First Regular Session of the 123rd General Assembly (2023)

PRINTING CODE. Amendments: Whenever an existing statute (or a section of the Indiana Constitution) is being amended, the text of the existing provision will appear in this style type, additions will appear in **this style type**, and deletions will appear in ~~this style type.~~

Additions: Whenever a new statutory provision is being enacted (or a new constitutional provision adopted), the text of the new provision will appear in **this style type**. Also, the word **NEW** will appear in that style type in the introductory clause of each SECTION that adds a new provision to the Indiana Code or the Indiana Constitution.

Conflict reconciliation: Text in a statute in *this style type* or ~~*this style type*~~ reconciles conflicts between statutes enacted by the 2022 Regular Session of the General Assembly.

SENATE ENROLLED ACT No. 5

AN ACT to amend the Indiana Code concerning trade regulation.

Be it enacted by the General Assembly of the State of Indiana:

SECTION 1. IC 24-15 IS ADDED TO THE INDIANA CODE AS A **NEW** ARTICLE TO READ AS FOLLOWS [EFFECTIVE JANUARY 1, 2026]:

ARTICLE 15. CONSUMER DATA PROTECTION

Chapter 1. Applicability

Sec. 1. (a) This article 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 derives more than fifty percent (50%) of gross revenue from the sale of personal data.

(b) This article does not apply to any of the following:

(1) Either of the following:

(A) The state, a state agency, or a body, authority, board, bureau, commission, district, or agency of any political subdivision of the state.

(B) A third party under contract with an entity described in clause (A), when acting on behalf of the entity. This clause does not exempt data held or created by third

parties outside of the scope of the contract with the entity.

(2) Any financial institutions and affiliates, or data subject to Title V of the federal Gramm-Leach-Bliley Act (15 U.S.C. 6801 et seq.).

(3) Any covered entity or business associate governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services (45 CFR Parts 160 and 164) pursuant to HIPAA.

(4) Any nonprofit organization.

(5) Any institution of higher education.

(6) Any public utility (as defined in IC 8-1-2-1(a)) or service company affiliated with a public utility (as defined in IC 8-1-2-1(a)). For purposes of this subdivision, "service company" means an associate company within a holding company system organized specifically for the purpose of providing goods or services to a public utility (as defined in IC 8-1-2-1(a)) in the same holding company system.

Sec. 2. The following information and data are exempt from this article:

(1) Protected health information under HIPAA and related regulations under 45 CFR Part 160, 45 CFR Part 162, and 45 CFR Part 164.

(2) Patient identifying information for purposes of 42 U.S.C. 290dd-2.

(3) Any of the following:

(A) Identifiable private information for purposes of the federal policy for the protection of human subjects under 45 CFR Part 46.

(B) Identifiable private information that is otherwise information collected as part of human subjects research under the good clinical practice guidelines issued by the International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use.

(C) The protection of human subjects under 21 CFR Parts 50 and 56.

(D) Personal data used or shared in research conducted in accordance with the requirements set forth in this article.

(E) Other research conducted in accordance with applicable law.

(4) Information and documents created for purposes of the federal Health Care Quality Improvement Act of 1986 (42 U.S.C. 11101 et seq.).

(5) Patient safety work product for purposes of the federal Patient Safety and Quality Improvement Act (42 U.S.C. 299b-21 et seq.).

(6) Information derived from any of the health care related information set forth in this section that is de-identified in accordance with the requirements for de-identification under HIPAA.

(7) Information:

(A) originating from;

(B) intermingled with so as to be indistinguishable from; or

(C) treated in the same manner as;

information that is exempt under this section and that is maintained by a covered entity or business associate, as defined in HIPAA, or a program or qualified service organization under 42 U.S.C. 290dd-2.

(8) Information used only for public health activities and purposes, as authorized by HIPAA.

