State of Wisconsin
2023 - 2024 LEGISLATURE

LRB-2054/1
MDE:cdc

2023 BILL

AN ACT ***to create*** 134.985 of the statutes; **relating to:** consumer data protection and providing a penalty.

Analysis by the Legislative Reference Bureau

This bill establishes requirements for controllers and processors of the personal data of consumers. The bill defines a "controller" as a person that, alone or jointly with others, determines the purpose and means of processing personal data, and the bill applies to controllers that control or process the personal data of at least 100,000 consumers or that control or process the personal data of at least 25,000 consumers and derive over 50 percent of their gross revenue from the sale of personal data. Under the bill, "personal data" means any information that is linked or reasonably linkable to an individual except for publicly available information.

The bill provides consumers with the following rights regarding their personal data: 1) to confirm whether a controller is processing the consumer's personal data and to access the personal data; 2) to correct inaccuracies in the consumer's personal data; 3) to require a controller to delete personal data provided by or about the consumer; 4) to obtain a copy of the personal data that the consumer previously provided to the controller; and 5) to opt out of the processing of the consumer's personal data for targeted advertising; the sale of the consumer's personal data; and certain forms of automated processing of the consumer's personal data. These rights are subject to certain exceptions specified in the bill. Controllers may not discriminate against a consumer for exercising rights under the bill, including by charging different prices for goods or providing a different level of quality of goods or services.

BILL

The bill requires controllers to respond to consumers' requests to invoke rights under the bill without undue delay. If a controller declines to take action regarding a consumer's request, the controller must inform the consumer of its justification without undue delay. The bill also requires that information provided in response to a consumer's request be provided free of charge once annually per consumer. Controllers must also establish processes for consumers to appeal a refusal to take action on a consumer's request. Within 60 days of receiving an appeal, a controller must 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 its decisions. If the appeal is denied, the controller must provide the consumer with a method through which the consumer can contact the attorney general to submit a complaint.

Under the bill, a controller must provide consumers with a privacy notice that discloses the categories of personal data processed by the controller; the purpose of processing the personal data; the categories of third parties, if any, with whom the controller shares personal data; the categories of personal data that the controller shares with third parties; and information about how consumers may exercise their rights under the bill. Controllers may not collect or process personal data for purposes that are not relevant to or reasonably necessary for the purposes disclosed in the privacy notice. The bill's requirements do not restrict a controller's ability to collect, use, or retain data for conducting internal research, effectuating a product recall, identifying and repairing technical errors, or performing internal operations that are reasonably aligned with consumer expectations or reasonably anticipated on the basis of a consumer's relationship with the controller.

Persons that process personal data on behalf of a controller must adhere to a contract between the controller and the processor, and such contracts must satisfy certain requirements specified in the bill. The bill also requires controllers to conduct data protection assessments related to certain activities, including processing personal data for targeted advertising, selling personal data, processing personal data for profiling purposes, and processing sensitive data, as defined in the bill. The attorney general may request that a controller disclose a data protection assessment that is relevant to an investigation being conducted by the attorney general.

The attorney general has exclusive authority to enforce violations of the bill's requirements. A controller or processor that violates the bill's requirements is subject to a forfeiture of up to $7,500 per violation, and the attorney general may recover reasonable investigation and litigation expenses incurred. Before bringing an action to enforce the bill's requirements, the attorney general must first provide a controller or processor with a written notice identifying the violations. If within 30 days of receiving the notice the controller or processor cures the violation and provides the attorney general with an express written statement that the violation is cured and that no such further violations will occur, then the attorney general may not bring an action against the controller or processor. The bill also prohibits cities, villages, towns, and counties from enacting or enforcing ordinances that regulate the collection, processing, or sale of personal data.

BILL

For further information see the state fiscal estimate, which will be printed as an appendix to this bill.

The people of the state of Wisconsin, represented in senate and assembly, do enact as follows:

SECTION 1. 134.985 of the statutes is created to read:

134.985 Consumer data protection. (1) DEFINITIONS. In this section:

(a) "Affiliate" means a legal entity that controls, is controlled by, or is under common control with another legal entity or shares common branding with another legal entity. For the purposes of this definition, "control" or "controlled" means ownership of, or the power to vote, more than 50 percent 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; or the power to exercise controlling influence over the management of a company.

