

**House Study Bill 12 - Introduced**

HOUSE FILE \_\_\_\_\_  
BY (PROPOSED COMMITTEE ON  
ECONOMIC GROWTH AND  
TECHNOLOGY BILL BY  
CHAIRPERSON SORENSEN)

**A BILL FOR**

1 An Act relating to consumer data protection, providing civil  
2 penalties, and including effective date provisions.  
3 BE IT ENACTED BY THE GENERAL ASSEMBLY OF THE STATE OF IOWA:

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

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

4 1. "*Affiliate*" means a legal entity that controls, is  
5 controlled by, or is under common control with another legal  
6 entity or shares common branding with another legal entity.  
7 For the purposes of this definition, "*control*" or "*controlled*"  
8 means:

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

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

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

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

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

24 4. "*Biometric data*" means data generated by automatic  
25 measurements of an individual's biological characteristics,  
26 such as a fingerprint, voiceprint, eye retinas, irises, or  
27 other unique biological patterns or characteristics that is  
28 used to identify a specific individual. "*Biometric data*"  
29 does not include a physical or digital photograph, a video or  
30 audio recording or data generated therefrom, or information  
31 collected, used, or stored for health care treatment, payment,  
32 or operations under HIPAA.

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

35 6. "*Consent*" means a clear affirmative act signifying a

1 consumer's freely given, specific, informed, and unambiguous  
2 agreement to process personal data relating to the consumer.  
3 "Consent" may include a written statement, including a  
4 statement written by electronic means, or any other unambiguous  
5 affirmative action.

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

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

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

15 10. "De-identified data" means data that cannot reasonably  
16 be linked to an identified or identifiable natural person.

17 11. "Fund" means the consumer education and litigation fund  
18 established pursuant to section 714.16C.

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

20 a. A general hospital, ambulatory surgical or treatment  
21 center, skilled nursing center, or assisted living center  
22 licensed or certified by the state.

23 b. A psychiatric hospital licensed by the state.

24 c. A hospital operated by the state.

25 d. A hospital operated by the state board of regents.

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

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

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

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

34 13. "Health Insurance Portability and Accountability Act"  
35 or "HIPAA" means the federal Health Insurance Portability and

1 Accountability Act of 1996, Pub. L. No. 104-191, including  
2 amendments thereto and regulations promulgated thereunder.

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

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

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

17 17. "*Nonprofit organization*" means any corporation organized  
18 under chapter 504, any organization exempt from taxation  
19 under sections 501(c)(3), 501(c)(6), or 501(c)(12) of the  
20 Internal Revenue Code, any organization exempt from taxation  
21 under section 501(c)(4) of the Internal Revenue Code that  
22 is established to detect or prevent insurance-related crime  
23 or fraud, and any subsidiaries and affiliates of entities  
24 organized pursuant to chapter 499.

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

29 19. "*Precise geolocation data*" means information derived  
30 from technology, including but not limited to global  
31 positioning system level latitude and longitude coordinates or  
32 other mechanisms, that identifies the specific location of a  
33 natural person with precision and accuracy within a radius of  
34 one thousand seven hundred fifty feet. "*Precise geolocation*  
35 *data*" does not include the content of communications, or any

1 data generated by or connected to advanced utility metering  
2 infrastructure systems or equipment for use by a utility.

3 20. *"Process"* or *"processing"* means any operation or set  
4 of operations performed, whether by manual or automated means,  
5 on personal data or on sets of personal data, such as the  
6 collection, use, storage, disclosure, analysis, deletion, or  
7 modification of personal data.

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

10 22. *"Protected health information"* means the same as  
11 protected health information established by HIPAA.

12 23. *"Pseudonymous data"* means personal data that cannot  
13 be attributed to a specific natural person without the use  
14 of additional information, provided that such additional  
15 information is kept separately and is subject to appropriate  
16 technical and organizational measures to ensure that  
17 the personal data is not attributed to an identified or  
18 identifiable natural person.

19 24. *"Publicly available information"* means information  
20 that is lawfully made available through federal, state, or  
21 local government records, or information that a business has  
22 reasonable basis to believe is lawfully made available to  
23 the general public through widely distributed media, by the  
24 consumer, or by a person to whom the consumer has disclosed the  
25 information, unless the consumer has restricted the information  
26 to a specific audience.

