HOUSE BILL No. 1554

DIGEST OF INTRODUCED BILL

Citations Affected: IC 24-15.

Synopsis: Consumer data protection. Establishes in the Indiana Code a new article concerning consumer data protection, to take effect January 1, 2024. Sets forth the following within the new article: (1) Definitions of terms that apply throughout the article. (2) Exemptions for certain: (A) persons; and (B) types of information and data; from the bill's requirements concerning the personal data of Indiana consumers (consumers). (3) The rights of a consumer with respect to personal data relating to the consumer. (4) The responsibilities of controllers of consumers' personal data (controllers). (5) The roles of: (A) controllers; and (B) processors of consumers' personal data (processors); with respect to a consumer's personal data. (6) Requirements for data protection assessments by controllers. (7) Requirements for processing de-identified data or pseudonymous data. (8) Limitations as to the scope of the new article. (9) The establishment, maintenance, and publication by the attorney general's consumer protection division of a quarterly listing of electronic mail addresses of consumers who request that their personal data not be sold. (10) Requirements for brokers of consumers' personal information (data brokers) to: (A) provide notification of security breaches; and (B) register annually with the attorney general. (11) The authority of the attorney general to investigate and enforce suspected or actual violations of the new article. (12) The establishment of the consumer privacy account within the state general fund to support the work of the attorney general in enforcing the new article. (13) The authority of the attorney general to: (A) to adopt rules to administer the new article; and (B) issue opinion letters and interpretive guidance to develop an

(Continued next page)

Effective: January 1, 2024.

Jeter

January 19, 2023, read first time and referred to Committee on Commerce, Small Business and Economic Development.

operational framework for persons subject to the new article. (14) The preemption of local rules, regulation, and laws regarding the processing of personal data.

Introduced

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.

HOUSE BILL No. 1554

A BILL FOR AN ACT to amend the Indiana Code concerning trade regulation and to make an appropriation.

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, 2024]:

ARTICLE 15. CONSUMER DATA PROTECTION

Chapter 1. Applicability

Sec. 1. (a) This article applies to a person that does business in Indiana, or that produces products or services that are purchased or used by residents of Indiana, and that:

(1) during a calendar year controls or processes personal data of at least one hundred thousand (100,000) consumers; or

(2) controls or processes personal data of at least twenty-five thousand (25,000) consumers and derives more than fifty percent (50%) of gross revenue from the sale of personal data.

(b) This article does not apply to any:

(1) body, authority, board, bureau, commission, district, or

agency of the state or of any political subdivision of the state;

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

(3) national securities association that is registered under Section 15(a) of the Securities Exchange Act of 1934 (15 U.S.C. 78o-3); or

(4) 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.

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

(1) Protected health information under HIPAA.

(2) Health records (as defined in IC 4-6-14-2.5).

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

(4) 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 6, 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.

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

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

(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, as defined in 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 or furnisher 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) with respect to an individual applying to, employed by, or acting as an agent or independent contractor of a controller, processor, or third party, to the extent the data is collected and used within the context of that role;

(B) as emergency contact information for an individual described in clause (A), if the data is used for emergency contact purposes; or

(C) to administer benefits for another individual related to an individual described in clause (A), if the data is used for the purposes of administering those benefits.

(14) Personal data collected, processed, sold, or disclosed relating to:

(A) price;

(B) route; or

(C) service;

as those terms are used in the federal Airline Deregulation Act (49 U.S.C 40101 et seq.), by an air carrier subject to that

act, to the extent this article is preempted by 49 U.S.C. 41713.

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. "Account" refers to the consumer privacy account established within the state general fund under IC 24-15-13-1.

Sec. 2. (a) "Affiliate" means a person that:

(1) directly or indirectly controls, is controlled by, or is under common control with another person; or

(2) shares common branding with another person.

(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.

The terms "controlling", "controlled by", and "under common control with" have corresponding meanings.

(c) For purposes of this section, notwithstanding subsections (a) and (b), a person is not considered to have control of a corporation if the person holds voting power in good faith and not for the purpose of circumventing this article, as an agent, bank, broker, nominee, custodian, or trustee for one (1) or more beneficial owners who do not individually or as a group have control of the corporation.

Sec. 3. "Authenticate" means to determine, through reasonable means, that a request to exercise any of the consumer rights afforded by this article is being made by, or on behalf of, the consumer who is entitled to exercise those rights with respect to the personal data at issue.

