SENATE BILL NO. 659

November 09, 2023, Introduced by Senators BAYER, CHERRY, CHANG, GEISS, SHINK, SANTANA and ANTHONY and referred to the Committee on Finance, Insurance, and Consumer Protection.

A bill to establish the privacy rights of consumers; to require certain persons to provide certain notices to consumers regarding the collection, processing, sale, sharing, and retention of personal data; to prohibit certain acts and practices concerning the collection, processing, sale, sharing, and retention of personal data; to establish standards and practices regarding the collection, processing, sale, sharing, and retention of personal data; to require the registration of data brokers; to provide for the powers and duties of certain state governmental officers and entities; to create certain funds; and to provide remedies.

THE PEOPLE OF THE STATE OF MICHIGAN ENACT:

Sec. 1. This act may be cited as the "personal data privacy act".

Sec. 3. For purposes of this act, the words and phrases defined in sections 5 to 9 have the meanings ascribed to them in those sections. These definitions, unless the context otherwise requires, apply to use of the defined terms in this act. Other definitions applicable to specific sections of the act are found in those sections.

Sec. 5. (1) "Affiliate" means, except as otherwise provided in section 11(2)(b), a person that controls, is controlled by, or is under common control with another person or shares common branding with another person. As used in this subsection, "control" or "controlled" means any of the following:

(a) Ownership of, or the power to vote, more than 50% of the outstanding shares of any class of voting security of a company.

(b) Control in any manner over the election of a majority of the directors or of individuals exercising similar functions.

(c) The power to exercise controlling influence over the management of a company.

(2) "Authenticate" means verifying through reasonable means that a consumer, entitled to exercise the consumer rights under this act, is the same consumer exercising those consumer rights with respect to the personal data at issue.

(3) "Biometric data" means data generated by automatic measurements of an individual's biological characteristics, including, but not limited to, a fingerprint, a voiceprint, eye retinas, irises, or other unique biological patterns or characteristics, that are used to identify a specific individual. Biometric data does not include any of the following:

(a) A physical or digital photograph.

(b) A video or audio recording.

(c) Any data generated from a physical or digital photograph, or a video or audio recording, unless the data is generated to identify a specific individual.

(4) "Business associate" means that term as defined in 45 CFR 160.103

(5) "Child" means an individual who is less than 13 years of age.

(6) "Collects", "collected", or "collection" means buying, renting, gathering, obtaining, receiving, or accessing personal data pertaining to a consumer by any means. Collects, collected, or collection includes receiving personal data from the consumer, either actively or passively, or observing the consumer's behavior.

(7) "Consent" means a clear affirmative act signifying a consumer's freely given, specific, informed, and unambiguous agreement to process personal data relating to the consumer. Consent may include a written statement, including a statement written by electronic means, or any other unambiguous affirmative action. Consent does not include any of the following:

(a) The acceptance of a general or broad terms of use or similar document that contains any description of personal data processing and other unrelated information.

(b) The act of hovering over, muting, pausing, or closing a given piece of content.

(c) An agreement obtained through the use of dark patterns.

(8) "Consumer" means an individual who is a resident of this state acting in an individual or household context. Consumer does not include an individual acting in a commercial or employment

context.

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

(10) "Covered entity" means that term as defined in 45 CFR 160.103.

(11) "Cross-context behavioral advertising" means the targeting of advertising to a consumer based on the consumer's personal information obtained from the consumer's activity across businesses, distinctly branded websites, applications, or services, other than the business, distinctly branded website, application, or service with which the consumer intentionally interacts.

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

(13) "Data broker" means a company, or a unit or units of a company, separately or together, that knowingly collects and sells, or licenses to a third party, the brokered personal data of a consumer with whom the company does not have a direct relationship.

(14) "Decisions that produce legal or similarly significant effects concerning a consumer" means decisions that result in the provision or denial of financial and lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunities, health care services, or access to basic necessities, including, but not limited to, food and water.

(15) "De-identified data" means data that cannot reasonably be linked to an identified or identifiable individual, or to a device linked to that individual.

Sec. 7. (1) "Identified or identifiable individual" means an

individual who can be readily identified, directly or indirectly.

(2) "Institution of higher education" means a degree- or certificate-granting public or private college or university, junior college, or community college located in this state.

(3) "Institutional review board" means that term as defined in 21 CFR 56.102.

(4) "Person" means an individual or a partnership, corporation, limited liability company, association, governmental entity, or other legal entity.

(5) "Personal data" means information that is linked or reasonably linkable to an identified or identifiable individual. Personal data does not include de-identified data or publicly available information.

