Indiana to Become the Seventh State to Pass Comprehensive Personal Privacy Law

Apr 27, 2023

Categories:

Blogs
Publications
Technology Blog

Authors:

Michael E. Nitardy
Jean Paul Yugo Nagashima
Brion St. Amour

On April 11, Indiana's state legislature passed a comprehensive state privacy legislation Senate Bill No. 5 (SB5), joining the ranks of California, Colorado, Connecticut, Iowa, Utah, and Virginia as a state with comprehensive state personal privacy law. Indiana's SB5 follows the trend set by Virginia's Consumer Data Protection Act in its scope of applicability, personal data rights, and controller-processor obligations. Once signed by the Indiana Governor, SB5 will take effect on January 1, 2026.

What Does SB5 Protect?

SB5 protects Indiana residents in an individual or household context, defining them as "Consumers." However, like Virginia, Colorado, Connecticut, Iowa, and Utah, the individuals acting in the employment or business-to-business context are not within the scope of consumers.

Like other state privacy laws, personal data under SB5 is defined as "information that is linked or reasonably linkable to an identified or identifiable natural person." But personal data does not include de-identified data, aggregate data, or publicly available data. This definition also follows the trend of Virginia, Colorado, Connecticut, Iowa, and Utah.

"Sale of personal data" is simply defined as the exchange of personal data for monetary consideration by the controller to a third party. This definition is narrower than the California Consumer Privacy Act/California Privacy Rights Act (CCPA/CPRA) and tracks the Virginia model of privacy protection.

Sensitive personal data is defined similarly to the CCPA/CPRA, covering racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, citizenship or immigration status, genetic or biometric data, precise geolocation data, and

FBT Gibbons

personal data of a child.

The Applicability of SB5 to Businesses

SB5 applies to:

- Person conducting business in the state of Indiana; or
- Produces products or services that are targeted to consumers who are residents of Indiana and during a calendar year does either of the following:
  - Controls or processes personal data of at least 100,000 consumers.
  - Controls or processes personal data of at least 25,000 customers and derives over fifty percent of gross revenue from the sale of personal data.

The threshold here is similar to other state privacy laws like Virginia, Colorado, Connecticut, Iowa, and Utah.

Exceptions to the Scope

Indiana has industry-sector-specific exceptions to the applicability of its state privacy law. These include exempting financial institutions subject to Gramm-Leach-Bliley Act (GLBA), persons subject to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH), nonprofits, and institutions of higher education.

Consumer Data Rights

Under SB5, consumers have similar rights to those states that have already implemented comprehensive state privacy laws. These include:

- Confirming whether or not a controller is processing personal data and access to that personal data;
- The right to correct inaccuracies in the consumer's personal data;

- The right to delete personal data;
- The right to data portability (with the exception of personal information subject to security breach protection); and
- The right to opt-out from targeted advertising, sale of personal data or profiling.

Controller's Responsibilities

SB5's controller obligations follow Virginia's approach. Specifically, SB5 requires the following responsibilities:

- Follow the data limitation principles and collect personal data that is adequate, relevant and reasonably necessary for the purpose of the processing;
- Establish reasonable, administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data.
- Not discriminating against consumers who exercise their consumer data rights.
- Not processing sensitive data unless the consumer provides consent, or in the case of a child's personal data, follow the consent process in accordance with Children's Online Privacy Protection Act.

Privacy Notice Requirements

Privacy Notice requirements for SB5 are similar to other state comprehensive privacy laws. Specifically, SB5 requires the privacy notice to disclose the following:

- The categories of personal data processed by the controller;
- Purpose of processing personal data;
- How consumers can exercise their data rights;
- Categories of personal data controller shares with third parties;
- The categories of third parties with whom the controller shares personal data; and

- Disclosure and the right to opt-out, if a controller sells personal data or engages in targeted advertising.

Under SB5, a controller is required to establish and describe reliable means for consumers to submit consumer rights requests. However, SB5 prohibits the controller from requiring the consumer to create a new account to exercise the consumer's rights.

Contractual Requirements Between Controller and Processor

SB5 requires the controller and the processor to enter a contract to govern the processor's data processing procedures. As with data protection requirements, controllers and processors must set forth the instructions for processing personal data, including the nature and purpose of processing, the type of data subject to processing, duration of the processing, and the rights and duties of both parties. In addition, the processing contract must include processor obligations very similar to those in the other state privacy laws. These include:

- Ensuring that each person processing personal data is subject to a duty of confidentiality with respect to the data;
- Obligating the processor to delete or return all personal data to the controller as requested by the controller at the end of the service;
- Making available information to demonstrate the processor's compliance with its obligations under SB5; and
- Allowing reasonable assessments by the controller or controller's designated assessor to review whether the processor is meeting its obligation to comply with the appropriate and accepted control standard for the technical and organizational measures.
- Requiring the processor to enter a written contract with a subprocessor and obligating the subprocessor to meet the same duties placed on the processor with respect to processing personal data.

No Private Right of Action

Like other state privacy laws, SB5 does not allow for a private right of action. This means enforcement is within the exclusive authority of the attorney general. In terms of enforcement, SB5 requires the attorney general to give 30 days' written notice identifying the provisions violated. If the controller or processor cures the violation, an enforcement action will not be initiated. However, if the violation is not cured, the attorney general may initiate an enforcement action. The civil penalties for such action may be up to $7500 for each violation.

Impact of the Bill

Companies in compliance with the other six state privacy laws will likely be in compliance with SB5.

For more information, please contact any other member of Frost Brown Todd's Data Privacy & Security practice group.

FBT Gibbons