27 25. *"Sale of personal data"* means the exchange of personal  
28 data for monetary consideration by the controller to a third  
29 party. *"Sale of personal data"* does not include:

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

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

35 c. The disclosure or transfer of personal data to an

1 affiliate of the controller.

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

6 *e.* The disclosure or transfer of personal data when a  
7 consumer uses or directs a controller to intentionally disclose  
8 personal data or intentionally interact with one or more third  
9 parties.

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

15 26. "*Sensitive data*" means a category of personal data that  
16 includes the following:

17 *a.* Racial or ethnic origin, religious beliefs, mental or  
18 physical health diagnosis, sexual orientation, or citizenship  
19 or immigration status, except to the extent such data is used  
20 in order to avoid discrimination on the basis of a protected  
21 class that would violate a federal or state anti-discrimination  
22 law.

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

25 *c.* The personal data collected from a known child.

26 *d.* Precise geolocation data.

27 27. "*State agency*" means the same as defined in 129 IAC  
28 10.2(8B).

29 28. "*Targeted advertising*" means displaying advertisements  
30 to a consumer where the advertisement is selected based on  
31 personal data obtained from that consumer's activities over  
32 time and across nonaffiliated websites or online applications  
33 to predict such consumer's preferences or interests. "*Targeted*  
34 *advertising*" does not include the following:

35 *a.* Advertisements based on activities within a controller's

1 own or affiliated websites or online applications.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

7 a. Protected health information under HIPAA.

8 b. Health records.

9 c. Patient identifying information for purposes of 42 U.S.C.  
10 §290dd-2.

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

14 e. Identifiable private information that is otherwise  
15 information collected as part of human subjects research  
16 pursuant to the good clinical practice guidelines issued by  
17 the international council for harmonization of technical  
18 requirements for pharmaceuticals for human use.

19 f. The protection of human subjects under 21 C.F.R. pts. 6,  
20 50, and 56.

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

24 h. Information and documents created for purposes of the  
25 federal Health Care Quality Improvement Act of 1986, 42 U.S.C.  
26 §11101 et seq.

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

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

34 k. Information originating from, and intermingled to be  
35 indistinguishable with, or information treated in the same



1 manner as information exempt under this subsection that is  
2 maintained by a covered entity or business associate as defined  
3 by HIPAA or a program or a qualified service organization as  
4 defined by 42 U.S.C. §290dd-2.

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

7 *m.* The collection, maintenance, disclosure, sale,  
8 communication, or use of any personal information bearing on a  
9 consumer's credit worthiness, credit standing, credit capacity,  
10 character, general reputation, personal characteristics, or  
11 mode of living by a consumer reporting agency or furnisher that  
12 provides information for use in a consumer report, and by a  
13 user of a consumer report, but only to the extent that such  
14 activity is regulated by and authorized under the federal Fair  
15 Credit Reporting Act, 15 U.S.C. §1681 et seq.

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

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

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

24 *q.* Data processed or maintained as follows:

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

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

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

35 *r.* Personal data used in accordance with the federal

1 Children's Online Privacy Protection Act, 15 U.S.C. §6501 –  
2 6506, and its rules, regulations, and exceptions thereto.

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

4 1. A consumer may invoke the consumer rights authorized  
5 pursuant to this section at any time by submitting a request to  
6 the controller, through the means specified by the controller  
7 pursuant to section 715D.4, subsection 6, specifying the  
8 consumer rights the consumer wishes to invoke. A known child's  
9 parent or legal guardian may invoke such consumer rights  
10 on behalf of the known child regarding processing personal  
11 data belonging to the child. A controller shall comply with  
12 an authenticated consumer request to exercise all of the  
13 following:

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

16 b. To delete personal data provided by the consumer.

17 c. To obtain a copy of the consumer's personal data, except  
18 as to personal data that is defined as "*personal information*"  
19 pursuant to section 715C.1 that is subject to security breach  
20 protection, that the consumer previously provided to the  
21 controller in a portable and, to the extent technically  
22 practicable, readily usable format that allows the consumer  
23 to transmit the data to another controller without hindrance,  
24 where the processing is carried out by automated means.

