HOUSE FILE 2506
BY COMMITTEE ON INFORMATION
TECHNOLOGY

(SUCCESSOR TO HSB 674)

A BILL FOR

An Act relating to consumer data protection, providing civil penalties, and including effective date provisions.

BE IT ENACTED BY THE GENERAL ASSEMBLY OF THE STATE OF IOWA:

Section 1. NEW SECTION. **715D.1 Definitions.**

As used in this chapter, unless the context otherwise requires:

1. *"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:

a. Ownership of, or the power to vote, more than fifty percent of the outstanding shares of any class of voting security of a company.

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

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

2. *"Aggregate data"* means information that relates to a group or category of consumers, from which individual consumer identities have been removed, that is not linked or reasonably linkable to any consumer.

3. *"Authenticate"* means verifying through reasonable means that a consumer, entitled to exercise their consumer rights in section 715D.3, is the same consumer exercising such consumer rights with respect to the personal data at issue.

4. *"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 is 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 HIPAA.

5. *"Child"* means any natural person younger than thirteen years of age.

6. *"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.

7. "*Consumer*" means a natural person who is a resident of the state acting only in an individual or household context and excluding a natural person acting in a commercial or employment context.

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

9. "*Covered entity*" means the same as "covered entity" defined by HIPAA.

10. "*Decisions that produce legal or similarly significant effects concerning a consumer*" means a decision made by a controller that results in the provision or denial by the controller of 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.

11. "*De-identified data*" means data that cannot reasonably be linked to an identified or identifiable natural person.

12. "*Health care provider*" means any of the following:

a. A general hospital, ordinary hospital, outpatient surgical hospital, nursing home, or certified nursing facility licensed or certified by the state.

b. A mental or psychiatric hospital licensed by the state.

c. A hospital operated by the state.

d. A hospital operated by universities within the state.

e. A person licensed to practice medicine or osteopathy in the state.

f. A person licensed to furnish health care policies or plans in the state.

g. A person licensed to practice dentistry in the state.

h. "Health care provider" does not include a continuing care retirement community or any nursing care facility of a religious body which depends upon prayer alone for healing.

13. *"Health Insurance Portability and Accountability Act"* or *"HIPAA"* means the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, including amendments thereto and regulations promulgated thereunder.

14. *"Health record"* means any written, printed, or electronically recorded material maintained by a health care provider in the course of providing health services to an individual concerning the individual and the services provided, including related health information provided in confidence to a health care provider.

15. *"Identified or identifiable natural person"* means a person who can be readily identified, directly or indirectly.

16. *"Institution of higher education"* means nonprofit private institutions of higher education and proprietary private institutions of higher education in the state, community colleges, and each associate-degree-granting and baccalaureate public institutions of higher education in the state.

17. *"Nonprofit organization"* means any corporation organized under chapter 504, any organization exempt from taxation under sections 501(c)(3), 501(c)(6), or 501(c)(12) of the Internal Revenue Code, and any subsidiaries and affiliates of entities organized pursuant to chapter 499.

18. *"Personal data"* means any information that is linked or reasonably linkable to an identified or identifiable natural person. *"Personal data"* does not include de-identified data or publicly available information.

19. *"Precise geolocation data"* means information derived from technology, including but not limited to global positioning system level latitude and longitude coordinates or other mechanisms, that identifies the specific location of a natural person with precision and accuracy within a radius of

one thousand seven hundred fifty 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.

20. *"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.

21. *"Processor"* means a person that processes personal data on behalf of a controller.

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

23. *"Protected health information"* means the same as protected health information established by HIPAA.

24. *"Pseudonymous data"* means personal data that cannot be attributed to a specific natural person 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 natural person.

25. *"Publicly available information"* means information that is lawfully made available through federal, state, or local government records, or information that a business has 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.

26. *"Sale of personal data"* means the exchange of personal

data for monetary or other valuable consideration by the controller to a third party. *"Sale of personal data"* does not include:

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

b. The disclosure of personal data to a third party for purposes of providing a product or service requested by the consumer or a parent of a child.

