Indiana Data Privacy Law Summary

On May 1, 2023, Governor Eric Holcomb (R) signed SB 5, the "Indiana Data Privacy Law". The Act's provisions take effect on January 1, 2026. A non-comprehensive summary of significant elements of the Act follows:

Covered Entities	The **Indiana Data Privacy Law** applies to a person that conduct business in the state or produces products or services that are targeted to residents of the state and during a calendar year: (a) controls or processes personal data of at least 100,000 consumers who are Indiana residents; or (b) controls or processes personal data of at least 25,000 consumers who are Indiana residents and derives more than 50% of gross revenue from the sale of personal data.
Covered Data	***"Personal data"***: information that is linked or reasonably linkable to an identified or identifiable individual. "Personal data" does not include de-identified data, aggregate data, or publicly available information. ***"Sensitive data"***: a category of personal data that includes any of the following: (a) personal data revealing racial or ethnic origin, religious beliefs, a mental or physical health diagnosis made by a healthcare provider, sexual orientation, or citizenship or immigration status; (b) genetic or biometric data that is processed for the purpose of uniquely identifying a specific individual; (c) personal data collected from a known child; (d) precise geolocation data.
Key Definitions	***"Consent"***: a clear affirmative act signifying a consumer's freely given, specific, informed, and unambiguous agreement to process personal data relating to the consumer. "Consent" may include a written statement, including a statement written by electronic means, or any other unambiguous affirmative action. ***"De-Identified Data"***: data that cannot reasonably be linked to an identified or identifiable individual because a controller that processes the data: (a) takes reasonable measures to ensure that the data cannot be associated with an individual; (b) publicly commits to maintaining and using the data without attempting to re-identify the data; and (c) obligates any recipients of the data through contractual requirements to comply with all applicable provisions. ***"Pseudonymous Data"***: personal data that cannot be attributed to a specific individual because additional information that would allow the data to be attributed to a specific individual is kept separately and subject to appropriate technical and organizational measures to ensure that the personal data is not attributed to an identified or identifiable individual. ***"Targeted Advertising"***: displaying an advertisement to a consumer in which 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. ***"Sale of Personal Data"***: the exchange of personal data for monetary consideration by a controller to a third party. "Sale of personal data" does not include: (a) the disclosure of personal data to a processor that processes the personal data on behalf of the controller; (b) the disclosure of personal data to a third party for purposes of providing a product or service requested by the consumer or the parent of a child to whom the personal data pertains; (c) the disclosure or transfer of personal information to an affiliate of the controller; (d) the disclosure of personal data in which the consumer intentionally made available to the general public via a channel of mass media and did not restrict to a specific audience; (e) the disclosure or transfer of personal data to a third party as an asset that is part of a proposed or actual merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the controller's assets.

Consumer Rights	• **Affirmative Consent**: Controllers are required to acquire affirmative consent for secondary uses (purposes that are neither reasonably necessary nor compatible with the disclosed purposes for processing) and processing sensitive data. • **Access**: A consumer has the right to confirm whether a controller is processing the consumer's personal data and, subject to certain set limitations, to access such personal data. • **Correction:** A consumer has the right to correct inaccuracies in the consumer's personal data that the consumer previously provided to a controller, taking into account the nature of the personal data and the purposes of the processing of the consumer's personal data. • **Deletion**: A consumer has the right to delete personal data provided by or obtained about the consumer. • **Portability:** A consumer has the right to obtain either: (a)a copy of or (b) a representative summary of the consumer's personal data that the consumer previously provided to the controller. Information provided to the consumer must be in a portable and, to the extent technically practicable, readily usable format that allows the consumer to transmit the data or summary to another controller without hindrance, in any case in which the processing is carried out by automated means. The controller has the discretion to send either a copy or a representative summary of the consumer's personal data, taking into account the nature of the personal data and the purposes of the processing of the consumer's personal data. • **Opt Out Rights**: A consumer has the right to opt out of the processing of the consumer's personal data for the purposes of targeted advertising, the sale of the consumer's personal data, or profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer.
Business Obligations	• **Responding to Consumer Requests**: A controller shall respond to a consumer without undue delay, but not later than 45 days of receipt of a request. The controller may extend the response period by 45 additional days when reasonably necessary, taking into account the complexity and number of the consumer's requests, provided the controller informs the consumer of the extension with the initial 45-day response period along with the reason for the extension. If a controller declines to act regarding the consumer's request, the controller shall inform the consumer without undue delay, but not later than 45 days after receipt of the request, of the justification for declining to act and provide instructions for how to appeal the decision. A consumer has the right to a free response once during any 12-month period. The controller bears the burden of demonstrating the manifestly unfounded, excessive, repetitive, or technically unfeasible nature of any denied requests and may charge the consumer a reasonable fee to cover such administrative costs or decline to act on such requests. A controller shall establish a process for a consumer to appeal the controller's refusal to take action on a request within a reasonable period of time after the consumer's receipt of the decision. The appeal process shall be conspicuously available and similar to the process for submitting requests to initiate action pursuant to this section. Within 60 days of receipt of an appeal, a controller shall inform the consumer in writing of any action taken in response to the appeal and provide the consumer with an online mechanism, if available, or other method through which the consumer may contact the attorney general to submit a complaint. • **Data Minimization**: A controller shall limit the collection of personal data to what is adequate, relevant, and reasonably necessary in relation to the purposes for which such data is processed, as disclosed to the consumer. • **Avoid Secondary Use**: A controller shall 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 controller obtains the consumer's consent. • **Data Security**: A controller shall establish, implement, and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data appropriate to the volume and nature of the personal data at issue. • **No Unlawful Discrimination:** A controller shall not process personal data in violation of state and federal laws that prohibit unlawful discrimination against consumers. A controller shall not

