Senate Fiscal Agency
P.O. Box 30036
Lansing, Michigan 48909-7536

BILL ANALYSIS

Telephone: (517) 373-5383
Fax: (517) 373-1986

Senate Bill 659 (as introduced 11-9-24)
Sponsor: Senator Rosemary Bayer
Committee: Finance, Insurance, and Consumer Protection

Date Completed: 12-3-24

INTRODUCTION

The bill would establish consumers' rights related to the collection and use of personal data. It also would establish requirements of collectors and processors of personal data. Among other requirements, a collector would have to obtain consent from a consumer before processing the consumer's personal data and provide a privacy notice concerning the purpose of that data processing. The bill prescribes the scope of its provisions, specifying that its requirements would not apply to State agencies or collectors of medical data governed by the Health Insurance Portability and Accountability Act (HIPAA), nor to other specified data. The bill would allow the Attorney General and consumers to initiate civil actions for violations and would create the Data Broker Registry and two funds for administration of the bill's provisions.

FISCAL IMPACT

The bill would have an indeterminate fiscal impact on the Department of Attorney General and a minor, negative fiscal impact on State circuit courts. The Attorney General would incur expenses to create and post an online registry for data brokers; however, the bill would allow the Attorney General the discretion to adjust the registration fees to cover this expense. The fees would go into the Data Broker Registry Fund and could be used by the Attorney General to maintain the registry. The Fund would not lapse into the General Fund at the end of the fiscal year. Maintenance of the online registry is likely to cost less than its initial setup, so it could be possible that such fees for data brokers could be adjusted down in subsequent years after initial setup. The fees also would depend on the number of data brokers that registered. It is not known how many data brokers currently operate in Michigan. For comparison, Vermont and California created similar registries in 2018 and 2019, respectively, and as of July 2021, there were 348 registry entries in Vermont and 444 in California. Vermont charges a $100 annual registry fee.

The Attorney General also would incur investigation and litigation costs under the bill to the degree the Attorney General pursues violators of the bill. Similar to the regulatory structure for registration fees, civil fines of $5,000 for a failure to cooperate with an Attorney General investigation and civil fines of $7,500 for a violation of the bill would be deposited into the proposed Consumer Privacy Fund. The Attorney General would use the Fund to offset the costs to enforce the bill. Lastly, civil action filing fees for the Attorney General would be waived under the bill. This would save some minor litigation costs for the Attorney General, but circuit courts would not collect those fees.

The bill likely would not have a significant fiscal impact on the Department of Treasury. It is unlikely that the average balance of the Consumer Privacy Fund or the Data Broker Registry Fund would exceed $1.0 million during a fiscal year. Associated costs with managing funds would be relatively low and current appropriations likely would be sufficient,

Legislative Analyst: Nathan Leaman
Fiscal Analyst: Elizabeth Raczkowski
Michael Siracuse

CONTENT

The bill would enact the "Personal Privacy Data Act" to do the following:

- **-- Prescribe specific rights of consumers related to a person's collection and use of their personal data in the course of business, including the right to obtain copies of collected data, have collected data deleted, and opt out of the use of data for specific purposes like targeted advertising.**
- **-- Specify that the bill's provisions would apply to a person that performed business in the State, a person that controlled or processed personal data of at least 100,0000 consumers, or a person that controlled or processed personal data of at least 25,000 consumers and derived revenue from the sale of personal data.**
- **-- Specify that the bill's provisions would not apply to certain entities, such as State agencies, institutions of higher education, or entities governed by HIPAA.**
- **-- Specify that the bill's provisions would not apply to certain data, such as protected health information under HIPAA and data collected in compliance with other Federal laws.**
- **-- Prohibit a controller of a consumer's data from processing personal data concerning a consumer without obtaining the consumer's consent.**
- **-- Prescribe the process for consumers to invoke the rights afforded by the bill with a request to a controller concerning the consumer's data.**
- **-- Require a controller of a consumer's data to provide a consumer with a privacy notice about the use of the consumer's data and prescribe the requirements of the notice.**
- **-- Require a consumer's data processor to assist the controller in meeting its obligations under the bill.**
- **-- Require a controller to conduct and document a data protection impact assessment on the use of the personal data it collects and processes.**
- **-- Prescribe requirements for a controller in possession of de-identified data.**
- **-- Specify that the bill would not restrict a controller's ability to use data for certain purposes, such as for compliance with State, Federal, or local laws or to conduct internal research or product recalls, among other things.**
- **-- Create the Data Broker Registry and require data brokers to register with the Attorney General.**
- **-- Allow the Attorney General and consumers to initiate a civil action for violations of the bill under certain circumstances.**
- **-- Prescribe civil fines for violations of the bill.**
- **-- Create the Consumer Privacy Fund in the State Treasury and require civil fines under the bill to be deposited into the Fund.**
- **-- Create the Data Broker Registry Fund in the State Treasury and require registration fees from the Data Broker Registry to be deposited into the Fund.**

