IOWA HOUSE REPUBLICANS

**REPUBLICAN CAUCUS STAFF**
HOUSE OF REPRESENTATIVES
STATE CAPITOL
DES MOINES, IOWA 50319

IOWAHOUSEREPUBLICANS.COM

# HOUSE REPUBLICAN STAFF ANALYSIS

| | | | |
|---|---|---|---|
| Bill: | HF 2506 (Formerly HSB 674) | House Committee: | **PASSED** February 15 (15-0) |
| Committee: | Info Tech | House Floor: | |
| Floor Manager: | Rep. Sorensen | Senate Floor: | |
| Date: | March 9, 2022 | Governor: | |
| Staff: | Ben Gentz (1-3452) | | |

## Consumer Data Privacy

- Establishes consumer rights for personal data
- Sets requirements for how controllers and processors handle consumer's personal data

---

## Section by Section Analysis

*Section 1 – Definitions (715D.1)*
Defines the following terms:

| | | | |
|---|---|---|---|
| Affiliate | Aggregate data | Authenticate | Biometric data |
| Child | Consent | Consumer | Controller |
| Covered entity | De-identified data | Fund | Health care provider |
| HIPPA | Health record | Identified or identifiable natural person | Institution of higher education |
| Nonprofit organization | Personal data | Precise geolocation data | Process or processing |
| Processor | Protected health information | Pseudonymous data | Publicly available information |
| Sale of personal data | Sensitive data | State agency | Targeted advertising |
| Third party | Trade secret | | |

*Section 2 – Scope and exemptions (715D.2)*
Chapter applies to a person conducting business in the state or producing products or services that are targeted to consumers who are residents of the state and during a calendar year does either of:

- Controls or processes personal data of 100,000+ consumers
- Controls or processes personal data of 25,000+ consumers and derive 50%+ of gross revenue from sale of data

Chapter does not apply to:

- State of Iowa
- Political subdivisions
- Financial institutions or affiliates subject to Gramm-Leach-Bliley
- Entities governed by privacy, security, and breach notifications issued by IA DHS

- Entities governed by privacy, security, and breach notifications issued by IDPH
- Entities governed by privacy, security, and breach notifications issued by HIPPA
- Nonprofit organizations
- Institutions of higher education

Following information and data is exempt from this chapter:

- Health information protected by HIPPA
- Health records
- Information subject to Federal confidentiality of records laws
- Private information subject to federal protection of human subjects
- Identifiable information collected as part of human research projects
- Protection of human subjects under FDA regulations
- Personal data used or shared in research
- Information and documents created for purposes of HQIA
- Patient safety work product for purposes of PSQIA
- Healthcare related information de-identified pursuant to HIPPA
- Consumer information regulated by Fair Credit Reporting Act
- Personal data collected in compliance with Drivers Privacy Protection Act
- Personal data regulated by Family Educational Rights and Privacy Act
- Personal data in compliance with Farm Credit Act
- Data processed or maintained as follows:
    - Employed, acting as an agent, or independent contractor to the extent data is used within that role
    - Necessary to obtain benefits for an individual under an individual identified above
    - Emergency contact information
- Personal data used in accordance with COPPA

*Section 3 – Consumer Data Rights (715D.3)*

A consumer may invoke their consumer rights by submitting a request to a controller. A parent or guardian may invoke rights on behalf their child. A controller must comply with an authenticate request to do all of the following:

- Confirm if a controller is processing the consumer's personal data and has access to personal data
- Delete personal data provided by the consumer
- Obtain a copy of personal data previously provided by the customer to the controller
- Opt out of
    - Targeted advertising
    - Sale of personal data

Unless excepted, a controller shall comply with consumers request to exercise rights under the chapter

- Controller must respond to consumer without undue delay. Maximum time before response is 45 days with one 45-day extension, if reasonable
- If controller refuses to act on consumer's request, the consumer must be informed of the decision and receive instructions for how to appeal the decision. If controller suspects a fraudulent request, they may state they are unable to authenticate the request.
- Information must be provided to the consumer free of charge, up to twice per year
- If controller cannot reasonable authenticate the request, they can ask customer for additional information to authenticate request

Controller must establish a process for a consumer to appeal a decision to refuse action on a consumer's request. If appeal is denied, controller must also provide an online mechanism to appeal to the attorney general

*Section 4 – Data controller duties (715D.4)*

Controller must adopt and implement data security practices. A controller shall not process sensitive data without consumer's consent or if known child without processing in compliance with COPPA.