	discriminate against a consumer for exercising any consumer rights. • **Transparency**: A controller shall provide consumers with a reasonably accessible, clear, and meaningful privacy notice that includes: (a) the categories of personal data processed by the controller; (b) the purpose for processing personal data; (c) how consumers may exercise their consumer rights, including how a consumer may appeal a controller's decision with regard to the consumer's request; (d) the categories of personal data that the controller shares with third parties, if any; (d) the categories of third parties, if any, with whom the controller shares personal data. • **Purpose Specification:** A controller shall not process personal data for purposes other than those expressly listed unless otherwise allowed by this article Personal data processed by a controller may be processed to the extent that the processing is: (a) reasonably necessary and proportionate and (b) adequate, relevant, and limited to what is necessary in relation to the specific listed purposes. • **Disclosure**: A controller shall clearly and conspicuously disclose if the controller sells personal data to third parties or uses the consumer's personal data for targeted advertising in addition to the manner in which a consumer may exercise the right to opt out of such activity.
Data Protection Impact Assessments	A controller shall conduct and document a data protection impact assessment for each of the following processing activities: (a) the processing of personal data for the purposes of targeted advertising; (b) the sale of personal data; (c) the processing of personal data for the purposes of profiling in which the profiling presents a reasonably foreseeable risk of: (i) unfair or deceptive treatment of unlawful disparate impact on consumers; (ii) financial, physical or reputational injury to consumers; (iii) a physical or other form of intrusion on the solitude or seclusion or the private affairs or concerns of consumers in which the intrusion would be offensive to a reasonable person, or; (iv) other substantial injury to consumers, and; (d) the processing of sensitive data. Data protection assessments must identify and weigh the benefits that may flow, directly and indirectly, from the processing to 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 the safeguards that can be employed by the controller to reduce the risks. The use of de-identified data and the reasonable expectations of consumers, as well as the context of the processing and the relationship between the controller and the consumer, must be factored into this assessment. The attorney general may require that a controller disclose any data protection assessment that is relevant to an investigation being conducted by the attorney general and reporter and the controller shall make assessment available. The attorney general may evaluate the assessment for compliance. Data protection assessments are confidential and exempt from public inspection and copying.
Controller / Processor Distinction	• **A processor shall adhere to the instructions of a controller and assist the controller** in meeting its obligations to include: (a) assisting the controller in meeting the controller's obligation to respond to consumer requests by appropriate technical and organizational measures insofar as this is reasonably practicable, and taking into account the nature of processing and the information available to the processor; (b) taking into account the nature of processing and the information available to the processor, assisting the controller in meeting the controller's obligations in relation to the security of processing the personal data and the notification of a breach of security of the system of the processor in order to meet the controller's obligations; and (c) providing necessary information to enable the controller to conduct and document data protection impact assessments. • A contract between a controller and a processor shall govern the processor's data processing procedures. The contract is binding and shall 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. The contract must also require that the processor: (a) ensure that each individual processing personal data is subject to a duty of confidentiality; (b) at the controller's direction, delete or return all personal data to the controller as requested at the end of the provision of services, unless retention of the personal data is required by law; (c) upon the reasonable request of the controller, make available to the controller all information in its possession

	necessary to demonstrate the processor's compliance with obligations; (d) allow, and cooperate with reasonable assessments by the controller or the controller's designated assessor, or the processor may arrange for a qualified and independent assessor to conduct an assessment of the processor's policies and technical organization measures in support of the obligations using an appropriate and accepted control standard or framework and assessment procedure for such assessments; a processor shall provide a report of each assessment upon controller request; and (e) engage a subcontractor pursuant to a written contract that requires the subcontractor to meet the obligations of the processor with respect to the personal data.
Exceptions and Exemptions	• A controller may disclose pseudonymous data or de-identified data with an exercise of reasonable oversight to monitor compliance with any contractual commitments and shall take appropriate steps to address any breaches of those contractual commitments. • The Indiana Data Privacy Law shall not be construed to restrict a controller's or processor's ability to: (a) comply with laws; (b) comply with inquiries by government authorities; (c) cooperate with law-enforcement agencies; (d) prepare for and defend legal claims; (e) provide a product or service requested by a consumer; (f) perform a contract to which the consumer, or a parent of a child, is a party, including fulfilling the terms of a written warranty, or take steps at the request of the consumer or parent before entering into a contract; (g) take immediate steps to protect an interest that is essential for the life or physical safety of the consumer or another individual if the processing cannot be manifestly based on another legal basis; (i) prevent, detect, protect against, or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities, or any illegal activity, investigate, report or prosecute those responsible for any such action, and preserve the integrity or security of systems; (j) engage in public or peer-reviewed scientific or statistical research in the public interest that adheres to all other applicable ethics and privacy laws and is approved, monitored or governed by an institutional review board or a similar independent oversight entity; (k) assist another controller, processor, or third party with obligations. • Data exempt from the Indiana Data Privacy Law includes: nonprofit organizations, institutions of higher education, protected information under HIPAA, the Health Care Quality Improvement Act of 1986, the Patient Safety and Quality Improvement Act, the Fair Credit Reporting Act, the Driver's Privacy Protection Act of 1994, FERPA, the Farm Credit Act, and COPPA.
Enforcement	• The Indiana Data Privacy Law does not provide the basis for a private right of action to violations of this Act. The attorney general has exclusive authority to enforce the Indiana Data Privacy Law. • **Right to Cure**: The attorney general may initiate an action and seek an injunction and a civil penalty not to exceed $7,500 per violation. Before initiating any action, the attorney general shall provide a controller or processor 30 days' written notice identifying specific provisions being violated. The right to cure does not sunset.