(b) "Authenticate" means verifying through reasonable means that the consumer, entitled to exercise his or her consumer rights under sub. (2), is the same consumer exercising such consumer rights with respect to the personal data at issue.

(c) "Biometric data" means data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that are used to identify a specific individual. "Biometric data" does not include a physical or digital photograph, a video or audio recording or data generated therefrom, or information collected, used, or stored for health care treatment, payment, or operations under the federal Health Insurance Portability and Accountability Act of 1996.

(d) "Business associate" has the meaning given in 45 CFR 160.103.

(e) "Child" means an individual younger than 13 years of age.

(f) "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.

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

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

(i) "Covered entity" has the meaning given in 45 CFR 160.103.

(ja) "Cures Act" means the federal 21st Century Cures Act and valid federal regulations enacted pursuant to such provisions.

(jg) "Decisions that produce legal or similarly significant effects concerning a consumer" means a decision made by the controller that results in the provision or denial by the controller of financial and lending services, housing, insurance, education enrollment, criminal justice, employment opportunities, health care services, or access to basic necessities, such as food and water.

(ka) "Deidentified data" means data that cannot reasonably be linked to an identified or identifiable individual, or a device linked to such person.

(kb) "Identified or identifiable individual" means a person who can be readily identified, directly or indirectly.

(La) "HIPAA" means the federal Health Insurance Portability and Accountability Act and valid federal regulations enacted pursuant to the act, including 45 CFR 164.500 to 164.534.

(Lg) "HITECH" means the federal Health Information Technology for Economic and Clinical Health Act and valid federal regulations enacted pursuant to the act.

(m) "Institution of higher education" has the meaning given in s. 39.32 (1) (a).

(n) "Nonprofit organization" means any corporation organized under ch. 181, any organization identified under s. 895.486 (2) (e), or any organization exempt from taxation under section 501 (c) (3), (6), or (12) of the Internal Revenue Code.

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

(p) "Precise geolocation data" means information derived from technology, including 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 any data generated by or connected to advanced utility metering infrastructure systems or equipment for use by a utility.

(q) "Process" or "processing" means any operation or set of operations performed, whether by manual or automated means, on personal data or on sets of personal data, such as the collection, use, storage, disclosure, analysis, deletion, or modification of personal data.

(r) "Processor" means an individual or person that processes personal data on behalf of a controller.

(s) "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.

(t) "Pseudonymous data" means personal data that cannot be attributed to a specific individual without the use of additional information, provided that such 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.

(u) "Publicly available information" means information that is lawfully made available through federal, state, or local government records, or information that a business 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.

(v) "Sale of personal data" means the exchange of personal data for monetary consideration by the controller to a 3rd party. "Sale of personal data" does not include any of the following:

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

2. The disclosure of personal data to a 3rd party for purposes of providing a product or service requested by the consumer.

3. The disclosure or transfer of personal data to an affiliate of the controller.

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

5. The disclosure or transfer of personal data to a 3rd party as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the 3rd party assumes control of all or part of the controller's assets.

(w) "Sensitive data" includes the following:

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

2. The processing of genetic or biometric data for the purpose of uniquely identifying an individual.

3. The personal data collected from a known child.

4. Precise geolocation data.

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

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

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

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

4. Processing personal data processed solely for measuring or reporting advertising performance, reach, or frequency.

(y) "Third party" means a person or association, authority, board, department, commission, independent agency, institution, office, society, or other body in state or

local government created or authorized to be created by the constitution or any law, other than a consumer, controller, processor, or an affiliate of the processor or the controller.

(z) "Trade secret" has the meaning given in s. 134.90.

(2) PERSONAL DATA RIGHTS; CONSUMERS. (a) A consumer may invoke the consumer rights authorized under this subsection at any time by submitting a request to a controller specifying the consumer rights the consumer wishes to invoke. A known child's parent or legal guardian may invoke such consumer rights on behalf of the child regarding processing personal data belonging to the known child. A controller shall comply with an authenticated consumer request to exercise any of the following rights:

1. To confirm whether or not a controller is processing the consumer's personal data and to access such personal data, unless such confirmation or access would require the controller to reveal a trade secret.

2. 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.

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

4. 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, provided such controller shall not be required to reveal any trade secret.

5. To opt out of the processing of the personal data for purposes of targeted advertising, the sale of personal data, or profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer.

(b) 1. Except as otherwise provided in this section, a controller shall comply with a request by a consumer to exercise the consumer rights authorized under par. (a).