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;

(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. "Brokered personal data" means computerized personal data that:

(1) pertains to an identified or identifiable individual; and

(2) is:

(A) categorized;

(B) organized; or

(C) intended;

for dissemination to third parties.

Sec. 6. "Business associate" has the meaning set forth in 45 CFR 160.103.

Sec. 7. "Child" means any individual who is less than eighteen (18) years of age.

Sec. 8. (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 by electronic means, or any other unambiguous affirmative action.

(c) The term "consent" does not include:

(1) acceptance of a general or broad terms of use agreement, or similar agreement, that contains descriptions of personal data processing along with other, unrelated information;

(2) hovering over, muting, pausing, or closing a given piece of content; or

(3) agreement obtained through the use of dark patterns.

Sec. 9. (a) "Consumer" means an individual who is a resident of Indiana.

(b) The term does not include:

(1) an individual acting in a commercial or employment context; or

(2) an individual:

(A) who is an employee, owner, director, officer, or

contractor of a company, partnership, sole proprietorship, nonprofit organization, or government agency; and

(B) whose communications or transactions with a controller occur solely within the context of that individual's role with the company, partnership, sole proprietorship, nonprofit organization, or government agency.

Sec. 10. "Controller" means a person that, alone or jointly with others, determines the purpose and means of processing personal data.

Sec. 11. "Covered entity" has the meaning set forth in 45 CFR 160.103.

Sec. 12. (a) "Dark pattern" means a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision making, or choice.

(b) The term includes any practice the Federal Trade Commission refers to as a "dark pattern".

Sec. 13. (a) "Data broker" means an entity (or one (1) or more units of an entity, separately or together) that knowingly:

(1) collects; and

(2) sells or licenses to third parties;

the brokered personal data of a consumer with whom the entity does not have a direct relationship.

(b) For purposes of this section, the term "sells or licenses" does not include actions in connection with:

(1) a one (1) time or occasional sale of assets of an entity, if the sale:

(A) is part of a transfer of control of those assets; and

(B) is not part of the ordinary conduct of the entity; or

(2) a sale or licensing of data, if the sale or licensing is merely incidental to the entity.

(c) For purposes of this section, a direct relationship with an entity includes an entity's relationship with a consumer who is a past or present:

(1) customer, client, subscriber, user, or registered user of the entity's goods or services;

(2) employee or agent of, or contractor for, the entity;

(3) investor in the entity; or

(4) donor to the entity.

(d) For purposes of this section, an entity is not a data broker solely because the entity performs one (1) or more of the following activities, or solely because the entity collects and sells or leases

brokered personal data incidental to conducting one (1) or more of the following activities:

(1) Developing or maintaining electronic commerce:

(A) applications; or

(B) platforms;

for third parties.

(2) Providing, on behalf of, or as a function of, a telecommunications carrier:

(A) 411 directory assistance services; or

(B) directory information services;

involving the names, addresses, and telephone numbers of consumers.

(3) Providing publicly available information related to a person's business or profession.

(4) Providing publicly available information through:

(A) real time; or

(B) near real time;

alert services for health or safety purposes.

Sec. 14. (a) "Data broker security breach" means an unauthorized acquisition, or a reasonable belief in the occurrence of an unauthorized acquisition:

(1) that is made with respect to computerized data maintained by a data broker; and

(2) that compromises the security, confidentiality, or integrity of brokered personal data.

(b) The term includes the unauthorized acquisition of computerized data that have been transferred to another medium, including paper, microfilm, or a similar medium, even if the transferred data are no longer in a computerized format.

(c) The term does not include a good faith but unauthorized acquisition of brokered personal data by an employee or agent of a data broker for a legitimate purpose of the data broker if the acquired brokered personal data is not:

(1) used for a purpose unrelated to the data broker's business; or

(2) subject to further unauthorized disclosure.

(d) For purposes of this section, an "unauthorized acquisition" is an acquisition that a data broker determines has been made, or reasonably believes has been made, by a person without valid authorization, based on the data broker's consideration of one (1) or more of the following factors:

(1) Indications that the brokered personal data is in the

physical possession of a person without valid authorization, such as in the case of a lost or stolen:

(A) computer; or

(B) other device;

containing brokered personal data.

(2) Indications that the brokered personal data has been downloaded or copied.

(3) Indications that the brokered personal data has been used by an unauthorized person, such as instances of:

(A) fraudulent accounts having been opened; or

(B) identity theft having been reported.