(9) The collection, maintenance, disclosure, sale, communication, or use of any personal information bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living by:

(A) a consumer reporting agency, furnisher, or user that provides information for use in a consumer report; or

(B) a user of a consumer report;

but only to the extent that such activity is regulated by and authorized under the federal Fair Credit Reporting Act (15 U.S.C. 1681 et seq.).

(10) Personal data collected, processed, sold, or disclosed in compliance with the federal Driver's Privacy Protection Act of 1994 (18 U.S.C. 2721 et seq.).

(11) Personal data regulated by the federal Family Educational Rights and Privacy Act (20 U.S.C. 1232g et seq.).

(12) Personal data collected, processed, sold, or disclosed in compliance with the federal Farm Credit Act (12 U.S.C. 2001 et seq.).

(13) Data processed or maintained:

(A) in the course of an individual applying to, 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 emergency contact information for an individual

under this article and used for emergency contact purposes; or

(C) that is necessary to retain to administer benefits for another individual relating to the individual under clause (A) and used for the purposes of administering those benefits.

Sec. 3. A:

(1) controller; or

(2) processor;

that complies with the Children's Online Privacy Protection Act (15 U.S.C. 6501 et seq.), and with any rules or regulations under that act, satisfies any obligation to obtain parental consent under this article.

Chapter 2. Definitions

Sec. 0.5. The definitions in this chapter apply throughout this article.

Sec. 1. (a) "Affiliate" means a legal entity that:

(1) controls, is controlled by, or is under common control with another legal entity; or

(2) shares common branding with another legal entity.

(b) For purposes of this section, "control", with respect to a company, means:

(1) ownership of, or the power to vote, more than fifty percent (50%) of the outstanding shares of any class of voting security of the company;

(2) control in any manner over the election of a majority of the directors or of individuals exercising similar functions; or

(3) the power to exercise controlling influence over the management of the company.

Sec. 2. "Aggregate data" means information:

(1) that relates to a group or category of consumers;

(2) from which individual consumer identities have been removed; and

(3) that is not linked or reasonably linkable to any consumer.

Sec. 3. "Authenticate" means to verify through reasonable means that a consumer who is entitled to exercise the personal data rights provided by IC 24-15-3 is the same consumer exercising such rights with respect to particular personal data.

Sec. 4. (a) "Biometric data" means data that:

(1) is generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, a voiceprint, images of the retina or iris, or other unique biological

patterns or characteristics; and

(2) is used to identify a specific individual.

(b) The term does not include:

(1) a physical or digital photograph, or data generated from a physical or digital photograph;

(2) a video or audio recording, or data generated from a video or audio recording; or

(3) information collected, used, or stored for health care treatment, payment, or operations under HIPAA.

Sec. 5. "Business associate" has the meaning set forth in 45 CFR 160.103.

Sec. 6. "Child" means any individual who is less than thirteen (13) years of age.

Sec. 7. (a) "Consent" means a clear affirmative act that signifies a consumer's freely given, specific, informed, and unambiguous agreement to process personal data relating to the consumer.

(b) For purposes of this section, a "clear affirmative act" includes a written statement, including a statement written by electronic means, or any other unambiguous affirmative action.

Sec. 8. (a) "Consumer" means an individual who:

(1) is a resident of Indiana; and

(2) is acting only for a personal, family, or household purpose.

(b) The term does not include an individual acting in a commercial or employment context.

Sec. 9. "Controller" means a person that, alone or jointly with others, determines the purpose and means of processing personal data.

Sec. 10. "Covered entity" has the meaning set forth in 45 CFR 160.103.

Sec. 11. "Decision that produces legal or similarly significant effects concerning a consumer" means a decision made by a controller that results in the provision or denial by the controller of:

(1) financial and lending services;

(2) housing;

(3) insurance;

(4) education enrollment;

(5) criminal justice;

(6) employment opportunities;

(7) health care services; or

(8) access to basic necessities, such as food and water.