(6) "Precise geolocation data" means information derived from technology, including, but not limited to, global positioning system level latitude and longitude coordinates or other mechanisms, that directly identifies the specific location of an individual with precision and accuracy within a radius of 1,750 feet. Precise geolocation data does not include the content of communications or data generated by or connected to advanced utility metering infrastructure systems or equipment for use by a utility.

(7) "Process" or "processing" means an operation or set of operations performed, whether by manual or automated means, on personal data or on sets of personal data, including, but not limited to, the collection, use, storage, disclosure, analysis, deletion, or modification of personal data.

(8) "Processor" means a person that processes personal data on behalf of a controller.

(9) "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.

(10) "Pseudonymous data" means personal data that cannot be attributed to a specific individual without the use of additional information, if the additional information is kept separately and is subject to appropriate technical and organizational measures to ensure that the personal data is not attributed to an identified or identifiable individual.

(11) "Publicly available information" means information that is lawfully made available through federal, state, or local government records, or information that a person has a reasonable basis to believe is lawfully made available to the general public through widely distributed media, by the consumer, or by a person to whom the consumer has disclosed the information, unless the consumer has restricted the information to a specific audience.

Sec. 9. (1) "Sale of personal data" means the exchange of personal data for monetary or other valuable consideration by a controller to a third party. Sale of personal data does not include any of the following:

(a) The disclosure of personal data to a processor that processes the personal data on behalf of the controller.

(b) The disclosure of personal data to a third party for the purpose of providing a product or service requested by the consumer.

(c) The disclosure or transfer of personal data to an affiliate of the controller.

(d) The disclosure of information that the consumer intentionally made available to the general public via a channel of mass media and did not restrict the information to a specific audience.

(e) The disclosure or transfer of personal data to a third party as an asset that is part of a merger, acquisition, bankruptcy, or other transaction, or a proposed merger, acquisition, bankruptcy, or other transaction, in which the third party assumes or will assume control of all or part of the controller's assets.

(2) "Sensitive data" means a category of personal data that includes all of the following:

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

(b) Genetic or biometric data for the purpose of uniquely identifying an individual.

(c) Personal data collected from a known child.

(d) Precise geolocation data.

(e) A consumer's Social Security number.

(f) A consumer's driver license number, official state personal identification card number, or passport number.

(g) A consumer's account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

(h) A consumer's username or email address in combination with a password or security question and answer that would permit access to an online account.

(3) "Share" means, except as otherwise provided in section 5(1) and section 11(3)(d), to rent, release, disclose, disseminate, making available, transfer, or otherwise communicate orally, in writing, or by electronic or other means, a consumer's personal information to a third party for cross-context behavioral advertising, whether or not for monetary or other valuable consideration.

(4) "State agency" means a state department, agency, bureau, division, section, board, commission, trustee, authority, or officer that is created by the state constitution of 1963, statute, or state agency action.

(5) "Subprocessor" means a person that has a contract with a processor to process personal data that is subject to a contract between the processor and a controller.

(6) "Targeted advertising" means displaying advertisements to a consumer if the advertisements are selected based on personal data obtained or inferred from that consumer's activities over time and across nonaffiliated websites or online applications to predict the consumer's preferences or interests. Targeted advertising does not include any of the following:

(a) Advertisements based on activities within a controller's own websites or online applications.

(b) Advertisements based on the context of a consumer's current search query, visit to a website, or online application.

(c) Advertisements directed to a consumer in response to the consumer's request for information or feedback.

(d) Processing personal data solely for the purpose of measuring or reporting advertising performance, reach, or frequency.

(7) "Third party" means a person other than the consumer, controller, processor, or an affiliate of the controller or processor.

Sec. 11. (1) This act applies to a person that does both of the following:

(a) Conducts business in this state or produces products or services that are targeted to residents of this state.

(b) During a calendar year, does either of the following:

(*i*) Controls or processes personal data of at least 100,000 consumers.

(*ii*) Controls or processes personal data of at least 25,000 consumers and derives any revenue from the sale of personal data.

(2) This act does not apply to any of the following:

(a) A state agency or any other political subdivision of this state.

(b) A financial institution or an affiliate of a financial institution that is subject to title V of the Gramm-Leach-Bliley act, 15 USC 6801 to 6827, and the regulations promulgated under that act.

(c) A covered entity or business associate governed by the privacy, security, and breach notification rules under the health insurance portability and accountability act of 1996, Public Law 104-191, and the regulations promulgated under that act, 45 CFR parts 160 and 164, and the health information technology for economic and clinical health act, Public Law 111-5.

(d) An institution of higher education.

(e) An entity that is subject to or regulated under the insurance code of 1956, 1956 PA 218, MCL 500.100 to 500.8302.

(f) A nonprofit organization that operates to detect or

prevent insurance-related crimes, including, but not limited to, insurance fraud.