25 d. To opt out of targeted advertising or the sale of  
26 personal data.

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

31 a. A controller shall respond to the consumer without undue  
32 delay, but in all cases within forty-five days of receipt  
33 of a request submitted pursuant to the methods described in  
34 this section. The response period may be extended once by  
35 forty-five additional days when reasonably necessary upon

1 considering the complexity and number of the consumer's  
2 requests by informing the consumer of any such extension within  
3 the initial forty-five-day response period, together with the  
4 reason for the extension.

5     *b.* If a controller declines to take action regarding the  
6 consumer's request, the controller shall inform the consumer  
7 without undue delay of the justification for declining to take  
8 action, except in the case of a suspected fraudulent request,  
9 in which case the controller may state that the controller was  
10 unable to authenticate the request. The controller shall also  
11 provide instructions for appealing the decision pursuant to  
12 subsection 3.

13     *c.* Information provided in response to a consumer request  
14 shall be provided by a controller free of charge, up to  
15 twice annually per consumer. If a request from a consumer  
16 is manifestly unfounded, excessive, repetitive, technically  
17 unfeasible, or the controller reasonably believes that the  
18 primary purpose of the request is not to exercise a consumer  
19 right, the controller may charge the consumer a reasonable fee  
20 to cover the administrative costs of complying with the request  
21 or decline to act on the request. The controller bears the  
22 burden of demonstrating the manifestly unfounded, excessive,  
23 repetitive, or technically unfeasible nature of the request.

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

30     3. A controller shall establish a process for a consumer  
31 to appeal the controller's refusal to take action on a request  
32 within a reasonable period of time after the consumer's  
33 receipt of the decision pursuant to this section. The appeal  
34 process shall be conspicuously available and similar to the  
35 process for submitting requests to initiate action pursuant

1 to this section. Within sixty days of receipt of an appeal,  
2 a controller shall inform the consumer in writing of any  
3 action taken or not taken in response to the appeal, including  
4 a written explanation of the reasons for the decision. If  
5 the appeal is denied, the controller shall also provide the  
6 consumer with an online mechanism through which the consumer  
7 may contact the attorney general to submit a complaint.

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

9 1. A controller shall adopt and implement reasonable  
10 administrative, technical, and physical data security practices  
11 to protect the confidentiality, integrity, and accessibility  
12 of personal data. Such data security practices shall be  
13 appropriate to the volume and nature of the personal data  
14 at issue. A controller shall not process sensitive data  
15 concerning a consumer or a nonexempt purpose without the  
16 consumer having been presented with clear notice and an  
17 opportunity to opt out of such processing, or, in the case of  
18 the processing of sensitive data concerning a known child,  
19 without processing such data in accordance with the federal  
20 Children's Online Privacy Protection Act, 15 U.S.C. §6501 et  
21 seq.

22 2. A controller shall not process personal data in  
23 violation of state and federal laws that prohibit unlawful  
24 discrimination against a consumer. A controller shall not  
25 discriminate against a consumer for exercising any of the  
26 consumer rights contained in this chapter, including denying  
27 goods or services, charging different prices or rates for  
28 goods or services, or providing a different level of quality  
29 of goods and services to the consumer. However, nothing in  
30 this chapter shall be construed to require a controller to  
31 provide a product or service that requires the personal data  
32 of a consumer that the controller does not collect or maintain  
33 or to prohibit a controller from offering a different price,  
34 rate, level, quality, or selection of goods or services to a  
35 consumer, including offering goods or services for no fee,

1 if the consumer has exercised the consumer's right to opt  
2 out pursuant to section 715D.3 or the offer is related to a  
3 consumer's voluntary participation in a bona fide loyalty,  
4 rewards, premium features, discounts, or club card program.

5 3. Any provision of a contract or agreement that purports to  
6 waive or limit in any way consumer rights pursuant to section  
7 715D.3 shall be deemed contrary to public policy and shall be  
8 void and unenforceable.

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

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

14 b. The purpose for processing personal data.