The bill would take effect one year after its enactment.

Definitions

"Affiliate" would mean, except as otherwise provided, a person that controls, is controlled by, or is under common control with another person or shares common branding with another person. As used above, "control" or "controlled" means any of the following:

- -- Ownership of, or the power to vote, more than 50% of the outstanding shares of any class of voting security of a company.
- -- Control in any manner over the election of a majority of the directors or of individuals exercising similar functions.
- -- The power to exercise controlling influence over the management of a company.

"Authenticate" would mean verifying through reasonable means that a consumer, entitled to exercise the consumer rights under the bill, is the same consumer exercising those consumer rights with respect to the personal data at issue.

"Biometric data" would mean 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. The term would not include any of the following:

-- A physical or digital photograph.
-- A video or audio recording.
-- Any data generated from a physical or digital photograph, or a video or audio recording, unless the data was generated to identify a specific individual.

"Business associate" would mean that term as defined in 45 CFR 160.103: generally, a person who creates, receives, maintains, or transmits protected health information for a function or activity regulated under the law on behalf of another entity or provides management, administrative, accreditation, or financial services for another entity, or to or for an organized health care arrangement in which the other entity participates, where the provision of the service involves the disclosure of protected health information from the other entity.

"Child" would mean an individual who is less than 13 years of age.

"Collects", "collected", or "collection" would mean buying, renting, gathering, obtaining, receiving, or accessing personal data pertaining to a consumer by any means. The terms would include receiving personal data from the consumer, either actively or passively, or observing the consumer's behavior.

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

-- The acceptance of a general or broad terms of use or similar document that contained any description of personal data processing and other unrelated information.
-- The act of hovering over, muting, pausing, or closing a given piece of content.
-- An agreement obtained through the use of dark patterns.

"Consumer" would mean an individual who was a resident of the State acting in an individual or household context. Consumer would not include an individual acting in a commercial or employment context.

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

"Covered entity" would mean a health plan, a health plan clearinghouse, or a health care provider who transmitted any health information in electronic form.

"Cross-context behavioral advertising" would mean 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.

"Dark pattern" would mean a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making, or choice.

"Data broker" would mean 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.

"Decisions that produce legal or similarly significant effects concerning a consumer" would mean 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.

"De-identified data" would mean data that cannot reasonably be linked to an identified or identifiable individual, or to a device linked to that individual. "Identified or identifiable individual" would mean an individual who can be readily identified, directly or indirectly.

"Institution of higher education" would mean a degree- or certificate-granting public or private college or university, junior college, or community college located in the State.

"Institutional review board" would mean any board, committee, or other group formally designated by an institution to review, to approve the initiation of, and to conduct periodic review of, biomedical research involving human subjects.

"Person" would mean an individual or a partnership, corporation, limited liability company, association, governmental entity, or other legal entity.

"Personal data" would mean information that is linked or reasonably linkable to an identified or identifiable individual. Personal data would not include de-identified data or publicly available information.

"Precise geolocation data" would mean 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 would 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.

"Process" or "processing" would mean 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.

"Processor" would mean a person that processes personal data on behalf of a controller.

"Profiling" would mean 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.

"Pseudonymous data" would mean 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.

"Publicly available information" would mean 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.

"Sale of personal data" would mean the exchange of personal data for monetary or other valuable consideration by a controller to a third party. Sale of personal data would not include any of the following:

-- The disclosure of personal data to a processor that processed the personal data on behalf of the controller.
-- The disclosure of personal data to a third party for the purpose of providing a product or service requested by the consumer.
-- The disclosure or transfer of personal data to an affiliate of the controller.
-- 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.
-- The disclosure or transfer of personal data to a third party as an asset that was part of a merger, acquisition, bankruptcy, or other transaction, or a proposed merger, acquisition, bankruptcy, or other transaction, in which the third party assumed or would assume control of all or part of the controller's assets.