(g) A nonprofit dental care corporation operating under 1963 PA 125, MCL 550.351 to 550.373.

(h) A third party administrator as that term is defined in section 2 of the third party administrator act, 1984 PA 218, MCL 550.902.

(3) The following information and data are exempt from this act:

(a) Protected health information under the health insurance portability and accountability act of 1996, Public Law 104-191, and the regulations promulgated under that act, 45 CFR parts 160 and 164.

(b) A record that is a medical record as that term is defined in section 3 of the medical records access act, 2004 PA 47, MCL 333.26263.

(c) Patient identifying information for purposes of 42 USC 290dd-2.

(d) Identifiable private information for the purpose of the federal policy for the protection of human subjects under 45 CFR part 46; identifiable private information that is otherwise information collected as part of human subjects research in accordance with the "Good Clinical Practice Guidelines" issued by the International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use; the protection of human subjects under 21 CFR parts 50 and 56; personal data used or shared in research conducted in accordance with the requirements under this act, or other research conducted in accordance with applicable law.

(e) Information and documents created for purposes of the health care quality improvement act of 1986, 42 USC 11101 to 11152.

(f) Patient safety work product for purposes of the patient safety and quality improvement act of 2005, Public Law 109-41.

(g) Information derived from any of the health care-related information listed in this subsection that is de-identified in accordance with the requirements for de-identification under the health insurance portability and accountability act of 1996, Public Law 104-191.

(h) Information originating from, and intermingled to be indistinguishable with, or information treated in the same manner as information exempt under this subsection that is maintained by a covered entity, business associate, program, or qualified service organization. As used in this subdivision, "program" and "qualified service organization" mean those terms as defined in 42 CFR 2.11.

(i) Information used only for public health activities and purposes as authorized under the health insurance portability and accountability act of 1996, Public Law 104-191.

(j) The collection, maintenance, disclosure, sale, communication, or use of any personal data bearing on a consumer's creditworthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living by a consumer reporting agency, furnisher, or user that provides information for use in a consumer report, and by a user of a consumer report, but only to the extent that the activity is regulated by and authorized under the fair credit reporting act, 15 USC 1681 to 1681x.

(k) Personal data collected, processed, sold, or disclosed in compliance with the driver's privacy protection act of 1994, 18 USC

2721 to 2725.

(*l*) Personal data regulated by the family educational rights and privacy act of 1974, 20 USC 1232g.

(m) Personal data collected, processed, sold, or disclosed in compliance with 12 USC 2001 to 2279cc.

(n) Data processed or maintained for any of the following purposes:

(*i*) 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.

(*ii*) As the emergency contact information of an individual for emergency contact purposes.

(*iii*) That is necessary to retain to administer benefits for another individual relating to the individual under subparagraph (*i*) and used for the purpose of administering those benefits.

(*iv*) That is necessary in any matter relating to an unemployment benefit claim or appeal under the Michigan employment security act, 1936 (Ex Sess) PA 1, MCL 421.1 to 421.75.

(o) Data that are subject to title V of the Gramm-Leach-Bliley act, 15 USC 6801 to 6827, and the regulations promulgated under that act.

(p) Information or data that are collected or obtained for the sole purpose of developing, testing, or operating an automated driving system or advanced driver assistance system in a motor vehicle. As used in this subdivision:

(*i*) "Advanced driver assistance system" means either of the following:

(A) A driver support feature on a vehicle that can assist an

individual with steering, or braking or accelerating, but not both simultaneously.

(B) A driver support feature on a vehicle that can control both steering, and braking or accelerating, simultaneously, under certain circumstances.

(*ii*) "Automated driving system" means a system, including hardware and software, that is collectively capable of performing the entire dynamic driving task on a sustained basis, regardless of whether the system is limited to a specific operational design domain, and regardless of the presence of a safety operator.

(4) A controller or processor that complies with the verifiable parental consent requirements of the children's online privacy protection act of 1998, 15 USC 6501 to 6506, satisfies any obligation to obtain parental consent under this act.

Sec. 13. (1) A consumer may invoke the consumer rights authorized under this section at any time by submitting a request to a controller specifying the consumer rights that the consumer wishes to invoke. A known child's parent or legal guardian may invoke the consumer rights on behalf of the child regarding processing personal data belonging to the known child. Except as otherwise provided in this act, a controller shall comply with an authenticated request by a consumer to exercise the consumer rights authorized under this section.

(2) A consumer has all of the following rights:

(a) To confirm whether or not the controller is processing the consumer's personal data and to access the personal data.

(b) 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.

(c) Except as otherwise provided in subsection (3)(e), to delete personal data provided by or obtained about the consumer.

