

House File 346 - Introduced

HOUSE FILE 346
BY COMMITTEE ON ECONOMIC
GROWTH AND TECHNOLOGY

(SUCCESSOR TO HSB 12)

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

1 any data generated by or connected to 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.; persons who are subject to and comply with regulations

1 promulgated pursuant to Tit. II, subtitle F of the federal
2 Health Insurance Portability And Accountability Act of 1996,
3 Pub. L. No. 104-191, and Tit. XIII, subtitle D of the federal
4 Health Information Technology for Economic and Clinical Health
5 Act of 2009, 42 U.S.C. §17921 - 17954; nonprofit organizations;
6 or institutions of higher education.

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

- 9 a. Protected health information under HIPAA.
- 10 b. Health records.
- 11 c. Patient identifying information for purposes of 42 U.S.C.
12 §290dd-2.
- 13 d. Identifiable private information for purposes of the
14 federal policy for the protection of human subjects under 45
15 C.F.R. pt. 46.
- 16 e. Identifiable private information that is otherwise
17 information collected as part of human subjects research
18 pursuant to the good clinical practice guidelines issued by
19 the international council for harmonization of technical
20 requirements for pharmaceuticals for human use.
- 21 f. The protection of human subjects under 21 C.F.R. pts. 6,
22 50, and 56.
- 23 g. Personal data used or shared in research conducted in
24 accordance with the requirements set forth in this chapter, or
25 other research conducted in accordance with applicable law.
- 26 h. Information and documents created for purposes of the
27 federal Health Care Quality Improvement Act of 1986, 42 U.S.C.
28 §11101 et seq.
- 29 i. Patient safety work product for purposes of the federal
30 Patient Safety and Quality Improvement Act, 42 U.S.C. §299b-21
31 et seq.
- 32 j. Information derived from any of the health care-related
33 information listed in this subsection that is de-identified in
34 accordance with the requirements for de-identification pursuant
35 to HIPAA.

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

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

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

18 *n.* Personal data collected, processed, sold, or disclosed in
19 compliance with the federal Driver's Privacy Protection Act of
20 1994, 18 U.S.C. §2721 et seq.

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

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

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

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

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

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

1 those benefits.

2 *r.* Personal data used in accordance with the federal
3 Children's Online Privacy Protection Act, 15 U.S.C. §6501 –
4 6506, and its rules, regulations, and exceptions thereto.

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

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

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

18 *b.* To delete personal data provided by the consumer.

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

27 *d.* To opt out of the sale of personal data.

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

32 *a.* A controller shall respond to the consumer without
33 undue delay, but in all cases within ninety days of receipt
34 of a request submitted pursuant to the methods described in
35 this section. The response period may be extended once by

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

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

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

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

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

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

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

10 1. A controller shall adopt and implement reasonable
11 administrative, technical, and physical data security practices
12 to protect the confidentiality, integrity, and accessibility
13 of personal data. Such data security practices shall be
14 appropriate to the volume and nature of the personal data at
15 issue.

16 2. A controller shall not process sensitive data collected
17 from a consumer for a nonexempt purpose without the consumer
18 having been presented with clear notice and an opportunity to
19 opt out of such processing, or, in the case of the processing
20 of sensitive data concerning a known child, without processing
21 such data in accordance with the federal Children's Online
22 Privacy Protection Act, 15 U.S.C. §6501 et seq.

23 3. A controller shall not process personal data in
24 violation of state and federal laws that prohibit unlawful
25 discrimination against a consumer. A controller shall not
26 discriminate against a consumer for exercising any of the
27 consumer rights contained in this chapter, including denying
28 goods or services, charging different prices or rates for
29 goods or services, or providing a different level of quality
30 of goods and services to the consumer. However, nothing in
31 this chapter shall be construed to require a controller to
32 provide a product or service that requires the personal data
33 of a consumer that the controller does not collect or maintain
34 or to prohibit a controller from offering a different price,
35 rate, level, quality, or selection of goods or services to a

1 consumer, including offering goods or services for no fee,
2 if the consumer has exercised the consumer's right to opt
3 out pursuant to section 715D.3 or the offer is related to a
4 consumer's voluntary participation in a bona fide loyalty,
5 rewards, premium features, discounts, or club card program.