"Sensitive data" would mean a category of personal data that includes all the following:

-- Personal data revealing racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status.
-- Genetic or biometric data for the purpose of uniquely identifying an individual.
-- Personal data collected from a known child.
-- Precise geolocation data.
-- A consumer's Social Security number.
-- A consumer's driver license number, official state personal identification card number, or passport number.
-- 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.
-- 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.

"Share" would mean 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.

"State agency" would mean a State department, agency, bureau, division, section, board, commission, trustee, authority, or officer that is created by the Michigan State Constitution, statute, or State agency action.

"Subprocessor" would mean 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.

"Targeted advertising" would mean 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. The term would not include any of the following:

-- Advertisements based on activities within a controller's own websites or online applications.
-- Advertisements based on the context of a consumer's current search query, visit to a website, or online application.
-- Advertisements directed to a consumer in response to the consumer's request for information or feedback.
-- Processing personal data solely for the purpose of measuring or reporting advertising performance, reach, or frequency.

"Third party" would mean a person other than the consumer, controller, processor, or an affiliate of the controller or processor.

Application

The bill would apply to a person that did any of the following:

-- Conducted business in the State or produced products or services that were targeted to residents of the State.
-- During a calendar year, controlled or processed personal data of at least 100,000 consumers.
-- During a calendar year, controlled or processed personal data of at least 25,000 consumers and derived any revenue from the sale of personal data.

The Act would not apply to any of the following:

-- A State agency or any other political subdivision of the State.
-- A financial institution or an affiliate of a financial institution that was subject to Title V of the Gramm-Leach-Bliley Act and the regulations promulgated under that Act.
-- A covered entity or business associate governed by the privacy, security, and breach notification rules under the HIPAA, the regulations promulgated under HIPAA, and the Health Information Technology for Economic and Clinical Health Act.
-- An institution of higher education.
-- An entity that was subject to or regulated under the Insurance Code.
-- A nonprofit organization that operated to detect or prevent insurance-related crimes, including insurance fraud.
-- A nonprofit dental care corporation operating under State law.
-- A third-party administrator as defined the Third Party Administrator Act: a person that directly or indirectly processes claims under a service contract and that may also provide one or more other administrative services under a service contract, other than under a worker's compensation self-insurance program.

The following information and data would be exempt from the bill:

-- Protected health information under HIPAA and the regulations promulgated under HIPAA.
-- A record that was a medical record as defined in the Medical Records Access Act: information oral or recorded in any form or medium that pertains to a patient's health care, medical history, diagnosis, prognosis, or medical condition and that is maintained by a health care provider or health facility in the process of caring for the patient's health.
-- Patient identifying information for purposes of Federal law.
-- Identifiable private information for the purpose of the Federal policy for the protection of human subjects; identifiable private information that was 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 (Protection of Human Subjects) and 56 (Institutional Review Boards); personal data used or shared in research conducted in accordance with the requirements under the bill, or other research conducted in accordance with applicable law.

-- Information and documents created for purposes of the Health Care Quality Improvement Act.
-- Patient safety work product for purposes of the Patient Safety and Quality Improvement Act.
-- Information derived from any of the health care-related information listed in the bill that was de-identified in accordance with the requirements for de-identification under HIPAA.
-- Information originating from, and intermingled to be indistinguishable with, or information treated in the same manner as information exempt under the bill that was maintained by a covered entity, business associate, program, or qualified service organization. As used in this subdivision, "program" and "qualified service organization" would mean those terms as defined in 42 CFR 2.11; "program" means a person that holds itself out as providing substance use treatment, an identified unit within a general medical facility that provides such treatment, and medical personnel providing such treatment; "qualified service organization" means a person providing services to a program.
-- Information used only for public health activities and purposes as authorized under HIPAA.
-- 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 provided information for use in a consumer report, and by a user of a consumer report, but only to the extent that the activity was regulated by and authorized under the Federal Fair Credit Reporting Act.
-- Personal data collected, processed, sold, or disclosed in compliance with the Federal Driver's Privacy Protection Act.
-- Personal data regulated by the Federal Family Educational Rights and Privacy Act.
-- Personal data collected, processed, sold, or disclosed in compliance with Federal Farm Credit System.
-- Data that were subject to Title V of the Gramm-Leach-Bliley Act and the regulations promulgated under that Act.