(d) To obtain a copy of the consumer's personal data that the consumer previously provided to 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, where the processing is carried out by automated means.

(e) To opt out of the processing of the personal data for any of the following purposes:

(*i*) Targeted advertising.

(*ii*) The sale of personal data.

(*iii*) Profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer.

(3) All of the following apply to complying with a request under subsection (1):

(a) A controller shall respond to a consumer without undue delay, but in all cases not more than 45 days after receipt of the request. The response period may be extended once by 45 additional days when reasonably necessary, taking into account the complexity and number of the consumer's requests, if the controller informs the consumer of the extension within the initial 45-day response period, together with the reason for the extension.

(b) If a controller declines to take action regarding a consumer's request, the controller must inform the consumer without undue delay, but in all cases and at the latest not more than 45 days after receipt of the request, of the justification for declining to take action and instructions for how to appeal the decision under subsection (4).

(c) Information provided in response to a consumer request must be provided by a controller free of charge, up to twice 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 that a request is manifestly unfounded, excessive, or repetitive.

(d) If a controller is unable to authenticate the request using commercially reasonable efforts, the controller is not required to comply with the request and may ask a consumer to provide additional information that is reasonably necessary to authenticate the consumer and the consumer's request.

(e) A controller that obtains personal data about a consumer from a source other than the consumer complies with a request to delete personal data under subsection (2)(c) if the controller acts in accordance with either of the following:

(*i*) The controller retains a record of the request, retains the minimum data necessary to ensure that the consumer's personal data remains deleted from the controller's records, and does not use the retained data for any other purpose authorized under this act.

(*ii*) The controller does not process the personal data for any purpose described in subsection (2)(e).

(4) A controller shall establish a process for a consumer to appeal the controller's refusal to take action on a request within a reasonable period of time after the consumer's receipt of the decision under subsection (3)(b). The appeal process must be conspicuously available and similar to the process for submitting requests to initiate action under subsection (1). Not more than 60

days after the 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 must 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.

Sec. 15. A controller shall do all of the following:

(a) Except as otherwise provided in subdivision (n), not process personal data concerning a consumer without obtaining the consumer's consent.

(b) Provide an effective mechanism for a consumer to revoke the consumer's consent that is at least as easy to use as the mechanism used by the consumer to provide the consumer's original consent.

(c) If consent is revoked by the consumer, cease to process data as soon as practicable, but not later than 15 days, after the revocation of the consent.

(d) If the personal data concern a known child, process that data in accordance with the children's online privacy protection act of 1998, 15 USC 6501 to 6506.

(e) Except as otherwise provided in subdivision (n), limit the collection of personal data to what is adequate, relevant, and reasonably necessary in relation to the purposes for which the data is processed, unless the personal data is sensitive data, in which case the controller must limit the collection of the sensitive data to what is strictly necessary in relation to the purposes for which the sensitive data is processed.

(f) Except as otherwise provided in subdivision (g), at or

before the point of collecting personal data, disclose to the consumer the purpose for which the personal data will be processed.

(g) If the controller determines that collected data will be processed for a purpose other than what was initially disclosed to the consumer under subdivision (f), disclose to the consumer the additional purpose for which the data will be processed and obtain the consumer's consent to process the data for that additional purpose.

(h) Establish, implement, and maintain technical and organizational measures to protect the confidentiality, integrity, and accessibility of personal data, which must be appropriate to the volume and nature of the personal data at issue.

(i) Not process personal data in violation of any state and federal law that prohibits unlawful discrimination against a consumer. A controller shall not discriminate against a consumer for exercising any of the consumer rights under this act, including denying goods or services, charging different prices or rates for goods or services, or providing a different level of quality of goods and services to the consumer. However, nothing in this subdivision requires 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 prohibits 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 this act or the offer is reasonably related to a consumer's voluntary participation in a bona fide loyalty, rewards, premium features, discounts, or club card program and the benefit to the consumer is proportional to the benefit received by

the controller in collecting personal information from the reward, feature, discount, or program.

(j) Subject to sections 13 and 27, permanently and completely delete personal data in response to a consumer's request to delete that information unless retention of the personal data is required by law.

(k) Not retain personal data in a form that permits identification of the consumer for longer than the period that is reasonably necessary for the purposes for which the personal data is processed unless retention is otherwise required by law or under section 29.

(*l*) Not retain sensitive data in a form that permits identification of the consumer for longer than the period that is strictly necessary for the purpose for which the sensitive data is processed unless retention is otherwise required by law or under section 29.

(m) If a consumer has opted out of the processing of the consumer's personal data under this act, notify any processor or third party to which the controller sold or otherwise disclosed the consumer's personal data that the consumer has opted out of the processing of the consumer's personal data.