(4) Instances in which the brokered personal data has been made public.

(5) Indications or instances of other similar events or occurrences.

Sec. 15. "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 or lending services;

(2) housing;

(3) insurance;

(4) education enrollment;

(5) criminal justice;

(6) employment opportunities;

(7) health care services; or

(8) access to essential goods or services, including basic necessities, such as food and water.

Sec. 16. "De-identified data" means data that cannot reasonably be used to infer information about, or be otherwise linked to, an identified or identifiable individual, or a device 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. 17. "Device" means any electronic equipment that is:

(1) capable of collecting, processing, or transferring data; and

(2) used by one (1) or more individuals.

Sec. 18. "Do business in Indiana" means to own or use the personal data of an Indiana resident for commercial purposes.

Sec. 19. "Encrypted" data means data that:

(1) have been transformed through the use of an algorithmic process into a form in which there is a low probability of assigning meaning without the use of a confidential process or key; or

(2) are secured by another method that renders the data unreadable or unusable.

Sec. 20. "Entity" has the meaning set forth in IC 23-1-20-10. However, the term does not include the state, the United States, or a foreign government unless otherwise specified in this article.

Sec. 21. "HIPAA" refers to:

(1) the federal Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. 1320d et seq.);

(2) the Health Information Technology for Economic and Clinical Health Act (Pub. L. No. 111-5, 123 Stat. 226 (2009)); and

(3) related regulations, including:

(A) 45 CFR Part 160;

(B) 45 CFR Part 162; and

(C) 45 CFR Part 164.

Sec. 22. "Identified or identifiable individual" means an individual who can be readily identified, directly or indirectly.

Sec. 23. "Indiana resident" means a person whose principal mailing address is in Indiana, as reflected in records maintained by a controller.

Sec. 24. (a) "License", with respect to data, means an action involving a grant of access to, or distribution of, the data by one (1) person to another person in exchange for consideration.

(b) The term does not include the use of data for the sole benefit of the data provider if the data provider maintains control over the use of the data.

Sec. 25. "Nonprofit organization" means:

(1) a domestic nonprofit corporation incorporated under or subject to IC 23-17;

(2) a foreign nonprofit corporation; or

(3) any organization exempt from taxation under Section 501(c)(3), 501(c)(4), 501(c)(6), or 501(c)(12) of the Internal Revenue Code.

Sec. 26. "Person" means an individual, corporation, business

trust, estate, trust, partnership, association, nonprofit organization, educational institution, or cooperative or any other legal entity.

Sec. 27. (a) "Personal data" means information that is linked or reasonably linkable to an identified or identifiable individual.

(b) The term includes the following:

(1) An individual's:

(A) Social Security number; or

(B) other government issued identification number;

that is not encrypted or redacted.

(2) An individual's:

(A) first and last names, or first initial and last name;

(B) address;

(C) date of birth; or

(D) mother's maiden name.

(3) An individual's biometric data.

(4) The name or address of a member of the individual's immediate family or household.

(5) Other information, that alone or in combination with other information sold or licensed, would allow a reasonable person to identify the individual with reasonable certainty.

(c) The term does not include information that is lawfully obtained from:

(1) publicly available information; or

(2) federal, state, or government records lawfully made available to the public.

Sec. 28. (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 an invidual with precision and accuracy within a radius of one thousand seven hundred fifty (1,750) feet.

(b) The term does not include the content of communications or any data generated by or connected to advanced utility metering infrastructure systems or equipment for use by a utility.

Sec. 29. "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. 30. "Processor" means a person that processes personal data on behalf of a controller.

Sec. 31. "Profiling" means any form of automated processing performed on personal data to evaluate, analyze, or predict

personal aspects related to an identified or identifiable individual's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.

Sec. 32. "Protected health information" has the meaning set forth in 45 CFR 160.103.

Sec. 33. "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. 34. "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 by the consumer to the general public through widely distributed media, unless the consumer has restricted the information to a specific audience.

Sec. 35. "Record" means any material on which written, drawn, spoken, visual, or electromagnetic information is recorded or preserved, regardless of physical form or characteristics.

Sec. 36. "Redact", with respect to data, means to render data so that the data:

(1) are unreadable; or

(2) in the case of an identification number, are truncated so that not more than the last four (4) digits of the identification number are accessible as part of the data.