2. A controller shall respond to a consumer without undue delay, but in all cases within 45 days of receipt of a request submitted under par. (a). 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, so long as the controller informs the consumer of any such extension within the initial 45–day response period, together with the reason for the extension.

3. If a controller declines to take action regarding a consumer's request, the controller shall inform the consumer without undue delay, but in all cases and at the latest within 45 days of receipt of the request, of the justification for declining to take action and instructions for how to appeal the decision under par. (c).

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

5. If a controller is unable to authenticate the request using commercially reasonable efforts, the controller may not be required to comply with a request to

initiate an action under par. (a) and may request that the consumer provide additional information reasonably necessary to authenticate the consumer and the consumer's request.

6. A controller that has obtained personal data about a consumer from a source other than the consumer shall be deemed in compliance with a consumer's request to delete the personal data under par. (a) 3. by doing any of the following:

a. Deleting the personal data, retaining a record of the request and the minimum data necessary to ensure the consumer's personal data remains deleted from the controller's records, and not using the retained data for any other purpose.

b. Not processing the consumer's personal data except as otherwise authorized under this section.

(c) 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 pursuant to par. (b) 3. The appeal process shall be conspicuously available and similar to the process for submitting requests to initiate action under par. (a). Within 60 days of receipt of an appeal, a controller shall inform the consumer in writing of any action taken or not taken in response to the appeal, including a written explanation of the reasons for the decisions. If the appeal is denied, the controller shall also provide the consumer with an online mechanism, if available, or other method through which the consumer may contact the attorney general to submit a complaint.

(3) DATA CONTROLLER RESPONSIBILITIES; TRANSPARENCY. (a) 1. A controller shall limit the collection of personal data to what is adequate, relevant, and reasonably necessary in relation to the purposes for which such data is processed, as disclosed to the consumer.

2. Except as otherwise provided in this section, a controller may not process personal data for purposes that are not reasonably necessary to and not compatible with the disclosed purposes for which such personal data is processed, as disclosed to the consumer, unless the controller obtains the consumer's consent.

3. A controller shall establish, implement, and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data. Such data security practices shall be appropriate to the volume and nature of the personal data at issue.

4. A controller may not process personal data in violation of state and federal laws that prohibit unlawful discrimination against consumers. A controller may not discriminate against a consumer for exercising any of the consumer rights contained in this section, 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. Nothing in this subdivision shall be construed to require a controller to provide a product or service that requires the personal data of a consumer that the controller does not collect or maintain, or to prohibit a controller from offering a different price, rate, level, quality, or selection of goods or services to a consumer, including offering goods or services for no fee, if the consumer has exercised his or her right to opt out under sub. (2) (a) 5. or the offer is related to a consumer's voluntary participation in a bona fide loyalty, rewards, premium features, discounts, or club card program.

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

(b) Any provision of a contract or agreement that purports to waive or limit consumer rights under sub. (2) is void and unenforceable.

(c) A controller shall provide consumers with a reasonably accessible, clear, and meaningful privacy notice that includes all of the following:

1. The categories of personal data processed by the controller.

2. The purpose of processing personal data.

3. How consumers may exercise their consumer rights under sub. (2), including how a consumer may appeal a controller's decision with regard to the consumer's request.

4. The categories of personal data that the controller shares with 3rd parties, if any.

5. The categories of 3rd parties, if any, with whom the controller shares personal data.

(d) If a controller sells personal data to 3rd parties or processes personal data for targeted advertising, the controller shall clearly and conspicuously disclose such processing, as well as the manner in which a consumer may exercise the right to opt out of such processing.

(e) A controller shall establish, and shall describe in a privacy notice, one or more secure and reliable means for consumers to submit a request to exercise their consumer rights under this section. Such means shall take into account the ways in which consumers normally interact with the controller, the need for secure and reliable communication of such requests, and the ability of the controller to authenticate the identity of the consumer making the request. Controllers may not require a consumer to create a new account in order to exercise consumer rights under sub. (2) but may require a consumer to use an existing account.

(4) RESPONSIBILITY ACCORDING TO ROLE; CONTROLLER AND PROCESSOR. (a) A processor shall adhere to the instructions of a controller and shall assist the controller in meeting its obligations under this section. Such assistance shall include the following:

1. Taking into account the nature of processing and the information available to the processor, by appropriate technical and organizational measures, insofar as this is reasonably practicable, to fulfill the controller's obligation to respond to consumer rights requests under sub. (2).