(n) If the controller has actual knowledge or willfully disregards that the consumer is between 13 and 18 years of age, not do either of the following:

(*i*) Process the personal data for the purpose of targeted advertising.

(*ii*) Sell the consumer's personal data without the consumer's consent.

Sec. 17. A provision of a contract or agreement of any kind

that purports to waive or limit in any way the consumer rights under this act is contrary to public policy and is void and unenforceable.

Sec. 19. (1) A controller shall provide a consumer with a reasonably accessible, clear, and meaningful privacy notice that includes all of the following:

(a) The categories of personal data processed by the controller.

(b) The purpose for processing personal data.

(c) A list of the consumer rights under this act.

(d) A summary of how the consumer may exercise the consumer rights under this act, including, but not limited, a description of the secure and reliable means established under section 21 and a summary of how the consumer may appeal a controller's decision with regard to the consumer's request.

(e) The categories of personal data that the controller sells to or shares with third parties, if any.

(f) The categories of third parties, if any, with whom the controller sells or shares personal data.

(g) That a controller or processor may use personal data to conduct internal research to develop, improve, or repair products, services, or technology, if the controller or processor conducting that research obtains consent from the consumer and maintains the same security measures as otherwise required for that personal data.

(h) The contact information of the controller, including an active email address or other online mechanism that the consumer may use to contact the controller.

(i) The length of time the controller intends to retain each

category of personal data, or, if that is impossible to determine, the criteria used by the controller to determine the length of time that the controller intends to retain each category of personal data.

(j) If a controller engages in profiling in furtherance of decisions that produce legal or similarly significant effects concerning a consumer, a disclosure of that fact and all of the following:

(*i*) A summary of how the profiling is used in the decision-making process.

(*ii*) The benefits and potential consequences of the decision concerning the consumer.

(k) The date that the privacy notice was last updated by the controller.

(2) A controller shall make its privacy notice available to the public in each language that the controller does either of the following:

(a) Provides a product or service that is subject to the privacy notice.

(b) Carries out activities related to the product or service.

(3) A controller shall ensure that its privacy notice can be accessed and used by individuals with disabilities.

(4) Except as otherwise provided in subsection (5), a controller shall post its privacy notice online using a conspicuous link with the word "privacy" on the controller's website homepage and any app store page, download page, or settings menu related to a mobile application of the controller.

(5) If a controller does not have a website, the controller must make its privacy notice available through a medium regularly

used by the controller to interact with consumers.

(6) If a controller makes a material change to its privacy notice, the controller must directly notify each consumer affected by the material change before implementing the material change, and if the material change relates to the collection, processing, or sale of personal data, ensure compliance with section 15.

(7) A controller is not required to provide a separate privacy notice applicable to this state if the controller's privacy notice otherwise complies with this section.

Sec. 21. (1) A controller shall establish 1 or more secure and reliable means for a consumer to submit a request to exercise the consumer rights under this act.

(2) The secure and reliable means described in subsection (1) must take into account the ways in which a consumer normally interacts with the controller, the need for secure and reliable communication of requests to exercise the consumer rights under this act, and the ability of the controller to authenticate the identity of the consumer making the request.

(3) A controller shall not require a consumer to create a new account to exercise the consumer rights under this act, but may require a consumer to use an existing account.

Sec. 23. (1) A processor shall adhere to the instructions of a controller and shall assist the controller in meeting its obligations under this act. The assistance provided by a processor to a controller must include all of the following:

(a) Fulfilling the controller's obligation to respond to consumer rights requests under this act, taking into account the nature of processing and the information available to the processor, by appropriate technical and organizational measures, to

the extent reasonably practicable.

(b) Assisting the controller in meeting obligations in relation to the security and processing of personal data and to the notification of a security breach under the identity theft protection act, 2004 PA 452, MCL 445.61 to 445.79d, taking into account the nature of processing and the information available to the processor.

(c) Providing necessary information to enable the controller to conduct and document data protection impact assessments under section 25.

(2) A contract between a controller and a processor must 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 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 include requirements that the processor do all of the following:

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

(b) At the controller's direction, delete or return all personal data to the controller as requested at the end of the provision of services, unless retention of the personal data is required by law.

(c) On 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 act.

(d) Either of the following:

(*i*) Allow, and cooperate with, reasonable assessments by the controller or the controller's designated assessor of the processor's policies and technical and organizational measures in support of the obligations under this act.

(*ii*) 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 obligations under this act using an appropriate and accepted control standard or framework and assessment procedure for those assessments. The processor shall provide a report of the assessment to the controller on request.

(e) Engage any subprocessor under a written contract that requires the subprocessor to meet the obligations of the processor with respect to the personal data.