Sec. 37. (a) "Sale of personal data" means the selling, exchanging, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating (whether orally, in writing, or by electronic or other means) personal data, including sensitive data, for monetary or other valuable consideration by a controller, processor, or data broker 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 the

consumer;

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

(4) the disclosure of personal data if the consumer directs the controller to disclose the personal data or intentionally uses the controller to interact with a third party;

(5) the disclosure of personal data that the consumer:

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

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

(6) 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. 38. "Sensitive data" means a category of personal data that includes:

(1) personal data revealing racial or ethnic origin, religious beliefs, a mental or physical health diagnosis, disability, sex life, gender, gender identity, sexual orientation, union membership, or citizenship or immigration status;

(2) genetic or biometric data that is processed for the purpose of uniquely identifying an individual;

(3) personal data collected from a known child; and

(4) precise geolocation data.

Sec. 39. (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:

(A) search query in; or

(B) 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. 40. "Third party", with respect to a context to which this article applies, means an individual or a legal entity (including a 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. 41. "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 subsection (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 or has processed, directly or indirectly, the consumer's personal data.

(2) To access the consumer's personal data processed by the controller, with the data provided in a human readable format that:

(A) is downloadable from the Internet; and

(B) a reasonable individual could understand.

(3) To correct inaccuracies in 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.

(4) To receive from the controller a list of all available sources of the consumer's personal data.

(5) To receive from the controller a list of receivers of the consumer's personal data.

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

(7) To obtain a copy of the consumer's personal data, held 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, in

any case in which the processing is carried out by automated means.

(8) 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 two (2) times 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 is not 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.

(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.

(e) The attorney general may create an online portal to facilitate the receipt of consumer requests under this chapter. If the attorney general creates a portal as authorized by this subsection, the following apply:

(1) The attorney general shall provide consumer requests submitted through the portal to controllers that elect to use the service.

(2) A request submitted through the portal is considered received by a controller upon the controller's receipt of the request from the attorney general.

(3) The attorney general shall establish a fee to be paid by a controller that elects to use the service. The fee established under this subdivision may not exceed the amount necessary to cover the attorney general's cost of providing the service.

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 to 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)(8) 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 personal data to third parties or processes 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 processing.

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.

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) Fulfilling 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.

(3) Providing necessary information to enable the controller to conduct and document data protection 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 who processes 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 the processor's 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 subcontractors only 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 the processor by virtue of either's 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 Assessments

Sec. 1. (a) The data protection assessment requirements set forth in this chapter apply to processing activities created or generated after December 31, 2023, and are not retroactive to any processing activities created or generated before January 1, 2024.

(b) A controller shall conduct and document a data protection assessment of compliance with this article and 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 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 assessment may address a comparable set of processing operations that include similar activities.

(e) A data protection 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 that a controller disclose any data protection 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 assessment available to the attorney general. Subject to subsection (b), the attorney general may evaluate the data protection assessment for a controller's compliance with the responsibilities set forth in IC 24-15-4.

(b) Data protection assessments, all assessment requests, and any communications or documents related to assessments are confidential and exempt from public inspection and copying under IC 5-14-3-4 unless and until confidentiality is waived by the controller.

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)(7); and

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

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) Subject to IC 24-15-15-1, comply with federal, state, or local laws, rules, or regulations.

(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 is a party, including fulfilling the terms of a written warranty, or take steps at the request of the consumer 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 involved 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, preserve the integrity or security of systems, or investigate, report, or prosecute those responsible for any such action.

(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 to be obtained from the research 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 the 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. Subject to section 7(b) of this chapter, the obligations imposed on a controller or a processor under this article do not restrict a controller's or processor's ability to collect, use, or retain 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 of a product, service, technology, or system.

(4) Perform internal operations that are:

(A) reasonably aligned with the expectations of a consumer;

(B) reasonably anticipated based on a 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

(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 prevent 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 the processing of 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 shall, as applicable, take into account the nature and purpose of the collection, use, or retention. Any personal data

collected, used, or retained must be subject to reasonable administrative, technical, and physical measures to:

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

(2) 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. Do Not Sell List: Right of Consumer to Opt Out of Sale of Personal Data

Sec. 1. As used in this chapter, "division" refers to the division of consumer protection of the office of the attorney general.

Sec. 2. (a) A quarterly listing of electronic mail addresses of consumers (as defined in IC 24-15-2-9) who request that their personal data not be sold shall be established, maintained, and published as provided in this section.

