

FIRST REGULAR SESSION

SENATE COMMITTEE SUBSTITUTE FOR

SENATE BILL NO. 7

102ND GENERAL ASSEMBLY

1183S.03C

KRISTINA MARTIN, Secretary

AN ACT

To amend chapters 37 and 407, RSMo, by adding thereto eight new sections relating to the protection of data.

Be it enacted by the General Assembly of the State of Missouri, as follows:

Section A. Chapters 37 and 407, RSMo, are amended by
2 adding thereto eight new sections, to be known as sections
3 37.060, 37.065, 407.2000, 407.2005, 407.2010, 407.2015,
4 407.2020, and 407.2025, to read as follows:

37.060. 1. (1) There is hereby created within the
2 office of administration the position of chief data officer,
3 who shall be appointed by the commissioner of administration
4 and shall report to the chief information officer or, in the
5 absence of a chief information officer, the commissioner of
6 administration.

7 (2) The chief data officer is authorized to oversee
8 each state agency's management of electronic data for
9 purposes of evaluating appropriate management and security
10 of the data.

11 (3) The chief data officer may require each state
12 agency to:

13 (a) Classify its electronic data into levels of
14 sensitivity identified by the chief data officer and
15 regularly review and update such classifications;

16 (b) Develop, adopt, and regularly update a written
17 policy for responding to breaches and suspected breaches of
18 the agency's electronic data;

19 (c) Develop, adopt, and regularly update a written
20 policy for the proper disposal, consistent with chapter 109,
21 of the agency's electronic data, including requiring the
22 agency to use the office of administration's electronic
23 waste contract for that purpose;

24 (d) Adopt data collection standards and procedures
25 identified by the chief data officer; and

26 (e) Develop, adopt, and regularly update other
27 policies and procedures the chief data officer deems
28 necessary to evaluate appropriate management and security of
29 the agency's electronic data.

30 (4) The chief data officer may prevent any state
31 agency from procuring or utilizing any information or
32 communication technologies, services, components, networks,
33 or systems, that:

34 (a) It has determined to pose an unacceptable risk to
35 the safety and security of the state of Missouri due to a
36 connection to or use by a country that the chief data
37 officer deems to pose a threat to the security of the state
38 of Missouri;

39 (b) A federal agency has prohibited, restricted the
40 transactions or licensing of, or otherwise limited the use
41 of because of national security concerns;

42 (c) Are designed, developed, manufactured, or supplied
43 by companies or affiliates determined by any federal or
44 state department, division, or agency to be owned,
45 controlled by, or domiciled in a country that the chief data
46 officer deems to pose a threat to the security of the state
47 of Missouri.

48 (5) The chief data officer may prevent the exposure of
49 any communication technology, services, equipment,
50 components, networks, or systems of the state of Missouri to
51 persons or entities that are determined by any federal
52 department or state agency to be owned, controlled by, or
53 domiciled in a country that the chief data officer deems to
54 pose a threat to the security of the state of Missouri.

55 2. (1) Each state agency is responsible for
56 identifying its various types of electronic data, the
57 location of such data, and the level of security required
58 for each type of data.

59 (2) Each state agency shall communicate the
60 information described in subdivision (1) of this subsection
61 to the chief data officer and shall provide updated
62 information as necessary for the chief data officer to
63 evaluate the security of the agency's electronic data.

64 3. Each state agency shall cooperate with the chief
65 data officer in implementing this section. The chief data
66 officer may provide guidance to a state agency in fulfilling
67 the functions described in this section.

68 4. In the absence of a chief data officer, the
69 commissioner of administration, or his or her designee, may
70 exercise the authority granted in this section.

71 5. Nothing in this section shall be construed as:

72 (1) Waiving sovereign immunity against the state, any
73 agency of the state, or any officer or employee of the
74 state; or

75 (2) Creating a cause of action against the state, any
76 agency of the state, or any officer or employee of the state.

77 6. The office of administration may promulgate rules
78 to implement the provisions of this section. Any rule or
79 portion of a rule, as that term is defined in section

80 536.010, that is created under the authority delegated in
81 this section shall become effective only if it complies with
82 and is subject to all of the provisions of chapter 536 and,
83 if applicable, section 536.028. This section and chapter
84 536 are nonseverable and if any of the powers vested with
85 the general assembly pursuant to chapter 536 to review, to
86 delay the effective date, or to disapprove and annul a rule
87 are subsequently held unconstitutional, then the grant of
88 rulemaking authority and any rule proposed or adopted after
89 August 28, 2023, shall be invalid and void.

