and indirectly, from the processing

for each of the controller, the consumer, other stakeholders, and the public against the potential risks to the rights of the consumer associated with the processing, as mitigated by safeguards that can be employed by the controller to reduce the risks.

A DPA conducted by a controller for the purpose of compliance with other laws, rules, or regulations may be used to comply with this section if the assessments have a reasonably comparable scope and effect. DPAs apply to processing activities created or generated after **July 1, 2024,** and are not retroactive.

Cure Window

Each of these state laws contains a provision enabling a controller to have a period of time to cure any notice of violation it receives from the state Attorney General.

Iowa: 90 days.

Indiana: 30 days.

Montana: 60 days, but this provision sunsets as of April 1, 2026.

Tennessee: 60 days.

Are Nonprofits Covered?

Under all four laws, Nonprofit organizations are exempt. In at least Iowa and Montana, higher education institutions are not covered.

Data Exemptions

Under all four laws, personal information collected by a controller under FERPA (“student data”) is exempted. Besides FERPA, collection of data subject to HIPAA (personal health information), COPPA (children’s data), and Gramm/Leach/Bliley Act (regulated financial information), are exempt.

Consumer Request Response Window

Iowa: 90 days, which can be extended once by an additional 45 days when reasonably necessary.

Indiana: 45 days, which can be extended once by an additional 45 days when reasonably necessary.

Montana: 45 days, which can be extended once by an additional 45 days when reasonably necessary.

Tennessee: 45 days, which can be extended once by an additional 45 days when reasonably necessary.

Right to Appeal Consumer Request Response

Iowa: Right to appeal consumer right request decision, required to inform consumer within 60 days.

Indiana: Right to appeal consumer right request decision, required to inform consumer within 60 days.

Montana: Right to appeal consumer right request decision, required to inform consumer within 60 days.

Tennessee: Right to appeal consumer right request decision, required to inform consumer within 60 days.

Private Right of Action/Enforcement

None of the four laws gives a consumer a private right of action to enforce the laws.

Rulemaking

Will the state Attorney General adopt written regulations interpreting the new privacy law to assist covered businesses in understanding how to comply with the new law?

Iowa: No formal rulemaking.

Indiana: No formal rulemaking. Law allows the Indiana Attorney General to publish a list of resources for controllers (including sample privacy notices and disclosures) to assist controllers with compliance.

Montana: No formal rulemaking.

Tennessee: No formal rulemaking.

Other Provisions

Are there additional provisions that testing organizations need to know about?

Iowa: None

Indiana: None

Montana: Requires controllers to allow a consumer to opt out of any processing of the consumer's personal data for the purposes of targeted advertising, or any sale of such personal data, through an opt-out preference signal sent with the consumer's consent, to the controller by a platform, technology, or

mechanism that:

1. may not unfairly disadvantage another controller;
2. may not make use of a default setting, but require the consumer to make an affirmative, freely given and unambiguous choice to opt out of any processing of a customer's personal data;
3. must be consumer-friendly and easy to use by the average consumer;
4. must be consistent with any federal or state law or regulation; and
5. must allow the controller to accurately determine whether the consumer is a resident of the

state and whether the consumer has made a legitimate request to opt out of any sale of a consumer's personal data or targeted advertising.

Tennessee: A unique requirement in the Tennessee law states that a controller or processor shall create, maintain, and comply with a written privacy program that **reasonably 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." This is the first state law to include such a reference to the NIST Framework.

When a subsequent revision to the NIST privacy framework is published, a controller or processor shall reasonably conform its privacy program to the revised framework not later than one (1) year after the publication date stated in the most recent revision.