Additionally, information or data would be exempt from the bill if it were 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. In this context, "advanced driver assistance system" would mean either of the following:

-- A driver support feature on a vehicle that can assist an individual with steering, or braking or accelerating, but not both simultaneously.
-- A driver support feature on a vehicle that can control steering and braking or accelerating, simultaneously, under certain circumstances.

"Automated driving system" would mean 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.

Data also would be exempt under the bill if it were processed or maintained for any of the following purposes:

-- 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 was collected and used within the context of that role.
-- As the emergency contact information of an individual for emergency contact purposes.
-- That was 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.
-- That was necessary in any matter relating to an unemployment benefit claim or appeal under the Michigan Employment Security Act.

Finally, a controller or processor that complied with the verifiable parental consent requirements of the Children's Online Privacy Protection Act would satisfy any obligation to obtain parental consent under the bill.

Consumer Rights

A consumer could invoke the consumer rights authorized under the bill at any time by submitting a request to a controller specifying the consumer rights that the consumer wished to invoke. A known child's parent or legal guardian could invoke the consumer rights on behalf of the child regarding processing personal data belonging to the known child. Except as otherwise provided in the bill, a controller would have to comply with an authenticated request by a consumer to exercise the consumer rights authorized under the bill.

A consumer would have all the following rights:

-- To confirm whether or not the controller was processing the consumer's personal data and to access the personal data.
-- 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.
-- Except as otherwise provided in the bill, to delete personal data provided by or obtained about the consumer.
-- 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 allowed the consumer to transmit the data to another controller without hindrance, where the processing was carried out by automated means.

A consumer also would have the right to opt out of the processing of the personal data for any of the following purposes:

-- Targeted advertising.
-- The sale of personal data.
-- Profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer.

Controller's Response to Consumer's Request

All the following would apply to a controller complying with a consumer's request specifying the rights the consumer wished to invoke.

A controller would have to respond to a consumer without undue delay and within 45 days after receipt of the request. The response period would have to 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 informed the consumer of the extension within the initial 45-day response period, together with the reason for the extension.

If a controller declined to take action regarding a consumer's request, the controller would have to inform the consumer without undue delay and 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.

Information provided in response to a consumer request would have to be provided by a controller free of charge, up to twice annually per consumer. If requests from a consumer were manifestly unfounded, excessive, or repetitive, the controller could 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 would bear the burden of demonstrating that a request was manifestly unfounded, excessive, or repetitive.

If a controller were unable to authenticate the request using commercially reasonable efforts, the controller would not be required to comply with the request and could ask a consumer to provide additional information that was reasonably necessary to authenticate the consumer and the consumer's request.

A controller that obtained personal data about a consumer from a source other than the consumer would have complied with a request to delete personal data under the bill if the controller acted in accordance with either of the following:

-- The controller retained a record of the request, retained the minimum data necessary to ensure that the consumer's personal data remained deleted from the controller's records, and did not use the retained data for any other purpose authorized under the bill.
-- The controller did not process the personal data for targeted advertising, the sale of personal data, or profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer.

A controller would have to establish a process for a consumer to appeal the controller's refusal to take action on a request within a reasonable period of time after the consumer's receipt of the decision. The appeal process would have to be conspicuously available and similar to the process for submitting requests to initiate action by invoking the consumer rights. No more than 60 days after the receipt of an appeal, a controller would have to 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 were denied, the controller would have to provide the consumer with an online mechanism, if available, or other method through which the consumer could contact the attorney general to submit a complaint.

Controller’s Responsibilities

Under the bill, a controller would be prohibited from processing personal data concerning a consumer without obtaining the consumer's consent.

A controller also would have to do all the following:

-- Provide an effective mechanism for a consumer to revoke the consumer's consent that was at least as easy to use as the mechanism used by the consumer to provide the consumer's original consent.
-- If consent were revoked by the consumer, cease to process data as soon as practicable, but no more than 15 days after the revocation of the consent.
-- If the personal data concerned a known child, process that data in accordance with the Children's Online Privacy Protection Act.
-- Except as otherwise provided in the bill, limit the collection of personal data to what was adequate, relevant, and reasonably necessary in relation to the purposes for which the

data was processed, unless the personal data was sensitive data, in which case the controller would have to limit the collection of the sensitive data to what was strictly necessary in relation to the purposes for which the sensitive data was processed.