2. Taking into account the nature of processing and the information available to the processor, by assisting the controller in meeting the controller's obligations in relation to the security of processing the personal data and in relation to giving notice of unauthorized acquisition of personal information under s. 134.98.

3. Providing necessary information to enable the controller to conduct and document data protection assessments under sub. (5).

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

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

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

3. Upon the reasonable request of the controller, make available to the controller all information in its possession necessary to demonstrate the processor's compliance with the obligations in this section.

4. At least one of the following:

a. Allow, and cooperate with, reasonable assessments by the controller or the controller's designated assessor.

b. 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 section using an appropriate and accepted control standard or framework and assessment procedure for such assessments. The processor shall provide a report of such assessment to the controller upon request.

5. Engage any subcontractor pursuant to a written contract in accordance with par. (c) that requires the subcontractor to meet the obligations of the processor with respect to the personal data.

(c) Nothing in this section shall be construed to relieve a controller or a processor from the liabilities imposed on it by virtue of its role in the processing relationship as defined by this section.

(d) 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 upon 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.

(5) DATA PROTECTION ASSESSMENTS. (a) A controller shall conduct and document a data protection assessment of each of the following processing activities involving personal data:

1. The processing of personal data for purposes of targeted advertising.

2. The sale of personal data.

3. The processing of personal data for purposes of profiling, where such profiling presents a reasonably foreseeable risk of any of the following:

a. Unfair or deceptive treatment of, or unlawful disparate impact on, consumers.

b. Financial, physical, or reputational injury to consumers.

c. Physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of consumers, where such intrusion would be offensive to a reasonable person.

d. Other substantial injury to consumers.

4. The processing of sensitive data.

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

(b) Data protection assessments conducted under par. (a) shall identify and weigh the benefits that may flow, directly and indirectly, from the processing to the controller, the consumer, other stakeholders, and the public against the potential risks to the rights of the consumer associated with such processing, as mitigated by safeguards that can be employed by the controller to reduce such risks. The use of deidentified data and the reasonable expectations of consumers, as well as the context of the processing and the relationship between the controller and the

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

(c) The attorney general may request, pursuant to a civil investigative demand issued under sub. (10) (a), that a controller disclose any data protection assessment that is relevant to an investigation conducted by the attorney general, and the controller shall make the data protection assessment available to the attorney general. The attorney general may evaluate the data protection assessment for compliance with the responsibilities set forth in sub. (3). Data protection assessments shall be confidential and not subject to the right of inspection and copying under s. 19.35 (1). The disclosure of a data protection assessment pursuant to a request from the attorney general shall not constitute a waiver of attorney–client privilege or work product protection with respect to the assessment and any information contained in the assessment.

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

(e) Data protection assessments conducted by a controller for the purpose of compliance with other laws or regulations may comply under this section if the assessments have a reasonably comparable scope and effect.

(f) Data protection assessment requirements shall apply to processing activities created or generated after January 1, 2024, and are not retroactive.

(6) PROCESSING DEIDENTIFIED DATA; EXEMPTIONS. (a) A controller in possession of deidentified data shall do all of the following:

1. Take reasonable measures to ensure that the data cannot be associated with an individual.

2. Publicly commit to maintaining and using deidentified data without attempting to reidentify the data.

3. Contractually obligate any recipients of the deidentified data to comply with all provisions of this section.

(b) Nothing in this section shall be construed to require a controller or processor to do any of the following:

1. Reidentify deidentified data or pseudonymous data.

2. Maintain data in identifiable form.

3. Collect, obtain, retain, or access any data or technology, in order to be capable of associating an authenticated consumer request with personal data.

(c) Nothing in this section shall be construed to require a controller or processor to comply with an authenticated consumer rights request under sub. (2) if all of the following are true:

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

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

3. The controller does not sell the personal data to any 3rd party or otherwise voluntarily disclose the personal data to any 3rd party other than a processor, except as otherwise permitted in this subsection.

(d) The consumer rights contained in subs. (2) (a) 1. to 4. and (3) shall not apply to pseudonymous data in cases where the controller is able to demonstrate any information necessary to identify the consumer is kept separately and is subject to

effective technical and organizational controls that prevent the controller from accessing such information.