A controller cannot process data in violation of unlawful discrimination laws

Any provision of a contract or agreement that proports to waive or limit consumer's rights under section 3 are void and unenforceable

Consumers must be provided with a privacy notice that includes the following:

- Categories of personal data processes by controller
- Purpose for processing personal data
- How to exercise rights under section 3 and process for appeal
- Categories of personal data shared with third parties
- Categories of third parties with whom personal data is shared

If controller sells personal data to third parties they must clearly disclose and the manner for the consumer to opt out

Controller must describe in the privacy notice the way to submit a request. Controller cannot require customers to establish a new account to exercise their rights

*Section 5 – Processor duties (715D.5)*

A processor will assist a controller in obligations required under this chapter

- Respond to consumer requests under section 3
- Data security under section 2

Contract will govern duties of processor on behalf of controller and must include following requirements:

- Ensure each person processing personal data is subject to a duty of confidentiality regarding the data
- Delete or return all personal data at the end of services, unless the law dictates otherwise
- Demonstrate compliance to controller
- Engage any subcontractor or agent under the same responsibilities regarding personal data

Nothing relieves a controller or processor of imposed liabilities by virtue of their role in processing data

Determining if a person is a controller or a processor is a fact-based determination

*Section 6 – Processing data – exemptions (715D.6)*

Nothing in the chapter can be construed to require any of the following:

- Controller or processor to re-identify de-identified or pseudonymous data
- Maintain data in an identifiable form
- Collect, obtain, retain or access any data or technology to associate an authenticated customer with personal data

Nothing in the chapter can be construed to require a controller or processor to comply with an authenticated request under section 3 if all of the following are true:

- Controller is not reasonably capable of associating request with personal data or it would be unreasonably burdensome to associate the request with personal data
- Controller does not use personal data to recognize or respond to specific customers
- Controller does not sell personal data to any third party or in any other way voluntarily disclose personal data to a third party unless permitted under this chapter

Consumer rights in sections 3 and 4 do not apply to pseudonymous data where the controller is able to show any information used to identify the customer is kept separately and is subject to measures that ensure personal data is not attributed to an identified natural person

Controllers that disclose pseudonymous data or de-identified data must exercise oversight to monitor compliance and take appropriate steps to address any breaches

*Section 7 – Limitations (715D.7)*

Nothing in this chapter should be construed to restrict a controller or processors' ability to do the following:

- Comply with federal, state, or local laws, rules, or regulations
- Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal state, local or other governmental authorities
- Cooperate with law enforcement agencies regarding conduct or activity that may violate federal, state or local laws, rules, or regulations
- Investigate, establish, exercise, prepare for, or defend legal claims
- Provide a product or service specifically requested by a consumer, perform a contract to which the consumer is a party, or take steps at the request of the consumer prior to entering a contract
- Take immediate steps to protect an interest essential for the life or physical safety of the consumer or another natural person
- Prevent, detect protect against, or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities, or any illegal activity
- Preserve the integrity or security of systems
- Investigate, report, or prosecute those responsible for any such action
- Engage in public or peer reviewed research in the public interest that adheres to applicable ethics and privacy laws, and is approved, monitored and governed by an institutional review board or similar independent oversight entity that determines the following:
    - Deletion of information is likely to provide substantial benefits that are not exclusive to the controller
    - Expected benefits of research outweigh privacy risks
    - Controller has implemented safeguards to mitigate privacy risks associated with research
- Assist another controller, processor, or third party with any obligations under this subsection

Obligations imposed on a controller or processor under this chapter do not restrict a controller's or processor's ability to collect, use, or retain data as follows:

- Conduct internal research to develop, improve, or repair products, services, or technology
- Effectuate a product recall
- Identify and repair technical errors that impair functionality
- Perform internal operations that are aligned with consumer expectations based on relationship with the consumer

Obligations imposed do not apply where compliance would violate evidentiary privilege.

Controller or processor is not in violation if third party controller or processor is in violation and controller or processor had no actual knowledge that there was intent to violate the law.

Nothing in this chapter should be construed as an obligation imposed that adversely affects First Amendment rights or applies to the processing of personal data by a person in the course of personal or household activity

Personal data processed by a controller under this section cannot be processed for any purpose except those expressly identified. Personal data may be processed to the extent it is as follows:

- Reasonably necessary and proportionate to the purpose listed in this section
- Adequate, relevant, and limited to what is necessary in relation to specific purposes listed in this section

A controller processing personal data under an exemption in this section bears burden to demonstrate action qualifies and complies with requirements

Processing personal data for the purposed identified in subsection 1, does not make the entity a controller

Controller, processor, third party, and consumers are not required to disclose trade secrets

*Section 8 – Enforcement – Penalties (715D.8)*
Attorney general has exclusive authority to enforce the provisions of this chapter and is empowered to issue a civil investigative demand
Prior to initiating any action, the AG shall provide 30 days written notice identifying the specific provisions that have been or are being violated. If within that period the noticed violations are cured, and the AG is provided a written statement the violations have been cured and there is no additional violation, no action can be initiated.
If there continues to be a violation or breach of the written statement following the cure period, the AG may initiate an action and seek an injunction and civil penalties up to $7500 for each violation
The AG may recover reasonable expenses incurred in investigating and preparing the case, including attorney fees
Nothing in this chapter shall be construed to provide the basis for a private right of action for violations under this chapter

*Section 9 – Preemption (715D.9)*
Supersedes and preempts city, county, municipality, or local agency laws, etc. regarding the processing of personal data
References to federal, state, or local law are deemed to include any accompanying rules, regulations, exemptions, etc.

*Section 10 – Effective Date*
Takes effect January 1, 2024

---

## Amendment Analysis

**H-8157 by Sorensen** – Strike after amendment. See analysis above.

**H-8173 by Smith** – Escalates fines for violations based on amount of pecuniary loss