(b) An electronic mail address of a consumer shall be placed on the listing if the consumer requests to be added to the listing according to a procedure approved by the division.

(c) The division shall update the listing upon receipt of a request from a consumer.

(d) A controller may obtain a copy of the listing upon request of the controller as provided in this section.

(e) The division shall establish a fee to be paid by a controller for obtaining a copy of the listing. The fee established under this subsection may not exceed the amount necessary to cover the cost of providing the listing to controllers.

Sec. 3. (a) A controller may not sell, or cause to be sold, the personal data associated with an electronic mail address if the electronic mail address appears in the most current quarterly listing published by the division under section 2 of this chapter.

(b) A controller shall do the following:

(1) Download from the attorney general's website the quarterly listing in order to determine whether the personal information associated with any of the listed electronic mail addresses is being sold, or is being caused to be sold, by the controller.

(2) Provide on the home page of the controller's website a

clear and conspicuous link, titled "Do Not Sell My Personal Data", to a web page that enables a consumer to opt out of the sale of the consumer's personal data.

(c) A controller shall not require a consumer to create an account in order to direct the controller not to sell the consumer's personal data.

Chapter 10. Data Brokers and Brokered Personal Data

Sec. 1. (a) A person shall not do the following:

(1) Acquire brokered personal data through fraudulent means.

(2) Acquire or use brokered personal data for the purpose of:

(A) stalking or harassing another person;

(B) committing a fraud, including identity theft, financial fraud, or electronic mail fraud; or

(C) engaging in unlawful discrimination, including employment discrimination or housing discrimination.

(b) A person that violates this section commits an unfair, abusive, or deceptive act in violation of IC 24-5-0.5.

(c) The attorney general has the same authority to conduct civil investigations, accept assurances of voluntary compliance, bring civil actions, and take other enforcement actions under IC 24-5-0.5-4 in connection with violations or suspected violations of this section.

Sec. 2. A data broker is subject to:

(1) the notification requirements set forth in IC 24-4.9-3; and

(2) the enforcement actions set forth in IC 24-4.9-4;

in connection with a data broker security breach.

Sec. 3. A data broker shall not sell, or cause to be sold, personal data, including sensitive data, of a consumer if that consumer's electronic mail address appears in the most current quarterly listing published by the division (as defined in IC 24-15-9-1) under IC 24-15-9.

Sec. 4. (a) Not later than January 31 of each year, beginning with the first year following the year in which a data broker first acts as a data broker (as defined in IC 24-15-2-13), a data broker shall do the following:

(1) Register with the attorney general in accordance with procedures prescribed by the attorney general.

(2) Pay an annual registration fee of one hundred dollars ($100).

(3) Provide the following information to the attorney general:

(A) The name and primary:

(i) physical;
(ii) electronic mail; and
(iii) Internet;
addresses of the data broker.
(B) If the data broker permits a consumer to opt out of the data broker's collecting of brokered personal data, opt out of the data broker's data bases, or opt out of certain sales of data:
(i) the one (1) or more methods by which a consumer may request an opt out;
(ii) if the ability to opt out applies only to certain activities or sales, a description of those activities or sales; and
(iii) whether the data broker permits a consumer to authorize a third party to request an opt out on the consumer's behalf.
(C) A statement specifying the data broker's:
(i) data collection activities;
(ii) data bases; and
(iii) sales of data;
from which a consumer may not opt out.
(D) A statement as to whether the data broker implements a purchaser credentialing process.
(E) The number of data broker security breaches experienced by the data broker during the immediately preceding calendar year and, if known, the total number of consumers affected by each breach.
(F) If the data broker has actual knowledge that the data broker possesses the brokered personal data of children (as defined in IC 24-15-2-7), a separate statement detailing the data broker's:
(i) data collection practices;
(ii) data bases;
(iii) sales activities; and
(iv) opt out policies;
that apply to the brokered personal data of children.
(G) Any additional information or explanation the data broker chooses to provide with respect to the data broker's data collection practices, data bases, sales activities, or opt out policies.

(b) A data broker that fails to register as required by this section is liable to the state for the following:

(1) A civil penalty in the amount of fifty dollars ($50) per day for each day the data broker fails to register as required by this section, but not to exceed a total amount of ten thousand dollars ($10,000) per calendar year.

(2) An amount equal to the fee required under subsection (a)(2) for each year the data broker fails to register as required by this section.

(3) Any other penalties imposed by law.