(e) A controller that discloses pseudonymous data or deidentified data shall exercise reasonable oversight to monitor compliance with any contractual commitments to which the pseudonymous data or deidentified data is subject and shall take appropriate steps to address any breaches of those contractual commitments.

(7) LIMITATIONS. (a) Nothing in this section shall be construed to restrict a controller's or processor's ability to do any of the following:

1. Comply with federal, state, or local laws, rules, or regulations.

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

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

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

5. Provide a product or service specifically requested by a consumer or the parent or guardian of a child, 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 prior to entering into a contract.

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

7. Prevent, detect, protect against, or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities, or any illegal activity;

preserve the integrity or security of systems; or investigate, report, or prosecute those responsible for any such action.

8. Engage in public or peer–reviewed scientific or statistical research 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:

a. If the deletion of the information is likely to provide substantial benefits that do not exclusively accrue to the controller.

b. The expected benefits of the research outweigh the privacy risks.

c. If the controller has implemented reasonable safeguards to mitigate privacy risks associated with research, including any risks associated with reidentification.

9. Assist another controller, processor, or 3rd party with any of the obligations under this section.

(b) The obligations imposed on controllers or processors under this section shall not restrict a controller's or processor's ability to collect, use, or retain data to do any of the following:

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

2. Effectuate a product recall.

3. Identify and repair technical errors that impair existing or intended functionality.

4. Perform internal operations that are reasonably aligned with the expectations of the consumer or reasonably anticipated on the basis of the consumer's existing relationship with the controller or are 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.

(c) The obligations imposed on controllers or processors under this section shall not apply where compliance by the controller or processor with this section would violate an evidentiary privilege under ch. 905. Nothing in this section shall be construed to prevent a controller or processor from providing personal data concerning a consumer to a person covered by an evidentiary privilege under ch. 905 as part of a privileged communication.

(d) A controller or processor that discloses personal data to a 3rd–party controller or processor, in compliance with the requirements of this section, is not in violation of this section if the 3rd–party controller or processor that receives and processes such personal data is in violation of this section, provided that, 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 3rd–party controller or processor receiving personal data from a controller or processor in compliance with the requirements of this section is likewise not in violation of this section for the transgressions of the controller or processor from which it receives such personal data.

(e) Nothing in this section shall be construed as an obligation imposed on controllers and processors that adversely affects the rights or freedoms of any persons, such as exercising the right of free speech pursuant to the First Amendment to the U.S. Constitution, or applies to the processing of personal data by a person in the course of a purely personal or household activity.

(f) Personal data processed by a controller pursuant to this subsection may not be processed for any purpose other than those expressly listed in this subsection

unless otherwise allowed by this section. Personal data processed by a controller pursuant to this subsection may be processed to the extent that such processing is both of the following:

1. Reasonably necessary and proportionate to the purposes listed in this subsection.

2. Adequate, relevant, and limited to what is necessary in relation to the specific purposes listed in this subsection. Personal data collected, used, or retained pursuant to par. (b) shall, where applicable, take into account the nature and purpose or purposes of such collection, use, or retention. Such data shall 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 such collection, use, or retention of personal data.

(g) If a controller processes personal data pursuant to an exemption in this section, the controller bears the burden of demonstrating that such processing qualifies for the exemption and complies with the requirements in par. (f).

(h) Processing personal data for the purposes expressly identified in par. (a) shall not solely make an entity a controller with respect to such processing.

(8) SCOPE; EXEMPTIONS. (a) This section applies to persons that conduct business in this state or produce products or services that are targeted to residents of this state and who satisfy either of the following:

1. During a calendar year, the person controls or processes personal data of at least 100,000 consumers.

2. The person controls or processes personal data of at least 25,000 consumers and derives over 50 percent of gross revenue from the sale of personal data.

(b) This section shall not apply to any of the following:

1. An association, authority, board, department, commission, independent agency, institution, office, society, or other body in state or local government created or authorized to be created by the constitution or any law.

2. Financial institutions, affiliates of financial institutions, or data subject to Title V of the federal Gramm–Leach–Bliley Act, 15 USC 6801 et seq.