-- Except as otherwise provided in the bill, at or before the point of collecting personal data, disclose to the consumer the purpose for which the personal data would be processed.
-- If the controller determined that collected data would be processed for a purpose other than what was initially disclosed to the consumer, disclose to the consumer the additional purpose for which the data would be processed and obtain the consumer's consent to process the data for that additional purpose.
-- Establish, implement, and maintain technical and organizational measures to protect the confidentiality, integrity, and accessibility of personal data, which would have to be appropriate to the volume and nature of the personal data at issue.
-- Permanently and completely delete personal data in response to a consumer's request to delete that information unless retention of the personal data was required by law.
-- Not retain personal data in a form that permitted identification of the consumer for longer than the period that was reasonably necessary for the purposes for which the personal data was processed unless retention was otherwise required by law or under the bill.
-- Not retain sensitive data in a form that permitted identification of the consumer for longer than the period that was strictly necessary for the purpose for which the sensitive data was processed unless retention was otherwise required by law.
-- If a consumer had opted out of the processing of the consumer's personal data under the bill, notify any processor or third party to which the controller sold or otherwise disclosed the consumer's personal data that the consumer had opted out of the processing of the consumer's personal data.
-- If the controller had actual knowledge or willfully disregarded that the consumer was between 13 and 18 years of age, not process the personal date for the purpose of targeted advertising or sell the consumer's personal data without the consumer's consent.

Additionally, the controller could not process personal data in violation of any State and Federal law that prohibited unlawful discrimination against a consumer. A controller could not discriminate against a consumer for exercising any of the consumer rights under the bill, 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 the bill would require a controller to provide a product or service that required the personal data of a consumer that the controller did not collect or maintain or 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 had exercised the consumer's right to opt out under the bill or the offer was 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 was proportional to the benefit received by the controller in collecting personal information from the reward, feature, discount, or program.

The bill stipulates that any provision of a contract or agreement of any kind that purported to waive or limit in any way the consumer rights under the bill would be contrary to public policy and would be void and unenforceable.

Controller's Privacy Notice to Consumers

Under the bill, a controller would have to provide a consumer with a reasonably accessible, clear, and meaningful privacy notice that included all the following:

-- The categories of personal data processed by the controller.
-- The purpose for processing personal data.

-- A list of the consumer rights under the bill.
-- A summary of how the consumer could exercise the consumer rights under the bill, including a description of the secure and reliable means established under the bill and a summary of how the consumer could appeal a controller's decision with regard to the consumer's request.
-- The categories of personal data that the controller sold to or shared with third parties, if any.
-- The categories of third parties, if any, with whom the controller sold or shared personal data.
-- That a controller or processor could use personal data to conduct internal research to develop, improve, or repair products, services, or technology, if the controller or processor conducting that research obtained consent from the consumer and maintained the same security measures as otherwise required for that personal data.
-- The contact information of the controller, including an active email address or other online mechanism that the consumer could use to contact the controller.
-- The length of time the controller intended to retain each category of personal data, or, if that was impossible to determine, the criteria used by the controller to determine the length of time that the controller intended to retain each category of personal data.
-- The date that the privacy notice was last updated by the controller.
-- If a controller engaged in profiling in furtherance of decisions that produced legal or similarly significant effects concerning a consumer, a disclosure of that fact, a summary of how the profiling was used in the decision-making process, and the benefits and potential consequences of the decision concerning the consumer.

A controller would have to make its privacy notice available to the public in each language that the controller provided a product or service that was subject to the privacy notice or carried out activities related to the product or service.

A controller would have to ensure that its privacy notice could be accessed and used by individuals with disabilities. Except as otherwise provided in the bill, a controller would have to 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.

If a controller did not have a website, the controller would have to make its privacy notice available through a medium regularly used by the controller to interact with consumers.

If a controller made a material change to its privacy notice, the controller would be required to directly notify each consumer affected by the material change before implementing the material change, and if the material change related to the collection, processing, or sale of personal data, ensure that the controller obtained consent for use of data in that manner.

A controller would not be required to provide a separate privacy notice applicable to the State if the controller's privacy notice otherwise complied with the bill.