Sec. 12. "De-identified data" means data that cannot reasonably

be linked to an identified or identifiable individual because a controller that possesses the data:

(1) takes reasonable measures to ensure that the data cannot be associated with an individual;

(2) publicly commits to maintaining and using the data without attempting to re-identify the data; and

(3) obligates any recipients of the data through contractual requirements to comply with all applicable provisions of this article.

Sec. 13. "Health care provider" has the meaning set forth in IC 4-6-14-2.

Sec. 14. "Health record" has the meaning set forth in IC 1-1-4-5(a)(6).

Sec. 15. "HIPAA" refers to the federal Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. 1320d et seq.).

Sec. 16. "Identified or identifiable individual" means an individual who can be readily identified, directly or indirectly.

Sec. 17. "Institution of higher education" means a public or private college or university.

Sec. 18. "Nonprofit organization" means any organization exempt from taxation under Section 501(c)(3), 501(c)(6), or 501(c)(12) of the Internal Revenue Code.

Sec. 19. (a) "Personal data" means information that is linked or reasonably linkable to an identified or identifiable individual.

(b) The term does not include:

(1) de-identified data;

(2) aggregate data; or

(3) publicly available information.

Sec. 20. (a) "Precise geolocation data" means information derived from technology, including global positioning system level latitude and longitude coordinates, that directly identifies the specific location of a natural person with precision and accuracy within a radius of one thousand seven hundred fifty (1,750) feet.

(b) The term does not include:

(1) the content of communications; or

(2) any data generated by or connected to advanced utility metering infrastructure systems or equipment for use by a utility.

Sec. 21. "Processing", with respect to personal data, means any operation or set of operations performed, whether by manual or automated means, on personal data or on sets of personal data,

such as the collection, use, storage, disclosure, analysis, deletion, or modification of personal data.

Sec. 22. "Processor" means a person that processes personal data on behalf of a controller.

Sec. 23. "Profiling" means any form of solely automated processing performed on personal data to evaluate, analyze, or predict personal aspects related to an identified or identifiable individual's economic situation, health or health records, personal preferences, interests, reliability, behavior, location, or movements.

Sec. 24. "Protected health information" has the meaning set forth in 45 CFR 160.103.

Sec. 25. "Pseudonymous data" means 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:

(1) kept separately; and

(2) subject to appropriate technical and organizational measures;

to ensure that the personal data is not attributed to an identified or identifiable individual.

Sec. 26. "Publicly available information" means information:

(1) that is lawfully made available through federal, state, or local government records; or

(2) that a business has a reasonable basis to believe is lawfully made available:

(A) to the general public through widely distributed media;

(B) by the consumer to whom the information pertains; or

(C) by a person to whom the consumer has disclosed the information;

unless the consumer has restricted the information to a specific audience.

Sec. 27. (a) "Sale of personal data" means the exchange of personal data for monetary consideration by a controller to a third party.

(b) The term does not include:

(1) the disclosure of personal data to a processor that processes the personal data on behalf of the controller;

(2) the disclosure of personal data to a third party for purposes of providing a product or service requested by:

(A) the consumer; or

(B) the parent of a child;

to whom the personal data pertains;

(3) the disclosure or transfer of personal data to an affiliate of the controller;

(4) the disclosure of information that the consumer:

(A) intentionally made available to the general public via a channel of mass media; and

(B) did not restrict to a specific audience; or

(5) 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.

Sec. 28. "Sensitive data" means a category of personal data that includes any of the following:

(1) Personal data revealing racial or ethnic origin, religious beliefs, a mental or physical health diagnosis made by a health care provider, sexual orientation, or citizenship or immigration status.

(2) Genetic or biometric data that is processed for the purpose of uniquely identifying a specific individual.

(3) Personal data collected from a known child.

(4) Precise geolocation data.

Sec. 29. "State agency" has the meaning set forth in IC 1-1-15-3.

Sec. 30. (a) "Targeted advertising" means the displaying of 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 the consumer's preferences or interests.