(f) Require the processor to notify the controller of its engagement with any subprocessor.

(3) This section does not relieve a controller or a processor from the liabilities imposed on it by virtue of its role in the processing relationship under this act.

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

Sec. 25. (1) A controller shall conduct and document a data protection impact assessment of each of the following processing activities involving personal data:

(a) The processing of personal data for purposes of targeted advertising.

(b) The sale of personal data.

(c) The processing of personal data for the purpose of profiling, if the profiling presents a reasonably foreseeable risk of any of the following:

(*i*) Unfair or deceptive treatment of, or unlawful disparate impact on, consumers.

(*ii*) Financial, physical, or reputational injury to consumers.

(*iii*) A physical or other intrusion on the solitude or seclusion, or the private affairs or concerns, of consumers where the intrusion would be offensive to a reasonable person.

(*iv*) Other substantial injury to consumers.

(d) The processing of sensitive data.

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

(2) A data protection impact assessment conducted under subsection (1) must identify and weigh the benefits that may flow, directly and indirectly, from the processing to the controller, the consumer, other stakeholders, and the public against the potential risks to the rights of the consumer associated with the processing, as mitigated by safeguards that can be employed by the controller to reduce those 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, must be factored into the assessment by the controller.

(3) Subject to section 33, the attorney general may request that a controller disclose any data protection impact assessment that is relevant to an investigation conducted by the attorney general, and the controller must make the data protection impact

assessment available to the attorney general. The attorney general may evaluate the data protection impact assessment for compliance with the responsibilities set forth in sections 15 to 21. A data protection impact assessment is confidential and exempt from public inspection and copying under the freedom of information act, 1976 PA 442, MCL 15.231 to 15.246. The disclosure of a data protection impact assessment in accordance with 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.

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

(5) A data protection impact assessment conducted by a controller for the purpose of complying with other laws or regulations may satisfy the requirements of this section if the assessment has a reasonably comparable scope and effect.

(6) The data protection impact assessment requirements of this section apply to processing activities created or generated after January 1, 2025 and are not retroactive.

Sec. 27. (1) A controller in possession of de-identified data shall do all of the following:

(a) Take reasonable measures to ensure that the data cannot be associated with an individual.

(b) Publicly commit to maintaining and using de-identified data without attempting to re-identify the data.

(c) Contractually obligate any recipients of the de-identified data to comply with all provisions of this act.

(2) This act does not require a controller or processor to re-

identify de-identified data or pseudonymous data or maintain data in identifiable form, or collect, obtain, retain, or access any data or technology, to be capable of associating an authenticated consumer request with personal data.

(3) A controller or processor is not required to comply with an authenticated consumer rights request under section 13 if all of the following apply:

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

(b) 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.

(c) 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, except as otherwise permitted in this section.

(4) The consumer rights contained in section 13 and the requirements of sections 15 to 21 do not apply to pseudonymous data if 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 measures that prevent the controller from accessing the information.

(5) 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.

Sec. 29. (1) This act does not restrict a controller's or processor's ability to do any of the following:

(a) Comply with federal, state, or local laws, rules, or regulations.

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

(c) Cooperate with a law enforcement agency 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.

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

(e) 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.

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

(g) 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 activity described in this subdivision.

(h) Engage in public or peer-reviewed scientific or statistical research in the public interest that adheres to all other applicable ethics and privacy laws and is approved, monitored, and governed by an institutional review board or similar independent oversight entities that determine all of the following:

(*i*) If the deletion of the information is likely to provide substantial benefits that do not exclusively accrue to the controller.

(*ii*) If the expected benefits of the research outweigh the privacy risks.

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

(i) Assist another controller, processor, or third party with any of the obligations under this section.

(2) An obligation imposed on a controller or processor under this act does not restrict the controller's or processor's ability to collect, use, or retain data to do any of the following:

(a) Conduct internal research to develop, improve, or repair products, services, or technology if the controller or processor conducting that research obtains consent from the consumer and maintains the same security measures as otherwise required for that personal data.

(b) Effectuate a product recall.

(c) Identify and repair a technical error that impairs existing or intended functionality.

(d) Perform an internal operation that is reasonably aligned with an expectation of a consumer or reasonably anticipated based on the consumer's existing relationship with the controller or is

otherwise compatible with processing data in furtherance of the provision of a product or service specifically requested by a consumer or the performance of a contract to which the consumer is a party.

(3) A requirement imposed under this act does not apply if compliance by a controller or processor with that requirement would violate an evidentiary privilege under state law. This act does not prevent a controller or processor from providing a consumer's personal data to a person covered by an evidentiary privilege under state law as part of a privileged communication.