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

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

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

27. *"Sensitive data"* means a category of personal data that includes the following:

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

b. Genetic or biometric data that is processed for the purpose of uniquely identifying a natural person.

c. The personal data collected from a known child.

d. Precise geolocation data.

28. *"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 the following:

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

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

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

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

29. *"Third party"* means a natural or legal person, public authority, agency, or body other than the consumer, controller, processor, or an affiliate of the processor or the controller.

30. *"Trade secret"* means information, including but not limited to a formula, pattern, compilation, program, device, method, technique, or process, that consists of the following:

a. Information that derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use.

b. Information that is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

Sec. 2. NEW SECTION. **715D.2 Scope and exemptions.**

1. This chapter applies to a person conducting business in the state or producing products or services that are targeted to residents of the state and that during a calendar year does either of the following:

a. Controls or processes personal data of at least one hundred thousand consumers.

b. Controls or processes personal data of at least twenty-five thousand consumers and derive over fifty percent of gross revenue from the sale of personal data.

2. This chapter shall not apply to the state or any political subdivision of the state, financial institutions or data subject to Tit. V of the federal Gramm-Leach-Bliley Act of 1999, 15 U.S.C. §6801 et seq., covered entities or business associates governed by the privacy, security, and

breach notification rules issued by the Iowa department of human services, the Iowa department of public health, 45 C.F.R. pts. 160 and 164 established pursuant to HIPAA, nonprofit organizations, or institutions of higher education.

3. The following information and data is exempt from this chapter:

a. Protected health information under HIPAA.

b. Health records.

c. Patient identifying information for purposes of 42 U.S.C. §290dd-2.

d. Identifiable private information for purposes of the federal policy for the protection of human subjects under 45 C.F.R. pt. 46.

e. 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.

f. The protection of human subjects under 21 C.F.R. pts. 6, 50, and 56.

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

h. Information and documents created for purposes of the federal Health Care Quality Improvement Act of 1986, 42 U.S.C. §11101 et seq.

i. Patient safety work product for purposes of the federal Patient Safety And Quality Improvement Act, 42 U.S.C. §299b-21 et seq.

j. Information derived from any of the health care-related information listed in this subsection that is de-identified in accordance with the requirements for de-identification pursuant to HIPAA.

k. Information originating from, and intermingled to be indistinguishable with, or information treated in the same manner as information exempt under this subsection that is maintained by a covered entity or business associate as defined by HIPAA or a program or a qualified service organization as defined by 42 U.S.C. §290dd-2.

l. Information used only for public health activities and purposes as authorized by HIPAA.

m. 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 or furnisher 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 U.S.C. §1681.

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

o. Personal data regulated by the federal Family Educational Rights and Privacy Act, 20 U.S.C. §1232 et seq.

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

q. Data processed or maintained as follows:

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

(2) As the emergency contact information of an individual under this chapter used for emergency contact purposes.

(3) That is necessary to retain to administer benefits for another individual relating to the individual under subparagraph (1) and used for the purposes of administering those benefits.

r. Personal data used in accordance with the federal

Children's Online Privacy Protection Act, 15 U.S.C. §6501 — 6506, and its rules, regulations, and exceptions thereto.

Sec. 3. NEW SECTION. **715D.3 Consumer data rights.**

1. A consumer may invoke the consumer rights authorized pursuant to this section 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 known child regarding processing personal data belonging to the child. A controller shall comply with an authenticated consumer request to exercise all of the following:

a. To confirm whether a controller is processing the consumer's personal data and to access such personal data.

b. To correct inaccuracies in the consumer's personal data, taking into account the nature of the personal data and the purposes of the processing of the consumer's personal data.

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

d. To obtain a copy of the consumer's personal data that the consumer previously provided to the controller in a portable and, to the extent technically practicable, readily usable format that allows the consumer to transmit the data to another controller without hindrance, where the processing is carried out by automated means.

e. To opt out of the processing of the personal data for 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.