(b) The term does not include:

(1) advertisements based on activities within a controller's own or affiliated websites or online applications;

(2) advertisements based on the context of a consumer's current search query, visit to a website, or online application;

(3) advertisements directed to a consumer in response to the consumer's request for information or feedback; or

(4) the processing of personal data solely for measuring or reporting advertising performance, reach, or frequency.

Sec. 31. "Third party", with respect to a context to which this article applies, means a natural or legal person, public authority, agency, or body other than:

(1) the consumer;

(2) the controller;

(3) the processor; or

(4) an affiliate of the processor or the controller.

Sec. 32. "Trade secret" has the meaning set forth in IC 24-2-3-2.

Chapter 3. Personal Data; Consumer Rights

Sec. 1. (a) A consumer may invoke one (1) or more rights set forth in subsection (b) by submitting to a controller a request specifying the rights the consumer wishes to invoke. A known child's parent or legal guardian may invoke on behalf of the child one (1) or more rights set forth in subsection (b) with respect to the processing of personal data belonging to the known child by submitting to a controller a request specifying the rights the consumer wishes to invoke on behalf of the child. Except as provided in IC 24-15-7-1(c) and IC 24-15-7-2, and subject to any limitations or conditions set forth in subsections (b) and (c), a controller shall comply with an authenticated consumer request to exercise a right set forth in subsection (b).

(b) A consumer has the following rights:

(1) To confirm whether or not a controller is processing the consumer's personal data and, subject to the limitations set forth in subdivision (4), to access such personal data.

(2) 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. Upon receiving a request from a consumer under this subdivision, a controller shall correct inaccurate information as requested by the consumer, taking into account the nature of the personal data and the purposes of the processing of the consumer's personal data.

(3) To delete personal data provided by or obtained about the consumer.

(4) 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 a consumer under this subdivision 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 under this

subdivision, taking into account the nature of the personal data and the purposes of the processing of the consumer's personal data. A controller is not required to provide a copy or a representative summary of a consumer's personal data to the same consumer under this subdivision more than one (1) time in a twelve (12) month period.

(5) To opt out of the processing of the consumer's personal data for purposes of:

(A) targeted advertising;

(B) the sale of personal data; or

(C) profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer.

(c) Except as otherwise provided in this article, a controller shall comply with a request by a consumer to exercise a consumer right set forth in subsection (b) as follows:

(1) A controller shall respond to the consumer without undue delay, but in any case not later than forty-five (45) days after receipt of the consumer's request under this section. The response period prescribed by this subdivision may be extended once by an additional forty-five (45) days when reasonably necessary, taking into account the complexity and number of the consumer's requests, as long as the controller informs the consumer of any such extension within the initial forty-five (45) day response period, along with the reason for the extension.

(2) If a controller declines to take action regarding the consumer's request, the controller shall inform the consumer without undue delay, but in any case not later than forty-five (45) days after receipt of the consumer's request under this section, of the justification for declining to take action, and shall provide instructions for how to appeal the decision under subsection (d).

(3) Information provided in response to a consumer request shall be provided by a controller free of charge, up to one (1) time annually per consumer. If requests from a consumer are manifestly unfounded, excessive, or repetitive, the controller may charge the consumer a reasonable fee to cover the administrative costs of complying with the request or decline to act on the request. The controller bears the burden of demonstrating the manifestly unfounded, excessive, or repetitive nature of the request.

(4) If a controller is unable to authenticate the request using

commercially reasonable efforts, the controller shall not be required to comply with a request to initiate an action under this section and may request that the consumer provide additional information reasonably necessary to authenticate the consumer and the consumer's request.

(5) A controller that has obtained personal data about a consumer from a source other than the consumer is considered to comply with a request by the consumer under subsection (b)(3) to delete the consumer's personal data if the controller:

(A) retains:

(i) a record of the consumer's request for deletion; and

(ii) the minimum data necessary to ensure that the consumer's personal data remains deleted from the controller's records; and

(B) does not use the data retained under clause (A)(ii) for any other purpose.