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

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

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

22 5. If a controller sells a consumer's personal data to third  
23 parties or engages in targeted advertising, the controller  
24 shall clearly and conspicuously disclose such activity, as well  
25 as the manner in which a consumer may exercise the right to opt  
26 out of such activity.

27 6. A controller shall establish, and shall describe in  
28 a privacy notice, secure and reliable means for consumers to  
29 submit a request to exercise their consumer rights under this  
30 chapter. Such means shall consider the ways in which consumers  
31 normally interact with the controller, the need for secure and  
32 reliable communication of such requests, and the ability of  
33 the controller to authenticate the identity of the consumer  
34 making the request. A controller shall not require a consumer  
35 to create a new account in order to exercise consumer rights

1 pursuant to section 715D.3, but may require a consumer to use  
2 an existing account.

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

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

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

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

15 2. A contract between a controller and a processor shall  
16 govern the processor's data processing procedures with respect  
17 to processing performed on behalf of the controller. The  
18 contract shall clearly set forth instructions for processing  
19 personal data, the nature and purpose of processing, the type  
20 of data subject to processing, the duration of processing, and  
21 the rights and duties of both parties. The contract shall also  
22 include requirements that the processor shall do all of the  
23 following:

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

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

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

34 d. Engage any subcontractor or agent pursuant to a written  
35 contract in accordance with this section that requires the

1 subcontractor to meet the duties of the processor with respect  
2 to the personal data.

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

7 4. Determining whether a person is acting as a controller or  
8 processor with respect to a specific processing of data is a  
9 fact-based determination that depends upon the context in which  
10 personal data is to be processed. A processor that continues  
11 to adhere to a controller's instructions with respect to a  
12 specific processing of personal data remains a processor.

13 Sec. 6. NEW SECTION. 715D.6 Processing data — exemptions.

14 1. Nothing in this chapter shall be construed to require the  
15 following:

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

18 b. Maintaining data in identifiable form.

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

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

26 a. The controller is not reasonably capable of associating  
27 the request with the personal data or it would be unreasonably  
28 burdensome for the controller to associate the request with the  
29 personal data.

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

34 c. The controller does not sell the personal data to any  
35 third party or otherwise voluntarily disclose the personal data

1 to any third party other than a processor, except as otherwise  
2 permitted in this chapter.

3 3. Consumer rights contained in sections 715D.3 and 715D.4  
4 shall not apply to pseudonymous data in cases where the  
5 controller is able to demonstrate any information necessary  
6 to identify the consumer is kept separately and is subject to  
7 appropriate technical and organizational measures to ensure  
8 that the personal data is not attributed to an identified or  
9 identifiable natural person.

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

16 Sec. 7. NEW SECTION. 715D.7 Limitations.

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

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

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

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

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

30 e. Provide a product or service specifically requested by a  
31 consumer or parent or guardian of a child, perform a contract  
32 to which the consumer or parent or guardian of a child is a  
33 party, including fulfilling the terms of a written warranty, or  
34 take steps at the request of the consumer or parent or guardian  
35 of a child prior to entering into a contract.



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

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

8     *h.* Preserve the integrity or security of systems.

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

11    *j.* Engage in public or peer-reviewed scientific or  
12 statistical research in the public interest that adheres to  
13 all other applicable ethics and privacy laws and is approved,  
14 monitored, and governed by an institutional review board, or  
15 similar independent oversight entities that determine the  
16 following:

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

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

22       (3) If the controller has implemented reasonable safeguards  
23 to mitigate privacy risks associated with research, including  
24 any risks associated with re-identification.

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

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

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

32       *b.* To effectuate a product recall.

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

35       *d.* To perform internal operations that are reasonably

1 aligned with the expectations of the consumer or reasonably  
2 anticipated based on the consumer's existing relationship with  
3 the controller or are otherwise compatible with processing  
4 data in furtherance of the provision of a product or service  
5 specifically requested by a consumer or parent or guardian of a  
6 child or the performance of a contract to which the consumer or  
7 parent or guardian of a child is a party.