2. Except as otherwise provided in this chapter, a controller shall comply with a request by a consumer to exercise the consumer rights authorized pursuant to this section as follows:

a. A controller shall respond to the consumer without undue delay, but in all cases within forty-five days of receipt of a request submitted pursuant to the methods described in this section. The response period may be extended once by forty-five additional days when reasonably necessary upon considering the complexity and number of the consumer´s requests by informing the consumer of any such extension within the initial forty-five-day response period, together with the reason for the extension.

b. If a controller declines to take action regarding the consumer´s request, the controller shall inform the consumer without undue delay of the justification for declining to take action and instructions for how to appeal the decision pursuant to this section.

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

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

3. 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 this section. The appeal process shall be conspicuously available and similar to the process for submitting requests to initiate action pursuant to this section. Within sixty 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 decision. If the appeal is denied, the controller shall also provide the consumer with an online mechanism through which the consumer may contact the attorney general to submit a complaint.

Sec. 4. NEW SECTION. **715D.4 Data controller duties.**

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. Except as otherwise provided in this chapter, a controller shall not process personal data for purposes that are neither reasonably necessary to nor 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. A controller shall adopt and implement 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. A controller shall not process sensitive data without the consumer´s consent, or, in the case of the processing of sensitive data concerning a known child, without processing such data in accordance with the federal Children´s Online Privacy Protection Act, 15 U.S.C. §6501 et seq.

2. A controller shall not process personal data in violation of state and federal laws that prohibit unlawful discrimination against a consumer. A controller shall not discriminate against a consumer for exercising any of the consumer rights contained in this chapter, including denying goods or services, charging different prices or rates for goods or services, or providing a different level of quality of goods and services to the consumer. However, nothing in this chapter 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 right to opt out pursuant to section 715D.3 or the offer is related to a consumer´s voluntary participation in a bona fide loyalty, rewards, premium features, discounts, or club card program.

3. Any provision of a contract or agreement that purports to waive or limit in any way consumer rights pursuant to section 715D.3 shall be deemed contrary to public policy and shall be void and unenforceable.

4. A controller shall provide consumers with a reasonably accessible, clear, and meaningful privacy notice that includes the following:

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

b. The purpose for processing personal data.

c. How consumers may exercise their consumer rights pursuant to section 715D.3, including how a consumer may appeal a controller´s decision with regard to the consumer´s request.

d. The categories of personal data that the controller shares with third parties, if any.

e. The categories of third parties, if any, with whom the controller shares personal data.

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

6. A controller shall establish, and shall describe in a privacy notice, secure and reliable means for consumers to submit a request to exercise their consumer rights under this chapter. Such means shall consider 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. A controller shall not require a consumer to create a new account in order to exercise consumer rights pursuant to section 715D.3, but may require a consumer to use an existing account.

Sec. 5. NEW SECTION. **715D.5 Processor duties.**

1. A processor shall assist a controller in duties required under this chapter, taking into account the nature of processing and the information available to the processor by appropriate technical and organizational measures, insofar as is reasonably practicable, as follows:

a. To fulfill the controller's obligation to respond to consumer rights requests pursuant to section 715D.3.

b. To meet the controller's obligations in relation to the security of processing the personal data and in relation to the notification of a security breach of the processor pursuant to section 715C.2.

c. To provide necessary information to enable the controller to conduct and document data protection assessments pursuant to section 715D.6.

2. 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 clearly set forth instructions for processing personal data, the nature and purpose of processing, the type of data subject to processing, the duration of processing, and the rights and duties of both parties. The contract shall also include requirements that the processor shall do all of the following:

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

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

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

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

e. Engage any subcontractor or agent pursuant to a written contract in accordance with this section that requires the subcontractor to meet the duties of the processor with respect to the personal data.

3. Nothing in this section shall be construed to relieve a controller or a processor from imposed liabilities by virtue of the controller or processor's role in the processing relationship as defined by this chapter.

4. Determining whether a person is acting as a controller or processor with respect to a specific processing of data is a fact-based determination that depends 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.