(4) A controller or processor that discloses personal data to a third-party controller or processor in compliance with this act does not violate this act if the third-party controller or processor that receives and processes the personal data violates this act, if, 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 that receives personal data from a controller or processor in compliance with this act does not violate this act if the controller or processor from which the third-party controller or processor received the personal data violated this act.

(5) This act does not impose an obligation on a controller or processor that adversely affects the rights or freedoms of any person, including, but not limited to, exercising the right of free speech, or apply to the processing of personal data by a person in the course of a purely personal or household activity.

(6) Except as otherwise provided in this act, personal data processed by a controller under this section must not be processed

for any purpose other than those expressly listed in this section. Personal data processed by a controller under this section may be processed to the extent that both of the following apply to that processing:

(a) The processing of the personal data is reasonably necessary and proportionate, or if the personal data is sensitive data, is strictly necessary, to the purposes described in this section.

(b) The processing of the personal data is adequate, relevant, and limited to what is necessary, or if the personal data is sensitive data, strictly necessary, in relation to the specific purposes described in this section. Personal data that is collected, used, or retained under subsection (2) must, if applicable, take into account the nature and purpose of the collection, use, or retention. The personal data is subject to reasonable administrative, technical, and physical measures to protect the confidentiality, integrity, and accessibility of the personal data and to reduce reasonably foreseeable risks of harm to consumers relating to the collection, use, or retention of personal data.

(7) If a controller processes personal data under an exemption in this section, the controller bears the burden of demonstrating that the processing qualifies for the exemption and complies with the requirements in subsection (6).

(8) The processing of personal data for the purposes in subsection (1) does not solely make a person a controller with respect to that processing.

Sec. 31. (1) Beginning on January 31, 2025, and on each January 31 thereafter, if for the previous calendar year a person

meets the definition of a data broker under this act, the person must register with the attorney general as a data broker.

(2) A person shall do all of the following when registering as a data broker:

(a) Pay a registration fee in an amount determined by the attorney general, not to exceed the reasonable costs of establishing and maintaining the informational website described in subsection (3).

(b) Provide all of the following information:

(*i*) Its name.

(*ii*) Its primary physical, email, and website addresses.

(*iii*) Any additional information or explanation that it chooses to provide concerning its data collection practices.

(3) The attorney general shall create a page on its website where the information provided by data brokers under subsection (2) is accessible by the public.

(4) The attorney general may bring a civil action under section 33 against a data broker that fails to register under this section.

(5) The registration fees received under this section must be deposited in the data broker registry fund created under section 39.

Sec. 33. (1) Before initiating a civil action under this act, if the attorney general has reasonable cause to believe that a person subject to this act has engaged in, is engaging in, or is about to engage in a violation of this act, the attorney general may initiate an investigation and may require the person or an officer, member, employee, or agent of the person to appear at a time and place specified by the attorney general to give

information under oath and to produce books, memoranda, papers, records, documents, or other relevant evidence in the possession, custody, or control of the person ordered to appear.

(2) When requiring the attendance of a person or the production of documents under subsection (1), the attorney general shall issue an order setting forth the time when and the place where attendance or production is required and shall serve the order on the person in the manner provided for service of process in civil cases at least 5 days before the date fixed for attendance or production. The order issued by the attorney general has the same force and effect as a subpoena. If a person does any of the following, the person may be ordered to pay a civil fine of not more than $5,000.00:

(a) Knowingly, without good cause, fails to appear when served with an order of the attorney general under this section.

(b) Knowingly avoids, evades, or prevents compliance, in whole or in part, with an investigation under this section, including the removal from any place, concealment, destruction, mutilation, alternation, or falsification of documentary material in the possession, custody, or control of the person subject to an order of the attorney general under this section.

(c) Knowingly conceals information that is relevant to the attorney general's investigation under this section.

(3) On application of the attorney general, an order issued by the attorney general under subsection (2), may be enforced by a court having jurisdiction over the person, Ingham County circuit court, or the circuit court of the county where the person receiving the order resides or is found in the same manner as though the notice were a subpoena. If a person fails or refuses to

obey the order issued by the attorney general under subsection (2), the court may issue an order requiring the person to appear before the court, to produce documentary evidence, or to give testimony concerning the matter in question. A failure to obey the order of the court is punishable by that court as contempt.

(4) Subject to subsections (5) and (6), if a person violates this act, the attorney general may bring a civil action seeking 1 or more of the following:

(a) If the violation is not a violation of section 31, a civil fine of not more than $7,500.00 for each violation.

(b) If the violation is a violation of section 31, 1 or more of the following:

(*i*) A civil fine of $100.00 for each day the data broker fails to register under section 31.