8 3. The obligations imposed on controllers or processors  
9 under this chapter shall not apply where compliance by the  
10 controller or processor with this chapter would violate an  
11 evidentiary privilege under the laws of the state. Nothing  
12 in this chapter shall be construed to prevent a controller or  
13 processor from providing personal data concerning a consumer to  
14 a person covered by an evidentiary privilege under the laws of  
15 the state as part of a privileged communication.

16 4. A controller or processor that discloses personal data  
17 to a third-party controller or processor, in compliance with  
18 the requirements of this chapter, is not in violation of  
19 this chapter if the third-party controller or processor that  
20 receives and processes such personal data is in violation of  
21 this chapter, provided that, at the time of disclosing the  
22 personal data, the disclosing controller or processor did not  
23 have actual knowledge that the recipient intended to commit a  
24 violation. A third-party controller or processor receiving  
25 personal data from a controller or processor in compliance with  
26 the requirements of this chapter is likewise not in violation  
27 of this chapter for the offenses of the controller or processor  
28 from which it receives such personal data.

29 5. Nothing in this chapter shall be construed as an  
30 obligation imposed on a controller or a processor that  
31 adversely affects the privacy or other rights or freedoms  
32 of any persons, such as exercising the right of free speech  
33 pursuant to the first amendment to the United States  
34 Constitution, or applies to personal data by a person in the  
35 course of a purely personal or household activity.

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

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

9 b. Adequate, relevant, and limited to what is necessary  
10 in relation to the specific purposes listed in this section.  
11 Personal data collected, used, or retained pursuant to  
12 this section shall, where applicable, take into account  
13 the nature and purpose or purposes of such collection, use,  
14 or retention. Such data shall be subject to reasonable  
15 administrative, technical, and physical measures to protect the  
16 confidentiality, integrity, and accessibility of the personal  
17 data.

18 7. If a controller processes personal data pursuant to an  
19 exemption in this section, the controller bears the burden of  
20 demonstrating that such processing qualifies for the exemption  
21 and complies with the requirements in subsection 6.

22 8. Processing personal data for the purposes expressly  
23 identified in subsection 1 shall not in and of itself make an  
24 entity a controller with respect to such processing.

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

27 **Sec. 8. NEW SECTION. 715D.8 Enforcement — penalties.**

28 1. The attorney general shall have exclusive authority to  
29 enforce the provisions of this chapter. Whenever the attorney  
30 general has reasonable cause to believe that any person has  
31 engaged in, is engaging in, or is about to engage in any  
32 violation of this chapter, the attorney general is empowered to  
33 issue a civil investigative demand. The provisions of section  
34 685.6 shall apply to civil investigative demands issued under  
35 this chapter.

1     2. Prior to initiating any action under this chapter,  
2 the attorney general shall provide a controller or processor  
3 thirty days' written notice identifying the specific provisions  
4 of this chapter the attorney general alleges have been or  
5 are being violated. If within the thirty-day period, the  
6 controller or processor cures the noticed violation and  
7 provides the attorney general an express written statement that  
8 the alleged violations have been cured and that no further such  
9 violations shall occur, no action shall be initiated against  
10 the controller or processor.

11     3. If a controller or processor continues to violate this  
12 chapter following the cure period in subsection 2 or breaches  
13 an express written statement provided to the attorney general  
14 under that subsection, the attorney general may initiate an  
15 action in the name of the state and may seek an injunction to  
16 restrain any violations of this chapter and civil penalties of  
17 up to seven thousand five hundred dollars for each violation  
18 under this chapter. Any moneys collected under this section  
19 including civil penalties, costs, attorney fees, or amounts  
20 which are specifically directed shall be paid into the consumer  
21 education and litigation fund established under section  
22 714.16C.

23     4. The attorney general may recover reasonable expenses  
24 incurred in investigating and preparing the case, including  
25 attorney fees, in any action initiated under this chapter.

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

29     Sec. 9. NEW SECTION. 715D.9 Preemption.

30     1. This chapter supersedes and preempts all rules,  
31 regulations, codes, ordinances, and other laws adopted by a  
32 city, county, municipality, or local agency regarding the  
33 processing of personal data by controllers or processors.