37.065. 1. Not later than January 1, 2024, the
2 commissioner of administration shall develop standards and
3 guidelines for all departments, divisions, and agencies of
4 the state requiring the removal of any covered application
5 from information technology.

6 2. This section shall not apply to the Missouri state
7 highway patrol to the extent necessary to conduct any law
8 enforcement activities.

9 3. For purposes of this section, the following terms
10 mean:

11 (1) "Covered application", the social networking
12 service TikTok or any successor application or service
13 developed or provided by ByteDance Limited or an entity
14 owned by ByteDance Limited;

15 (2) "Department", any department, office, board,
16 commission, bureau, institution, or any other agency of the
17 state;

18 (3) "Information technology", includes the following:

19 (a) Any equipment or interconnected system or
20 subsystem of equipment, used in the automatic acquisition,
21 storage, analysis, evaluation, manipulation, management,
22 movement, control, display, switching, interchange,

23 transmission, or reception of data or information by a
24 department, if the equipment is used by the department
25 directly or is used by a contractor under a contract with a
26 department that requires the use:

27 a. Of that equipment; or

28 b. Of that equipment to a significant extent in the
29 performance of a service or the furnishing of a product;

30 (b) Computers, ancillary equipment, including imaging
31 peripherals, input, output, and storage devices necessary
32 for security and surveillance;

33 (c) Peripheral equipment designed to be controlled by
34 the central processing unit of a computer, software,
35 firmware and similar procedures, services (including support
36 services), and related resources.

407.2000. For the purposes of sections 407.2000 to
2 407.2025, the following terms mean:

3 (1) "Account", the consumer privacy restricted account
4 established in section 407.2015;

5 (2) "Affiliate", an entity that:

6 (a) Controls, is controlled by, or is under common
7 control with another entity; or

8 (b) Shares common branding with another entity;

9 (3) "Aggregated data", information that relates to a
10 group or category of consumers:

11 (a) From which individual consumer identities have
12 been removed; and

13 (b) That is not linked or reasonably linkable to any
14 consumer;

15 (4) "Air carrier", the same meaning as in 49 U.S.C.
16 Section 40102;

17 (5) "Authenticate", using reasonable means to
18 determine that a consumer's request to exercise the rights

19 described in subsection 1 of section 407.2005 is made by the
20 consumer who is entitled to exercise those rights;

21 (6) (a) "Biometric data", data generated by automatic
22 measurements of an individual's unique biological
23 characteristics, including data that are generated by
24 automatic measurements of an individual's fingerprint,
25 voiceprint, eye retinas, irises, or any other unique
26 biological pattern or characteristic that is used to
27 identify a specific individual;

28 (b) "Biometric data" does not include:

29 a. A physical or digital photograph;

30 b. A video or audio recording;

31 c. Data generated from an item described in paragraph
32 (a) of this subdivision;

33 d. Information captured from a patient in a health
34 care setting; or

35 e. Information collected, used, or stored for
36 treatment, payment, or health care operations as those terms
37 are defined in 45 C.F.R. Parts 160, 162, and 164;

38 (7) "Business associate", the same meaning as in 45
39 C.F.R. Section 160.103;

40 (8) "Child", an individual younger than thirteen years
41 old;

42 (9) "Consumer", an individual who is a resident of
43 Missouri. "Consumer" does not include an individual acting
44 in an employment or commercial context;

45 (10) "Control" or "controlled", any of the following:

46 (a) Ownership of, or the power to vote, more than
47 fifty percent of the outstanding shares of any class of
48 voting securities of an entity;

49 (b) Control in any manner over the election of a
50 majority of the directors or of the individuals exercising
51 similar functions; or

52 (c) The power to exercise controlling influence of the
53 management of an entity;

54 (11) "Controller", a person doing business in Missouri
55 who determines the purposes for which and the means by which
56 personal data are processed, regardless of whether the
57 person makes the determination alone or with others;

58 (12) "Covered entity", the same meaning as in 45
59 C.F.R. Section 160.103;

60 (13) "Deidentified data", data that:

61 (a) Cannot reasonably be linked to an identified
62 individual or an identifiable individual; and

63 (b) Are possessed by a controller who:

64 a. Takes reasonable measures to ensure that a person
65 cannot associate the data with an individual;

66 b. Publicly commits to maintain and use the data only
67 in deidentified form and not attempt to reidentify the data;
68 and

69 c. Contractually obligates any recipients of the data
70 to comply with the requirements described in subparagraphs a
71 and b of this paragraph;

72 (14) "Identifiable individual", an individual who can
73 be readily identified, directly or indirectly;

74 (15) "Institution of higher education", a public or
75 private institution of higher education;