(*ii*) An amount equal to the registration fees that were due during the period the data broker failed to register under section 31.

(c) Expenses incurred by the attorney general in the investigation and prosecution of the civil action, including, but not limited to, attorney fees, as the court deems appropriate.

(d) Injunctive or declaratory relief.

(e) Any other relief the court deems appropriate.

(5) Except as otherwise provided in subsection (6), the attorney general shall not initiate an action under this section unless the attorney general provides notice as required under subdivision (a) and subdivision (b) does not apply:

(a) Before initiating an action under this section, the attorney general shall provide a person that the attorney general alleges has been or is violating this act 30 days' written notice

identifying the specific provisions of this act the attorney general alleges have been or are being violated.

(b) If, within 30 days of receiving the notice under subdivision (a), the person cures the noticed violations and provides the attorney general with an express written statement that the violations have been cured and further violations will not occur, the attorney general must not initiate a civil action against the person under this section.

(6) If a person continues to violate this act in breach of the express written statement under subsection (5) or if the person fails to cure a violation within 30 days after being notified of the alleged noncompliance, the attorney general may initiate a civil action under this section.

(7) A default in the payment of a civil fine or costs ordered under this act or an installment of the fine or costs may be remedied by any means authorized under chapter 40 or 60 of the revised judicature act of 1961, 1961 PA 236, MCL 600.4001 to 600.4065 and 600.6001 to 600.6098.

(8) A civil fine or expense collected under this section must be deposited in the consumer privacy fund created in section 37.

(9) The registration fees collected under this section must be deposited in the data broker registry fund created under section 39.

(10) If the attorney general commences a civil action under this act, the attorney general's filing fees for that action must be waived.

Sec. 35. (1) Subject to subsections (2) and (3), if a controller or processor processes a consumer's personal data in violation of this act, the consumer may bring a civil action

seeking 1 or more of the following:

(a) Actual damages.

(b) Injunctive or declaratory relief.

(c) Any other relief the court deems appropriate.

(2) Except as otherwise provided in subsection (3), a consumer shall not initiate an action under this section unless the consumer provides notice as required under subdivision (a) and subdivision (b) does not apply:

(a) Before initiating an action under this section, whether on an individual or class-wide basis, except as otherwise provided in this subdivision, a consumer shall provide a controller or processor that the consumer alleges has been or is violating this act 30 days' written notice identifying the specific provisions of this act the consumer alleges have been or are being violated. A consumer is not required to provide notice under this subdivision before initiating a civil action solely for actual pecuniary damages suffered as a result of the alleged violations.

(b) If, within 30 days of receiving the notice under subdivision (a), the controller or processor cures the noticed violations and provides the consumer with an express written statement that the violations have been cured and further violations will not occur, the consumer must not initiate a civil action against the controller or processor under this section.

(3) If the controller or processor continues to violate this act in breach of the express written statement under subsection (2) or if the controller or processor fails to cure a violation within 30 days after being notified of the alleged noncompliance, the consumer may initiate a civil action against the controller or processor to enforce the express written statement and pursue

damages for each breach of the express written statement and any other violation of this act that occurs after the express written statement.

(4) Unless expressly stated otherwise, this act does not relieve a person from any duty or obligation under any other law.

Sec. 37. (1) The consumer privacy fund is created within the state treasury.

(2) The state treasurer may receive money or other assets from any source for deposit into the fund. The state treasurer shall direct the investment of the fund. The state treasurer shall credit to the fund interest and earnings from fund investments.

(3) Money in the fund at the close of the fiscal year remains in the fund and does not lapse to the general fund.

(4) The department of attorney general is the administrator of the fund for auditing purposes.

(5) The department of attorney general shall expend money from the fund, subject to appropriation, to enforce the provisions of this act and to offset costs incurred by the attorney general in connection with this act.

(6) As used in this section, "fund" means the consumer privacy fund created under subsection (1).

Sec. 39. (1) The data broker registry fund is created within the state treasury.

(2) The state treasurer may receive money or other assets from any source for deposit into the fund. The state treasurer shall direct the investment of the fund. The state treasurer shall credit to the fund interest and earnings from fund investments.

(3) Money in the fund at the close of the fiscal year remains in the fund and does not lapse to the general fund.

(4) The department of attorney general is the administrator of the fund for auditing purposes.

(5) The department of attorney general shall expend money from the fund, subject to appropriation, to provide all of the following information on the website described under section 31:

(a) The name of the data broker and its primary physical, email, and website addresses.

(b) Any additional information or explanation that the data broker chooses to provide concerning its data collection practices.

(6) As used in this section, "fund" means the data broker registry fund created under subsection (1).

Enacting section 1. This act takes effect 1 year after the date it is enacted into law.