(c) The attorney general may maintain a civil action in a court of competent jurisdiction to collect the penalties authorized by this section and to seek appropriate injunctive relief.

Chapter 11. Investigative Authority

Sec. 1. (a) If the attorney general has reasonable cause to believe that a person may:

(1) be in possession, custody, or control of documentary material; or

(2) have knowledge of a fact;

that is relevant to an investigation to determine if a person is or has been engaged in a violation of this article, the attorney general may issue in writing, and cause to be served upon the person or the person's representative or agent, an investigative demand under IC 4-6-3.

(b) An investigative demand issued and served under subsection (a) may require that the person served do any combination of the following:

(1) Produce the documentary material for inspection and copying or reproduction.

(2) Answer under oath and in writing written interrogatories.

(3) Appear and testify under oath before the attorney general or the attorney general's duly authorized representative.

(c) The attorney general has the authority to:

(1) enforce compliance with this section by investigation and subsequent commencement of a civil action;

(2) seek civil penalties for violations of this section; and

(3) seek appropriate injunctive relief, including prohibiting a person from obtaining personal data for an appropriate time period, as determined by the attorney general.

(d) In carrying out an investigation and maintaining a civil action under this section, the attorney general and any deputy or assistant attorney general is authorized to:

(1) subpoena witnesses, compel their attendance, and examine them under oath; and

(2) require that any books, records, documents, papers, or electronic records relevant to the inquiry be turned over for inspection, examination, or audit.

Subpoenas issued under this subsection may be enforced pursuant to the Indiana Rules of Civil Procedure.

Chapter 12. Enforcement

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

Sec. 2. (a) Before initiating an action under 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 subsection, 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) no further violations will occur;

the attorney general shall not initiate an action against the controller or processor. This subsection expires January 1, 2026.

(b) If a controller or processor:

(1) continues to violate this article following the thirty (30) day period set forth in subsection (a) (before its expiration on January 1, 2026); or

(2) breaches an express written statement provided to the attorney general under subsection (a)(2) (before its expiration on January 1, 2026);

the attorney general may initiate an action in the name of the state. In an action initiated under this subsection, the attorney general may seek an injunction to restrain any violations of this article and may seek a civil penalty not to exceed seven thousand five hundred dollars ($7,500) for each violation of this article. This subsection expires January 1, 2026.

(c) After December 31, 2025, the attorney general:

(1) is not required to provide:

(A) a notice of an alleged violation of this article; or

(B) a thirty (30) day cure period with respect to the alleged violation;

in accordance with subsection (a) (before its expiration on January 1, 2026); and

(2) may initiate an action in the name of the state and may

seek:

(A) an injunction to restrain any violations of this article; and

(B) a civil penalty not to exceed seven thousand five hundred dollars ($7,500) for each violation of this article.

(d) In any action initiated under this chapter, the attorney general may recover:

(1) reasonable expenses incurred in investigating and preparing the case, including attorney's fees; or

(2) any amount necessary to restore to any person any money or property that may have been acquired from the person by the alleged violator in connection with the violation.

Sec. 3. This article shall not be construed as providing the basis for a private right of action for violations of this article or any other law.

Chapter 13. Consumer Privacy Account

Sec. 1. (a) The consumer privacy account is established within the state general fund to support the work of the attorney general in enforcing this article.

(b) The account consists of the following:

(1) All civil penalties, expenses, and attorney's fees collected by the attorney general under IC 24-15-10, IC 24-15-11, and IC 24-15-12.

(2) Money appropriated to the account by the general assembly.

(3) Donations, gifts, and money received from any other source, including transfers from other funds or accounts.

(c) Money in the account is continuously appropriated for the purposes of this section.

(d) Interest earned on money in the account shall remain in the account and be credited to the account.

(e) Money in the account at the end of a state fiscal year does not revert to the state general fund.

Chapter 14. Attorney General: Rulemaking and Interpretive Guidance

Sec. 1. The attorney general may adopt rules under IC 4-22-2, including emergency rules in the manner provided by IC 4-22-2-37.1, that the attorney general considers necessary to enforce this article.

Sec. 2. The attorney general may issue opinion letters and interpretive guidance to develop an operational framework for persons subject to this article. In issuing an opinion letter or

interpretive guidance under this section, the attorney general may provide for a good faith reliance defense with respect to an action that may otherwise constitute a violation of this article.

Chapter 15. 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.