Sec. 6. NEW SECTION. **715D.6 Data protection assessments.**

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

a. The sale of personal data.

b. The processing of personal data for targeted advertising.

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

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

(2) Financial, physical, or reputational injury to consumers.

(3) A 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.

(4) Other substantial injury to consumers.

d. The processing of sensitive data.

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

2. Data protection assessments conducted pursuant to subsection 1 shall identify and weigh the benefits that may flow, directly and indirectly, from the processing to the controller, the consumer, other stakeholders, and the public against the potential risks to the rights of the consumer associated with such processing, as mitigated by safeguards that can be employed by the controller to reduce such risks. The use of de-identified data and the reasonable expectations of consumers, as well as the context of the processing and the relationship between the controller and the consumer whose personal data will be processed, shall be factored into this assessment by the controller.

3. The attorney general may request, pursuant to a civil investigative demand, 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 section 715D.4. The controller shall make the data protection assessment available to the attorney general. Data protection assessments shall be confidential and exempt from public inspection and copying under section 22.1. 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 data protection assessment and any information contained in the data protection assessment. The attorney general may evaluate the data protection assessment for compliance with the responsibilities set forth in section 715D.4.

4. 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. A single data protection assessment may address a comparable set of processing operations that include similar activities. Data protection assessment requirements shall apply to processing activities created or generated after January 1, 2024, and are not retroactive.

Sec. 7. NEW SECTION. **715D.7 Processing data —— exemptions.**

1. A controller in possession of de-identified data shall comply with the following:

a. Take reasonable measures to ensure that the data cannot be associated with a natural person.

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

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

2. Nothing in this chapter shall be construed to require the following:

a. A controller or processor to re-identify de-identified data or pseudonymous data.

b. Maintaining data in identifiable form.

c. Collecting, obtaining, retaining, or accessing any data or technology, in order to be capable of associating an authenticated consumer request with personal data.

3. Nothing in this chapter shall be construed to require a controller or processor to comply with an authenticated consumer rights request, pursuant to section 715D.3, if all of the following are true:

a. 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.

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

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

4. Consumer rights contained in sections 715D.3 and 715D.4 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.

5. Controllers that disclose pseudonymous data or de-identified data shall exercise reasonable oversight to monitor compliance with any contractual commitments to which the pseudonymous data or de-identified data is subject and shall take appropriate steps to address any breaches of those contractual commitments.

Sec. 8. NEW SECTION. **715D.8 Limitations.**

1. Nothing in this chapter shall be construed to restrict a controller′s or processor′s ability to do the following:

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

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

c. Cooperate with 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.

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

e. Provide a product or service specifically requested by a consumer, perform a contract to which the consumer is a party, including fulfilling the terms of a written warranty, or take steps at the request of the consumer prior to entering into a contract.

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

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

h. Preserve the integrity or security of systems.

i. Investigate, report, or prosecute those responsible for any such action.

j. 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 the following:

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

(2) The expected benefits of the research outweigh the privacy risks.

(3) If the controller has implemented reasonable safeguards to mitigate privacy risks associated with research, including

any risks associated with re-identification.

k. Assist another controller, processor, or third party with any of the obligations under this subsection.

2. The obligations imposed on a controller or processor under this chapter shall not restrict a controller's or processor's ability to collect, use, or retain data as follows:

a. To conduct internal research to develop, improve, or repair products, services, or technology.

b. To effectuate a product recall.

c. To identify and repair technical errors that impair existing or intended functionality.

d. To perform internal operations that are reasonably aligned with the expectations of the consumer or reasonably anticipated based on 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.

3. The obligations imposed on controllers or processors under this chapter shall not apply where compliance by the controller or processor with this chapter would violate an evidentiary privilege under the laws of the state. Nothing in this chapter 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 the laws of the state as part of a privileged communication.

4. A controller or processor that discloses personal data to a third-party controller or processor, in compliance with the requirements of this chapter, is not in violation of this chapter if the third-party controller or processor that receives and processes such personal data is in violation of this chapter, 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 third-party controller or processor receiving

personal data from a controller or processor in compliance with the requirements of this chapter is likewise not in violation of this chapter for the offenses of the controller or processor from which it receives such personal data.