Secure and Reliable Means for Consumers to Make a Request

A controller would have to establish one or more secure and reliable means for a consumer to submit a request to exercise the consumer rights under the bill. The secure and reliable means would have to account for the ways in which a consumer normally interacted with the controller, the need for secure and reliable communication of requests to exercise the consumer rights under the bill, and the ability of the controller to authenticate the identity of the consumer making the request. A controller could not require a consumer to create a new

account to exercise the consumer rights, but could require a consumer to use an existing account.

Requirements of Controller's Processors

A processor would have to adhere to the instructions of a controller and would have to assist the controller in meeting its obligations under the bill. The assistance provided by a processor to a controller would have to include all the following:

-- 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.
-- 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, taking into account the nature of processing and the information available to the processor.
-- Providing necessary information to enable the controller to conduct and document data protection impact assessments under the bill.

A contract between a controller and a processor would have to govern the processor's data processing procedures with respect to processing performed on behalf of the controller. The contract would have to 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 would have to include requirements that the processor do all the following:

-- Ensure that each person processing personal data would be subject to a duty of confidentiality with respect to the data.
-- 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 was required by law.
-- 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 the bill.
-- Engage any subprocessor under a written contract that required the subprocessor to meet the obligations of the processor with respect to the personal data.
-- Require the processor to notify the controller of its engagement with any subprocessor.

The contract also would have to include requirements that the processor do either of the following:

-- 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 the bill.
-- 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 the bill using an appropriate and accepted control standard or framework and assessment procedure for those assessments; the processor would have to provide a report of the assessment to the controller on request.

The bill would not relieve a controller or a processor from the liabilities imposed on it by virtue of its role in the processing relationship under the bill.

Determining whether a person was acting as a controller or processor with respect to a specific processing of data would be a fact-based determination that depended on the context in which personal data was to be processed. A processor that continued to adhere to a controller's instructions with respect to a specific processing of personal data would remain a processor.

Data Protection Impact Assessment

A controller would have to conduct and document a data protection impact assessment of each of the following processing activities involving personal data:

-- The processing of personal data for purposes of targeted advertising.
-- The sale of personal data.
-- The processing of sensitive data.
-- Any processing activities involving personal data that present a heightened risk of harm to consumers.

A controller also would have to conduct and document a data protection impact assessment of processing of personal data for the purpose of profiling, if the profiling presented a reasonably foreseeable risk of any of the following:

-- Unfair or deceptive treatment of, or unlawful disparate impact on, consumers.
-- Financial, physical, or reputational injury to consumers.
-- 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.
-- Other substantial injury to consumers.

A data protection impact assessment would have to identify and weigh the benefits that could 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 could 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 would be processed, would have to be factored into the assessment by the controller.

The Attorney General could request that a controller disclose any data protection impact assessment that was relevant to an investigation conducted by the Attorney General, and the controller would have to make the data protection impact assessment available to the Attorney General. The Attorney General could evaluate the data protection impact assessment for compliance with the responsibilities set forth in the bill. A data protection impact assessment would be confidential and exempt from public inspection and copying under the Freedom of Information Act. The disclosure of a data protection impact assessment in accordance with a request from the Attorney General would not constitute a waiver of attorney-client privilege or work product protection with respect to the assessment and any information contained in the assessment.

A single data protection impact assessment could address a comparable set of processing operations that include similar activities. A data protection impact assessment conducted by a controller for the purpose of complying with other laws or regulations could satisfy the requirements of the bill if the assessment had a reasonably comparable scope and effect.

The data protection impact assessment requirements would apply to processing activities created or generated after January 1, 2025, and would not be retroactive.

Requirements of Controller's Possession of De-identified Data

A controller in possession of de-identified data would have to do all the following:

-- Take reasonable measures to ensure that the data could not be associated with an individual.
-- Publicly commit to maintaining and using de-identified data without attempting to re-identify the data.
-- Contractually obligate any recipients of the de-identified data to comply with all provisions of the bill.

The bill would 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.

A controller or processor would not be required to comply with an authenticated consumer rights request under the bill if all of the following applied:

-- The controller was 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.
-- The controller did 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.
-- The controller did 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 the bill.

These consumer rights and requirements would not apply to pseudonymous data if the controller were able to demonstrate that any information necessary to identify the consumer was kept separately and was subject to effective technical and organizational measures that prevented the controller from accessing the information.