(d) A controller shall establish a process for a consumer to appeal, within a reasonable period of time after the consumer's receipt of a decision by the controller under subsection (c)(2), the controller's refusal to take action on a request by the consumer under this section. The appeal process shall be conspicuously available and similar to the process for submitting requests to invoke a right under this section. Not later than sixty (60) days after receipt of an appeal, a controller shall inform the consumer in writing of any action taken or not taken in response to the appeal, including a written explanation of the reasons for the decisions. If the appeal is denied, the controller shall also 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.

Chapter 4. Data Controller Responsibilities; Transparency

Sec. 1. Except as provided in IC 24-15-7-2, a controller has the following responsibilities:

(1) 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.

(2) Except as otherwise provided in this article, 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.

(3) 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. The data security practices required under this subdivision must be appropriate to the volume and nature of the personal data at issue.

(4) 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 of the consumer rights set forth in this article, including by denying goods or services to the consumer, charging different prices or rates for goods and services, or providing a different level or quality of goods or services to the consumer. However, nothing in this subdivision shall be construed to:

(A) require a controller to provide a product or service that requires the personal data of a consumer that the controller does not collect or maintain; or

(B) prohibit a controller from offering a different price, rate, level, quality, or selection of goods or services to a consumer, including offering goods or services for no fee, if the consumer has exercised the consumer's right to opt out under IC 24-15-3-1(b)(5) or if the offer is related to a consumer's voluntary participation in a bona fide loyalty, rewards, premium features, discount, or club card program.

(5) A controller shall not process sensitive data concerning a consumer without obtaining the consumer's consent, or, in the case of the processing of sensitive data concerning a known child, without processing such data in accordance with the federal Children's Online Privacy Protection Act (15 U.S.C. 6501 et seq.).

Sec. 2. Any provision of a contract or agreement of any kind that purports to waive or limit in any way a consumer's rights under IC 24-15-3 is contrary to public policy and is void and unenforceable.

Sec. 3. A controller shall provide consumers with a reasonably accessible, clear, and meaningful privacy notice that includes:

(1) the categories of personal data processed by the controller;

(2) the purpose for processing personal data;

(3) how consumers may exercise their consumer rights under

IC 24-15-3, including how a consumer may appeal a controller's decision with regard to the consumer's request;

(4) the categories of personal data that the controller shares with third parties, if any; and

(5) the categories of third parties, if any, with whom the controller shares personal data.

Sec. 4. If a controller sells a consumer's personal data to third parties or uses a consumer's personal data for targeted advertising, the controller shall clearly and conspicuously disclose such activity, as well as the manner in which a consumer may exercise the right to opt out of such sales or use.

Sec. 5. A controller shall establish, and shall describe in a privacy notice provided under section 3 of this chapter, one (1) or more secure and reliable means for consumers to submit a request to exercise their rights under IC 24-15-3. Such means must take into account:

(1) the ways in which consumers normally interact with the controller;

(2) the need for the secure and reliable communication of such requests; and

(3) the ability of the controller to authenticate the identity of the consumer making the request.

A controller may not require a consumer to create a new account in order to exercise the consumer's rights under IC 24-15-3 but may require a consumer to use an existing account.

Sec. 6. The attorney general may maintain on the attorney general's website a list of resources for controllers, including sample privacy notices and disclosures, to assist controllers in complying with this chapter.

Chapter 5. Responsibility According to Role; Controllers and Processors

Sec. 1. A processor shall adhere to the instructions of a controller and shall assist the controller in meeting its obligations under this chapter. Such assistance shall include the following:

(1) Assisting the controller in meeting the controller's obligation to respond to consumer requests under IC 24-15-3 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.

(2) 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:

(A) the security of processing the personal data; and

(B) the notification of a breach of security of the system of the processor under IC 24-4.9;

in order to meet the controller's obligations.

(3) Providing necessary information to enable the controller to conduct and document data protection impact assessments under IC 24-15-6.