5. Nothing in this chapter shall be construed as an obligation imposed on a controller or a processor 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 United States Constitution, or applies to the processing of personal data by a person in the course of a purely personal or household activity.

6. Personal data processed by a controller pursuant to this section shall not be processed for any purpose other than those expressly listed in this section unless otherwise allowed by this chapter. Personal data processed by a controller pursuant to this section may be processed to the extent that such processing is as follows:

a. Reasonably necessary and proportionate to the purposes listed in this section.

b. Adequate, relevant, and limited to what is necessary in relation to the specific purposes listed in this section. Personal data collected, used, or retained pursuant to this section 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.

7. 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 subsection 6.

8. Processing personal data for the purposes expressly

identified in subsection 1 shall not solely make an entity a controller with respect to such processing.

9. This chapter shall not require a controller, processor, third party, or consumer to disclose trade secrets.

Sec. 9. NEW SECTION. **715D.9 Enforcement —— penalties.**

1. The attorney general shall have exclusive authority to enforce the provisions of this chapter. Whenever the attorney general has reasonable cause to believe that any person has engaged in, is engaging in, or is about to engage in any violation of this chapter, the attorney general is empowered to issue a civil investigative demand.

2. Prior to initiating any action under this chapter, the attorney general shall provide a controller or processor thirty days′ written notice identifying the specific provisions of this chapter the attorney general alleges have been or are being violated. If within the thirty-day period, 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 further such violations shall occur, no action shall be initiated against the controller or processor.

3. If a controller or processor continues to violate this chapter following the cure period in subsection 2 or breaches an express written statement provided to the attorney general under that subsection, the attorney general may initiate an action in the name of the state and may seek an injunction to restrain any violations of this chapter and civil penalties of up to seven thousand five hundred dollars for each violation under this chapter. Any moneys collected under this section including civil penalties, costs, attorneys fees, or amounts which are specifically directed shall be paid into the consumer education and litigation fund established under section 714.16C.

4. The attorney general may recover reasonable expenses incurred in investigating and preparing the case, including

attorney fees, in any action initiated under this chapter.

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

Sec. 10. EFFECTIVE DATE. This Act takes effect January 1, 2024.

EXPLANATION

The inclusion of this explanation does not constitute agreement with the explanation's substance by the members of the general assembly.

This bill relates to consumer data protection.

The bill contains several definitions. The bill defines "controller" to mean a person that, alone or jointly with others, determines the purpose and means of processing personal data. The bill defines "identified or identifiable natural person" to mean a person who can be readily identified, directly or indirectly. The bill defines "personal data" to mean any information that is linked or reasonably linkable to an identified or identifiable natural person, but does not include de-identified data or publicly available information. The bill defines "process" or "processing" to mean 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. The bill defines "processor" to mean a person that processes personal data on behalf of a controller. The bill defines "pseudonymous data" to mean personal data that cannot be attributed to a specific natural person without the use of additional information. The bill defines "publicly available information" to mean information that is lawfully made available to the general public through certain records or information that a business has reasonable basis to believe is lawfully made available under certain conditions. The bill defines "targeted advertising" to mean 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, with exceptions. The bill defines "third party" to mean a natural or legal person, public authority, agency, or body other than the consumer, controller, processor, or an affiliate of the processor or the controller. The bill contains other defined terms.

The bill provides that persons conducting business in the state or producing products or services targeted to Iowans that annually control or process personal data of over 99,999 consumers or control or process personal data of 25,000 consumers with 50 percent of gross revenue derived from the sale of the personal data shall be subject to the provisions of the bill. The state and political subdivisions of the state, financial institutions or data subject to the Gramm-Leach-Bliley Act of 1999, certain organizations governed by rules by the department of human services, the department of health, certain federal governance laws and the federal Health Insurance Portability and Accountability Act, nonprofit organizations, higher learning institutions, and certain protected information and personal data collected under state or federal laws are exempt from provisions in the bill.