A controller that disclosed pseudonymous data or de-identified data would have to exercise reasonable oversight to monitor compliance with any contractual commitments to which the pseudonymous data or de-identified data was subject and would have to take appropriate steps to address any breaches of those contractual commitments.

Unrestricted Activity of a Controller

The bill would not restrict a controller's or processor's ability to do any of the following:

-- Comply with Federal, State, or local laws, rules, or regulations.
-- Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by Federal, State, local, or other governmental authorities.
-- Cooperate with a law enforcement agency concerning conduct or activity that the controller or processor reasonably and in good faith believed may violate federal, state, or local laws, rules, or regulations.
-- Investigate, establish, exercise, prepare for, or defend legal claims.
-- Provide a product or service specifically requested by a consumer, perform a contract to which the consumer was a party, including fulfilling the terms of a written warranty, or take steps at the request of the consumer before entering a contract.

-- Take immediate steps to protect an interest that was essential for the life or physical safety of the consumer or another individual, and where the processing could not be manifestly based on another legal basis.
-- 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 of these activities.
-- Assist another controller, processor, or third party with any obligations under the bill.

The bill also would not restrict a controller from engaging in public or peer-reviewed scientific or statistical research in the public interest that adhered to all other applicable ethics and privacy laws and was approved, monitored, and governed by an institutional review board or similar independent oversight entities that determine all the following:

-- If the deletion of the information were likely to provide substantial benefits that do not exclusively accrue to the controller.
-- If the expected benefits of the research outweighed the privacy risks.
-- If the controller had implemented reasonable safeguards to mitigate privacy risks associated with research, including any risks associated with re-identification.

An obligation imposed on a controller or processor under the bill would not restrict the controller's or processor's ability to collect, use, or retain data to do any of the following:

-- Conduct internal research to develop, improve, or repair products, services, or technology if the controller or processor conducting that research obtained consent from the consumer and maintained the same security measures as otherwise required for that personal data.
-- Effectuate a product recall.
-- Identify and repair a technical error that impaired existing or intended functionality.
-- Perform an internal operation that was reasonably aligned with an expectation of a consumer or reasonably anticipated based on the consumer's existing relationship with the controller or was 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 was a party.

A requirement imposed under the bill would not apply if compliance by a controller or processor with that requirement would violate an evidentiary privilege under State law. The bill would 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.

A controller or processor that disclosed personal data to a third-party controller or processor in compliance with the bill would not violate the bill if the third-party controller or processor that received and processed the personal data violated the bill, 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 received personal data from a controller or processor in compliance with the bill would not violate the Act if the controller or processor from which the third-party controller or processor received the personal data violated the bill.

The bill would not impose an obligation on a controller or processor that adversely affected the rights or freedoms of any person, including 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.

Except as otherwise provided in the bill, personal data processed by a controller under the bill could not be processed for any purpose other than those expressly listed below. Personal data processed by a controller under the bill could be processed to the extent that the following applied to that processing:

-- The processing of the personal data was reasonably necessary and proportionate, or if the personal data were sensitive data, was strictly necessary for the purposes described above.
-- The processing of the personal data was adequate, relevant, and limited to what was necessary, or if the personal data were sensitive data, strictly necessary, in relation to the specific purposes described here.

Personal data that was collected, used, or retained as described above would have to consider the nature and purpose of the collection, use, or retention. The personal data would be 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.

If a controller processed personal data under an above exemption, the controller would bear the burden of demonstrating that the processing qualified for the exemption and complied with the requirements above.

Data Broker Registry

Beginning on January 31, 2025, and each January 31 after, if for the previous calendar year a person met the definition of a data broker under the bill, the person would have to register with the Attorney General as a data broker. When registering, a person would have to pay a registration fee in an amount determined by the Attorney General, not to exceed reasonable costs to establish and maintain the webpage described below, and provide the person's name, primary physical, email, and website addresses, and any additional information that the person chose to provide concerning its data collection practices.

The Attorney General would have to create a page on its website where the information provided above would be accessible by the public. The Attorney General could bring a civil action against a data broker that failed to register. The registration fees received from data brokers would have to be deposited in the Data Broker Registry Fund created by the bill.

Attorney General Civil Action Requirements

Before initiating a civil action under the bill, if the Attorney General had reasonable cause to believe that a person subject to the bill had engaged in, was engaging in, or was about to engage in a violation of bill, the Attorney General could initiate an investigation and could 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.