Sec. 2. (a) 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. The contract must be binding and clearly set forth instructions for processing personal 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 include requirements that the processor do the following:

(1) Ensure that each individual processing personal data is subject to a duty of confidentiality with respect to the data.

(2) 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.

(3) 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 the obligations in this chapter.

(4) Allow, and cooperate with, reasonable assessments by the controller or the controller's designated assessor. Alternatively, the processor may arrange for a qualified and independent assessor to conduct an assessment of the processor's policies and technical and organizational measures in support of the processor's obligations under this chapter using an appropriate and accepted control standard or framework and assessment procedure for such assessments. The processor shall provide a report of any such assessment to the controller upon request.

(5) Subject to subsection (b), engage any subcontractor pursuant to a written contract that requires the subcontractor to meet the obligations of the processor with respect to the personal data.

(b) Nothing in this section shall be construed to relieve a controller or a processor from the liabilities imposed on the

controller or processor by virtue of its role in the processing relationship.

Sec. 3. Determining whether a person is acting as a controller or a processor with respect to a specific processing of data is a fact based determination that depends upon the context in which personal data is processed. A processor that continues to adhere to a controller's instructions with respect to a specific processing of personal data remains a processor.

Chapter 6. Data Protection Impact Assessments

Sec. 1. (a) The data protection impact assessment requirements set forth in this chapter apply to processing activities created or generated after December 31, 2025, and are not retroactive to any processing activities created or generated before January 1, 2026.

(b) A controller shall conduct and document a data protection impact assessment of 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 a reasonably foreseeable risk of:

(A) unfair or deceptive treatment of, or unlawful disparate impact on, consumers;

(B) financial, physical, or reputational injury to consumers;

(C) a physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of consumers, if such intrusion would be offensive to a reasonable person; or

(D) other substantial injury to consumers.

(4) The processing of sensitive data.

(5) Any processing activities involving personal data that present a heightened risk of harm to consumers.

(c) Data protection impact assessments conducted under this chapter shall 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 such processing, as mitigated by safeguards that can be employed by the controller to reduce such 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

whose personal data will be processed, shall be factored into this assessment by the controller.

(d) A single data protection impact assessment may address a comparable set of processing operations that include similar activities.

(e) A data protection impact assessment conducted by a controller for the purpose of compliance with other laws or regulations may be used to comply with this section if the assessment has a reasonably comparable scope and effect to an assessment conducted under this section.

Sec. 2. (a) The attorney general may request, pursuant to a civil investigative demand, that a controller disclose any data protection impact assessment that is relevant to an investigation conducted by the attorney general. Upon receipt of such a request, the controller shall make the data protection impact assessment available to the attorney general. Subject to subsection (b), the attorney general may evaluate the data protection impact assessment for a controller's compliance with the responsibilities set forth in IC 24-15-4.

(b) Data protection impact assessments are confidential and exempt from public inspection and copying under IC 5-14-3-4. The disclosure of a data protection impact assessment pursuant to a request from the attorney general does not constitute a waiver of attorney-client privilege or work product protection with respect to the assessment and any information contained in the assessment.

Chapter 7. Processing De-identified Data or Pseudonymous Data; Exemptions

Sec. 1. (a) A controller in possession of de-identified data shall:

(1) take reasonable measures to ensure that the data cannot be associated with an individual;

(2) publicly commit to maintaining and using de-identified data without attempting to re-identify the data; and

(3) contractually obligate any recipients of the de-identified data to comply with all provisions of this chapter.

(b) This chapter shall not be construed to require a controller or processor to:

(1) re-identify de-identified data or pseudonymous data;

(2) maintain data in identifiable form; or

(3) collect, obtain, retain, or access any data or technology;

in order to be capable of associating an authenticated consumer request with personal data.

(c) This chapter shall not be construed to require a controller or

processor to comply with a request of a consumer under IC 24-15-3 if all of the following conditions are met:

(1) The controller is not reasonably capable of associating the request with the personal data or it would be unreasonably burdensome for the controller to associate the request with the personal data.