34     2. Any reference to federal, state, or local law or statute  
35 in this chapter shall be deemed to include any accompanying

1 rules or regulations or exemptions thereto, or in the case of a  
2 federal agency, guidance issued by such agency thereto.

3 Sec. 10. EFFECTIVE DATE. This Act takes effect January 1,  
4 2025.

5 EXPLANATION

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

8 This bill relates to consumer data protection.

9 The bill contains several definitions. The bill defines  
10 "controller" to mean a person that, alone or jointly with  
11 others, determines the purpose and means of processing personal  
12 data. The bill defines "identified or identifiable natural  
13 person" to mean a person who can be readily identified,  
14 directly or indirectly. The bill defines "personal data" to  
15 mean any information that is linked or reasonably linkable to  
16 an identified or identifiable natural person, but does not  
17 include de-identified data or publicly available information.  
18 The bill defines "process" or "processing" to mean any  
19 operation or set of operations performed, whether by manual or  
20 automated means, on personal data or on sets of personal data,  
21 such as the collection, use, storage, disclosure, analysis,  
22 deletion, or modification of personal data. The bill defines  
23 "processor" to mean a person that processes personal data  
24 on behalf of a controller. The bill defines "pseudonymous  
25 data" to mean personal data that cannot be attributed to  
26 a specific natural person without the use of additional  
27 information. The bill defines "publicly available information"  
28 to mean information that is lawfully made available to the  
29 general public through certain records or information that  
30 a business has reasonable basis to believe is lawfully made  
31 available under certain conditions. The bill defines "targeted  
32 advertising" to mean displaying advertisements to a consumer  
33 where the advertisement is selected based on personal data  
34 obtained from that consumer's activities over time and across  
35 nonaffiliated websites or online applications to predict such

1 consumer's preferences or interests, with exceptions. The bill  
2 defines "third party" to mean a natural or legal person, public  
3 authority, agency, or body other than the consumer, controller,  
4 processor, or an affiliate of the processor or the controller.  
5 The bill contains other defined terms.

6 The bill provides that persons conducting business in  
7 the state or producing products or services targeted to  
8 Iowans that annually control or process personal data of  
9 over 99,999 consumers or control or process personal data of  
10 25,000 consumers with 50 percent of gross revenue derived  
11 from the sale of the personal data shall be subject to the  
12 provisions of the bill. The state and political subdivisions  
13 of the state, financial institutions or data subject to the  
14 federal Gramm-Leach-Bliley Act of 1999, certain organizations  
15 governed by rules by the department of health and human  
16 services, certain federal governance laws and the federal  
17 Health Insurance Portability and Accountability Act, nonprofit  
18 organizations, higher learning institutions, and certain  
19 protected information and personal data collected under state  
20 or federal laws are exempt from provisions in the bill.

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

29 The bill requires that controllers provide responses to  
30 defined personal data requests within 45 days of a consumer  
31 initiating a request. Responses to personal data requests  
32 shall be provided to a consumer free of charge up to twice per  
33 year except where requests are overly burdensome or manifestly  
34 unfounded. A business may extend the deadline for good cause,  
35 including complexity, once by up to 45 days after informing the

1 consumer of the reason for the extension. The bill provides  
2 that controllers are not required to comply with requests where  
3 a controller is unable through commercially reasonable efforts  
4 to verify the identity of the consumer submitting the request.  
5 The bill requires that controllers permit consumers to access  
6 an appeals process except in cases that are unable to be  
7 authenticated and provide consumers with information regarding  
8 the appeals process in situations where a consumer's request  
9 is denied.

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

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

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

34 The bill includes personal data processing exemptions,  
35 including pseudonymous data and de-identified data as defined

1 by the bill. The bill identifies exceptions where controllers  
2 or processors are not required to comply with a consumer rights  
3 request pursuant to the bill. The bill requires controllers  
4 disclosing pseudonymous or de-identified data to exercise  
5 reasonable oversight of contractual commitments regarding such  
6 data.

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

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

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

33 The bill provides that a rule, regulation, code, ordinance,  
34 or other law adopted regarding processing of personal data is  
35 preempted by the bill.



H.F. \_\_\_\_\_

1 The bill takes effect January 1, 2025.