The bill provides consumers have personal data rights that may be invoked at any time. Consumers or the parent of a child may submit a request to a controller for a copy of the controller's information relating to personal data. The controller shall comply with such requests to confirm or deny whether the controller is processing the personal data, to delete or correct inaccuracies in personal data, to provide the consumer with a copy of their personal data, and to remove the consumer or child from personal data processing.

The bill requires that controllers provide responses to defined personal data requests within 45 days of a consumer initiating a request. Responses to personal data requests shall be provided to a consumer free of charge up to twice per year except where requests are overly burdensome or manifestly unfounded. A business may extend the deadline for good cause, including complexity, once by up to 45 days after informing the consumer of the reason for the extension. The bill provides that controllers are not required to comply with requests where a controller is unable through commercially reasonable efforts to verify the identity of the consumer submitting the request. The bill requires that controllers permit consumers to access an appeals process and provide consumers with information regarding the appeals process in situations where a consumer's request is denied.

The bill provides that controllers shall limit the collection of personal data to the extent reasonably necessary. Controllers must disclose to the consumer the types of data being collected and obtain consent from the consumers regarding the collection of personal data and sensitive personal data processing. Controllers must securely store personal data of consumers through administrative, technical, and physical security practices. Controllers shall not discriminate against consumers that exercise consumer data rights as provided in the bill by denying a consumer goods or services, charging different prices, or providing lower quality goods with exceptions. Contract provisions that require consumers to waive rights defined by the bill will be considered void and unenforceable.

The bill provides that controllers give consumers reasonably accessible and clear privacy notices that inform consumers of the information regarding personal data transfer and purposes and the methods for consumers to exercise rights. The bill provides that controllers selling personal data to third parties or using targeted advertising must clearly disclose such activity and the right for the consumer to opt out of such sales or use. The bill requires a controller to create a method for private and secure processing of consumer requests.

The bill requires processors and the assigns or subcontractors of processors to assist controllers in complying with duties created by the bill.

The bill requires controllers to conduct assessments of processing activities regarding certain personal data. Data protection assessments shall consider benefits and risks regarding personal data processing to the controller, consumer, public, and other stakeholders among other factors identified by the bill. The bill provides that the attorney general may request an investigation and require that a controller disclose relevant data protection assessment information and analyze the provided information for compliance with duties described by the bill. Other data protection assessments a controller has conducted may suffice for purposes of the bill if the assessments are reasonably similar.

The bill includes personal data processing exemptions, including pseudonymous data and de-identified data as defined by the bill. The bill requires that controllers in possession of de-identified data take measures to ensure that the data remains de-identified, publicly commit to a de-identified maintenance process, and require agents and assigns to adhere to provisions of the bill. The bill identifies exceptions where controllers or processors are not required to comply with a consumer rights request pursuant to the bill. The bill requires controllers disclosing pseudonymous or de-identified data to exercise reasonable oversight of contractual commitments regarding such data.

The bill provides that the bill shall not restrict controller or processor abilities to improve business or function. Controllers or processors sharing personal data with third parties are not liable for the noncompliance of third parties if the controller or processor did not have personal knowledge of the violation or intent to commit a violation, nor is a third party liable for violations of a controller or processor. The bill provides that if a controller seeks certain exemptions, the controller bears the burden of demonstrating that the controller qualifies for the exemption and the exemption complies with the requirements in the bill.

The bill shall not require a business, consumer, or other party to disclose trade secrets.

The bill provides that the attorney general shall investigate controllers and processors upon reasonable cause for violations of provisions of the bill. The attorney general shall provide 30 days′ notice to a controller or processor including the reason for which the entity is subject to an investigation and permit the entity to cure the defect prior to filing a civil action. A controller or processor found to be in violation of provisions of the bill is subject to a civil penalty of up to $7,500 per violation. Moneys collected by the attorney general under the bill shall be paid into the consumer education and litigation fund established under Code section 714.16C. The attorney general shall recover reasonable expenses for expenses related to the investigation.

The bill takes effect January 1, 2024.