3. A covered entity or business associate governed by HIPAA or HITECH.

4. A nonprofit organization.

5. An institution of higher education.

6. The entity under contract under s. 153.05 (2m) (a) and its contractors.

7. The data organization under contract under s. 153.05 (2r) and its contractors.

(c) The following information and data are exempt from this section:

1. Any health care information or record that is governed by HIPAA, HITECH, Cures Act, or any other federal law governing the use, disclosure, access or creation of health care information or records, including any derived, identifiable, de–identifiable, confidential or non–confidential health care information or records as defined by such federal laws.

2. Any health care information or record that is governed by s. 51.30, 146.816, 146.82, 146.83, or 146.84, chapter 153, or other Wisconsin law governing the use, disclosure, access or creation of health care information or records, including any derived, identifiable, de–identifiable, confidential or non–confidential health care information or records as defined by such Wisconsin laws.

3. Any of the following:

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

b. Identifiable private information that is otherwise information collected as part of human subjects research pursuant to the good clinical practice guidelines issued by the International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use or under 21 CFR Parts 50 and 56.

c. Personal data used or shared in research conducted in accordance with the requirements set forth in this section, or other research conducted in accordance with applicable law.

4. Information and documents created for purposes of the federal Health Care Quality Improvement Act of 1986, 42 USC 11101 et seq.

5. Patient safety work product for purposes of the federal Patient Safety and Quality Improvement Act, 42 USC 299b–21 et seq.

6. Information originating from, and intermingled to be indistinguishable with, or information treated in the same manner as information exempt under this paragraph.

7. The collection, maintenance, disclosure, sale, communication, or use of any personal information bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living by a 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 such activity is regulated by and authorized under the federal Fair Credit Reporting Act, 15 USC 1681 et seq.

8. Personal data collected, processed, sold, or disclosed in compliance with the federal Driver's Privacy Protection Act of 1994, 18 USC 2721 et seq.

9. Personal data regulated by the federal Family Educational Rights and Privacy Act, 20 USC 1232g et seq.

10. Personal data collected, processed, sold, or disclosed in compliance with the federal Farm Credit Act, 12 USC 2001 et seq.

11. Data processed or maintained for any of the following purposes:

a. In the course of an individual applying to, employed by, or acting as an agent or independent contractor of a controller, processor, or 3rd party, to the extent that the data is collected and used within the context of that role.

b. As the emergency contact information of an individual under this section used for emergency contact purposes.

c. That is necessary to retain to administer benefits for another individual relating to an individual described in subd. 15. a. and used for the purposes of administering those benefits.

12. Personal data collected, processed, and maintained in compliance with the Children's Online Privacy Protection Act of 1998, 15 USC 6501 et seq., as amended, and regulations thereto.

(9) VIOLATIONS. (a) The attorney general shall have exclusive authority to enforce violations of this section.

(b) 1. Prior to initiating any action under this section, the attorney general shall provide a controller or processor 30 days' written notice identifying the specific provisions of this section the attorney general, on behalf of a consumer, alleges have been or are being violated. If within the 30 days the controller or processor cures the noticed violation and provides the attorney general an express written statement that the alleged violations have been cured and that no such further violations shall

occur, no action for statutory damages shall be initiated against the controller or processor.

2. If a controller or processor continues to violate this section in breach of an express written statement provided to the consumer under this section, the attorney general may initiate an action and seek damages for up to $7,500 for each violation under this section.

(c) Nothing in this section shall be construed as providing the basis for, or be subject to, a private right of action to violations of this section or under any other law.

(10) ENFORCEMENT. (a) The attorney general retains exclusive authority to enforce this section by bringing an action in the name of the state, or on behalf of persons residing in the state. The attorney general may issue a civil investigative demand to any controller or processor believed to be engaged in, or about to engage in, any violation of this section, and by the civil investigative demand the attorney general may compel the attendance of any officers or agents of the controller or processor, examine the officers or agents of the controller or processor under oath, require the production of any books or papers that the attorney general deems relevant or material to the inquiry, and issue written interrogatories to be answered by the officers or agents of the controller or processor.

(b) Any controller or processor that violates this section is subject to an injunction and liable for a forfeiture of not more than $7,500 for each violation.

(c) Notwithstanding s. 814.04 (1), the attorney general may recover reasonable expenses incurred in investigating and preparing the case, including attorney fees, of any action initiated under this section.

(11) LOCAL PREEMPTION. No city, village, town, or county may enact or enforce an ordinance that regulates the collection, processing, or sale of personal data.

SECTION 2. Effective date.

(1) This act takes effect on January 1, 2025.

(END)