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

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

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

15 b. The purpose for processing personal data.

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

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

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

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

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

1 to create a new account in order to exercise consumer rights
2 pursuant to section 715D.3, but may require a consumer to use
3 an existing account.

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

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

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

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

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

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

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

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

35 d. Engage any subcontractor or agent pursuant to a written

1 contract in accordance with this section that requires the
2 subcontractor to meet the duties of the processor with respect
3 to the personal data.

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

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

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

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

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

19 b. Maintaining data in identifiable form.

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

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

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

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

35 c. The controller does not sell the personal data to any

1 third party or otherwise voluntarily disclose the personal data
2 to any third party other than a processor, except as otherwise
3 permitted in this chapter.

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

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

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

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

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

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

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

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

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

1 of a child prior to entering into a contract.

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

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

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

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

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

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

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

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

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

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

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

33 *b.* To effectuate a product recall.

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

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

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

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

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

1 course of a purely personal or household activity.

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

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

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

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

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

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

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

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

1 this chapter.

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

12 3. If a controller or processor continues to violate this
13 chapter following the cure period in subsection 2 or breaches
14 an express written statement provided to the attorney general
15 under that subsection, the attorney general may initiate an
16 action in the name of the state and may seek an injunction to
17 restrain any violations of this chapter and civil penalties of
18 up to seven thousand five hundred dollars for each violation
19 under this chapter. Any moneys collected under this section
20 including civil penalties, costs, attorney fees, or amounts
21 which are specifically directed shall be paid into the consumer
22 education and litigation fund established under section
23 714.16C.

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

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

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

32 2. Any reference to federal, state, or local law or statute
33 in this chapter shall be deemed to include any accompanying
34 rules or regulations or exemptions thereto, or in the case of a
35 federal agency, guidance issued by such agency thereto.

1 authority, agency, or body other than the consumer, controller,
2 processor, or an affiliate of the processor or the controller.
3 The bill contains other defined terms.

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

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

27 The bill requires that controllers provide responses to
28 defined personal data requests within 90 days of a consumer
29 initiating a request. Responses to personal data requests
30 shall be provided to a consumer free of charge up to twice per
31 year except where requests are overly burdensome or manifestly
32 unfounded. A business may extend the deadline for good cause,
33 including complexity, once by up to 45 days after informing the
34 consumer of the reason for the extension. The bill provides
35 that controllers are not required to comply with requests where

1 a controller is unable through commercially reasonable efforts
2 to verify the identity of the consumer submitting the request.
3 The bill requires that controllers permit consumers to access
4 an appeals process except in cases that are unable to be
5 authenticated and provide consumers with information regarding
6 the appeals process in situations where a consumer's request
7 is denied.

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

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

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

32 The bill includes personal data processing exemptions,
33 including pseudonymous data and de-identified data as defined
34 by the bill. The bill identifies exceptions where controllers
35 or processors are not required to comply with a consumer rights

1 request pursuant to the bill. The bill requires controllers
2 disclosing pseudonymous or de-identified data to exercise
3 reasonable oversight of contractual commitments regarding such
4 data.

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

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

18 The bill provides that the attorney general shall
19 investigate controllers and processors upon reasonable cause
20 for violations of provisions of the bill. The attorney general
21 shall provide 90 days' notice to a controller or processor
22 including the reason for which the entity is subject to an
23 investigation and permit the entity to cure the defect prior
24 to filing a civil action. A controller or processor found to
25 be in violation of provisions of the bill is subject to a civil
26 penalty of up to \$7,500 per violation. Moneys collected by the
27 attorney general under the bill shall be paid into the consumer
28 education and litigation fund established under Code section
29 714.16C.

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

33 The bill takes effect January 1, 2025.