When requiring the attendance of a person or the production of documents, the Attorney General would have to issue an order setting forth the time when and the place where attendance or production was required and would have to serve the order on the person in the manner provided for service of process in civil cases at least five days before the date fixed for attendance or production. The order would have the same force and effect as a subpoena. If a person did any of the following, the person could be ordered to pay a maximum civil fine of $5,000:

-- Knowingly, without good cause, failed to appear when served with an order.
-- Knowingly avoided, evaded, or prevented compliance, in whole or in part, with an investigation under the bill, 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.
-- Knowingly concealed information that was relevant to the Attorney General's investigation.

On application of the Attorney General, an order could 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 resided or was found in the same manner as though the notice were a subpoena. If a person failed or refused to obey the order, the court could 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 would be punishable by that court as contempt.

Subject to provisions below, if a person violated the bill, the Attorney General could bring a civil action seeking one or more of the following:

-- If the violation were not a violation of the bill's Data Broker Registry requirements, a civil fine of up to $7,500 for each violation.
-- If the violation were a violation of the bill's Data Broker Registry requirements, a civil fine of $100 for each day the broker failed to register or an amount equal to the registration fees due during the period the broker failed to register, or both.
-- Expenses incurred by the Attorney General in the investigation and prosecution of the civil action, including attorney fees as the court deems appropriate.
-- Injunctive or declaratory relief.
-- Any other relief the court deemed appropriate.

Except as otherwise provided below, the Attorney General could not initiate an action under the bill unless the Attorney General provided notice as required below and the second bullet did not apply:

-- The attorney general would have to provide a person alleged of being in violation of the bill 30 days' written notice identifying the specific provisions of the bill the Attorney General alleged had been or were being violated.
-- If, within 30 days of receiving the notice, the person cured the noticed violations and provided the Attorney General with an express written statement that the violations had been cured and further violations would not occur, the Attorney General could not initiate a civil action against the person.

If a person continued to violate the bill in breach of the express written statement above or if the person failed to cure a violation within 30 days after being notified of the alleged noncompliance, the Attorney General could initiate a civil action.

A default in the payment of a civil fine or costs ordered under the bill or an installment of the fine or costs could be remedied by any means authorized under the Revised Judicature Act. A civil fine or expense collected under the bill would have to be deposited in the Consumer Privacy Fund created by the bill. If the Attorney General commenced a civil action under the bill, the filing fees for that action would have to be waived.

Consumer Right to Civil Action

If a controller or processor processed a consumer's personal data in violation of the bill, the

consumer could bring a civil action seeking actual damages, injunctive or declaratory relief, or any other relief the court deemed appropriate.

A consumer could not initiate an action under the bill unless the consumer provided notice as required below and the second bullet did not apply:

-- Before initiating an action, whether on an individual or class-wide basis, except as otherwise provided, a consumer would have to provide a controller or processor that the consumer alleged had been or was violating the bill 30 days' written notice identifying the specific provisions of the bill that the consumer alleged had been or were being violated.
-- If, within 30 days of receiving notice, the controller or processor cured the noticed violations and provided the consumer with an express written statement that the violations had been cured and further violations would not occur, the consumer could not initiate a civil action against the controller or processor.

If the controller or processor continued to violate the bill in breach of the express written statement or if the controller or processor failed to cure a violation within 30 days after being notified of the alleged noncompliance, the consumer could 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 the bill that occurred after the express written statement.

Creation of the Consumer Privacy Fund and the Data Broker Registry Fund

The bill would create the Consumer Privacy Fund and the Data Broker Registry Fund within the State Treasury. The State Treasurer could receive money or other assets from any source for deposit into the Funds. The State Treasurer would have to direct the investment of the Funds and credit to the them interest and earnings from their respective investments. Money in the Funds at the close of the fiscal year would remain in the respective Funds and would not lapse to the General Fund. The Department of Attorney General would be the administrator of each Fund for auditing purposes.

The Department of Attorney General would have to spend money from the Consumer Privacy Fund, subject to appropriation, to enforce the provisions of the bill and to offset costs incurred by the bill. The Department would have to spend money from the Data Broker Registry Fund, subject to appropriation, to provide all the following information on the data broker registry webpage:

-- The name of the data broker and its primary physical, email, and website addresses.
-- Any additional information or explanation that the data broker chose to provide concerning its data collection practices.

SAS\S2324\s659sa