(2) The controller does not use the personal data to recognize or respond to the specific consumer who is the subject of the personal data, or associate the personal data with other personal data about the same specific consumer.

(3) The controller does not sell the personal data to any third party or otherwise voluntarily disclose the personal data to any third party other than a processor.

Sec. 2. The:

(1) rights of a consumer set forth in IC 24-15-3-1(b)(1) through IC 24-15-3-1(b)(4); and

(2) responsibilities of a controller under IC 24-15-4-1(1) through IC 24-15-4-1(5);

do not apply to pseudonymous data in any case in which the controller is able to demonstrate that any information necessary to identify the consumer is kept separately and is subject to effective technical and organizational controls that prevent the controller from accessing such information.

Sec. 3. A controller that discloses pseudonymous data or de-identified data shall exercise reasonable oversight to monitor compliance with any contractual commitments to which the pseudonymous data or de-identified data is subject and shall take appropriate steps to address any breaches of those contractual commitments.

Chapter 8. Limitations

Sec. 1. (a) This article shall not be construed to restrict a controller's or processor's ability to do any of the following:

(1) Comply with federal, state, or local laws, rules, or regulations or, in the case of an owner of a riverboat licensed under IC 4-33-6, implement and operate a facial recognition program approved by the Indiana gaming commission.

(2) Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by a federal, state, local, or other governmental authority.

(3) Cooperate with law enforcement agencies concerning conduct or activity that the controller or processor reasonably and in good faith believes may violate federal, state, or local

laws, rules, or regulations.

(4) Investigate, establish, exercise, prepare for, or defend legal claims.

(5) Provide a product or service specifically requested by a consumer, 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.

(6) Take immediate steps to protect an interest that is essential for the life or physical safety of the consumer or of another individual, if the processing cannot be manifestly based on another legal basis.

(7) 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.

(8) Engage in public or peer reviewed scientific or statistical research that is in the public interest and that adheres to all applicable ethics and privacy laws and is approved, monitored, and governed by an institutional review board, or a similar independent oversight entity, that determines if:

(A) the information is likely to provide substantial benefits that do not exclusively accrue to the controller;

(B) the expected benefits of the research outweigh the privacy risks; and

(C) the controller has implemented reasonable safeguards to mitigate privacy risks associated with research, including any risks associated with re-identification.

(9) Assist another controller, processor, or third party with any obligation described in this section.

(b) Processing personal data for a purpose expressly identified in subsection (a)(1) through (a)(9) does not by itself make a person a controller with respect to such processing.

Sec. 2. The obligations imposed on a controller or a processor under this article do not prohibit or restrict a controller or processor from collecting, using, or retaining data to do the following:

(1) Conduct internal research to develop, improve, or repair products, services, or technology.

(2) Effectuate a product recall.

(3) Identify and repair technical errors that impair existing or

intended functionality.

(4) Perform internal operations that are:

(A) reasonably compatible with the expectations of the consumer;

(B) reasonably anticipated based on the consumer's existing relationship with the controller; or

(C) otherwise compatible with:

(i) processing data in furtherance of the provision of a product or service specifically requested by a consumer, or the parent of a child; or

(ii) the performance of a contract to which the consumer is a party.

Sec. 3. The obligations imposed on a controller or a processor under this article do not apply if compliance by the controller or processor with this article would violate an evidentiary privilege under Indiana law. This article shall not be construed to prohibit a controller or processor from providing, as part of a privileged communication, personal data concerning a consumer to a person covered by an evidentiary privilege under Indiana law.

Sec. 4. A controller or processor that discloses personal data to a third party controller or processor in compliance with this article is not in violation of this article if the third party controller or processor that receives and processes the personal data violates this article, as long as, at the time of disclosing the personal data, the disclosing controller or processor did not have actual knowledge that the recipient intended to commit a violation. A third party controller or processor receiving personal data from a controller or processor is likewise not in violation of this article solely because of the transgressions of the controller or processor from which it receives such personal data.

Sec. 5. This article:

(1) shall not be construed as an obligation imposed on controllers and processors that adversely affects the rights or freedoms of any persons, such as exercising the right of free speech under the First Amendment to the Constitution of the United States; and

(2) does not apply to personal data in the context of a purely personal or household activity.

Sec. 6. Nothing in this article shall be construed as requiring a controller to disclose trade secrets.

Sec. 7. (a) Personal data processed by a controller for a purpose authorized under this chapter may not be processed for any other

purpose unless otherwise allowed under this article. Personal data processed by a controller under this chapter may be processed to the extent that such processing is:

(1) reasonably necessary and proportionate to a purpose authorized under this chapter; and

(2) adequate, relevant, and limited to what is necessary in relation to the specific purpose.

(b) Personal data collected, used, or retained under section 2 of this chapter:

(1) shall, as applicable, take into account the nature and purpose of the collection, use, or retention; and

(2) must be subject to reasonable administrative, technical, and physical measures to:

(A) protect the confidentiality, integrity, and accessibility of the personal data; and

(B) reduce reasonably foreseeable risks of harm to consumers relating to such collection, use, or retention of the personal data.

(c) If a controller processes personal data pursuant to an exemption under this chapter, the controller bears the burden of demonstrating that such processing:

(1) qualifies for the exemption; and

(2) complies with the requirements set forth in this section.

Chapter 9. Investigative Authority

Sec. 1. Whenever the attorney general has reasonable cause to believe that any person has engaged in, is engaging in, or is about to engage in any violation of this article, the attorney general is empowered to issue a civil investigative demand to investigate the suspected violation.

Chapter 10. Enforcement

Sec. 1. The attorney general has exclusive authority to enforce the provisions of this article.

Sec. 2. (a) The attorney general may initiate an action in the name of the state and may seek an injunction to restrain any violations of this article and a civil penalty not to exceed seven thousand five hundred dollars ($7,500) for each violation under this article.

(b) The attorney general may recover reasonable expenses incurred in investigating and preparing the case, including attorney's fees, in any action initiated under this chapter.

Sec. 3. (a) Before initiating an action under section 2 of this chapter, the attorney general shall provide a controller or

processor thirty (30) days written notice identifying the specific provisions of this article that the attorney general alleges have been or are being violated. If within the thirty (30) day period set forth in this section, the controller or processor:

(1) cures the alleged violation; and

(2) provides the attorney general an express written statement that:

(A) the alleged violation has been cured; and

(B) actions have been taken to ensure no further such violations will occur;

the attorney general shall not initiate an action against the controller or processor.

(b) If a controller or processor:

(1) continues the alleged violation following the thirty (30) day period set forth in subsection (a); or

(2) breaches an express written statement provided to the attorney general under subsection (a)(2);

the attorney general may initiate an action under section 2 of this chapter.

Sec. 4. Nothing in this article shall be construed as providing the basis for a private right of action for violations of this article or any other law.

Chapter 11. Preemption; Other Laws

Sec. 1. This article supersedes and preempts all rules, regulations, codes, ordinances, and other laws adopted by a city, county, city and county, municipality, or local agency regarding the processing of personal data by controllers or processors.

Sec. 2. Any reference to federal, state, or local law or statute in this article includes any accompanying rules, regulations, or exemptions.

SECTION 2. [EFFECTIVE UPON PASSAGE] **(a) As used in this SECTION, "controller" has the meaning set forth in IC 24-15-2-9, as added by this act.**

(b) The attorney general may, not later than December 31, 2025, establish on the attorney general's website a list of resources for controllers, including sample privacy notices and disclosures, to assist controllers in complying with IC 24-15-4, as added by this act.

(c) This SECTION expires July 1, 2026.

SECTION 3. **An emergency is declared for this act.**

President of the Senate

President Pro Tempore

Speaker of the House of Representatives

Governor of the State of Indiana

Date: _____ Time: _____

SEA 5 — Concur