76 (16) "Personal data", information that is linked or
77 reasonably linkable to an identified individual or an
78 identifiable individual. "Personal data" does not include
79 deidentified data, aggregated data, or publicly available
80 information;

81 (17) "Process", an operation or set of operations
82 performed on personal data, including collection, use,
83 storage, disclosure, analysis, deletion, or modification of
84 personal data;

85 (18) "Processor", a person who processes personal data
86 on behalf of a controller;

87 (19) "Protected health information", the same meaning
88 as in 45 C.F.R. Section 160.103;

89 (20) "Pseudonymous data", personal data that cannot be
90 attributed to a specific individual without the use of
91 additional information, if the additional information is:

92 (a) Kept separate from the consumer's personal data;
93 and

94 (b) Subject to appropriate technical and
95 organizational measures to ensure that the personal data are
96 not attributable to an identified individual or an
97 identifiable individual;

98 (21) "Public body", the state of Missouri, any
99 department, division, agency, board, or commission of the
100 state, and any political subdivision;

101 (22) "Publicly available information", information
102 that a person:

103 (a) Lawfully obtains from a record of a public body;

104 (b) Reasonably believes a consumer or widely
105 distributed media has lawfully made available to the general
106 public; or

107 (c) If the consumer has not restricted the information
108 to a specific audience, obtains from a person to whom the
109 consumer disclosed the information;

110 (23) "Right", a consumer right described in subsection
111 1 of section 407.2005;

112 (24) "Sale", "sell", or "sold", the exchange of
113 personal data for monetary consideration by a controller to
114 a third party. "Sale", "sell", or "sold" does not include:

115 (a) A controller's disclosure of personal data to a
116 processor who processes the personal data on behalf of the
117 controller;

118 (b) A controller's disclosure of personal data to an
119 affiliate of the controller;

120 (c) Considering the context in which the consumer
121 provided the personal data to the controller, a controller's
122 disclosure of personal data to a third party if the purpose
123 is consistent with a consumer's reasonable expectations;

124 (d) The disclosure or transfer of personal data when a
125 consumer directs a controller to:

126 a. Disclose the personal data; or

127 b. Interact with one or more third parties;

128 (e) A consumer's disclosure of personal data to a
129 third party for the purpose of providing a product or
130 service requested by the consumer or a parent or legal
131 guardian of a child;

132 (f) The disclosure of information that the consumer:

133 a. Intentionally makes available to the general public
134 via a channel of mass media; and

135 b. Does not restrict to a specific audience; or

136 (g) A controller's transfer of personal data to a
137 third party as an asset that is part of a proposed or actual
138 merger, an acquisition, or a bankruptcy in which the third
139 party assumes control of all or part of the controller's
140 assets;

141 (25) (a) "Sensitive data", any of the following:

142 a. Personal data that reveals:

143 (i) An individual's racial or ethnic origin;

144 (ii) An individual's religious beliefs;
145 (iii) An individual's sexual orientation;
146 (iv) An individual's citizenship or immigration
147 status; or
148 (v) Information regarding an individual's medical
149 history, mental or physical health condition, or medical
150 treatment or diagnosis by a health care professional;
151 b. The processing of genetic personal data or
152 biometric data, if the processing is for the purpose of
153 identifying a specific individual; or
154 c. Specific geolocation data.
155 (b) "Sensitive data" does not include personal data
156 that reveals an individual's:
157 a. Racial or ethnic origin, if the personal data are
158 processed by a video communication service; or
159 b. Information regarding an individual's medical
160 history, mental or physical health condition, or medical
161 treatment or diagnosis by a health care professional;
162 (26) "Specific geolocation data", information derived
163 from technology, including global position system level
164 latitude and longitude coordinates, that directly identifies
165 an individual's specific location, accurate within a radius
166 of one thousand seven hundred fifty feet or less. "Specific
167 geolocation data" does not include:
168 (a) The content of a communication; or
169 (b) Any data generated by or connected to advanced
170 utility metering infrastructure systems or equipment for use
171 by a utility;
172 (27) "Targeted advertising", displaying an
173 advertisement to a consumer where the advertisement is
174 selected based on personal data obtained from the consumer's
175 activities over time and across nonaffiliated websites or

176 online applications to predict the consumer's preferences or
177 interests. "Targeted advertising" does not include
178 advertising:

179 (a) Based on a consumer's activities within a
180 controller's website or online application or any affiliated
181 website or online application;

182 (b) Based on the context of a consumer's current
183 search query or visit to a website or online application;

184 (c) Directed to a consumer in response to the
185 consumer's request for information, product, a service, or
186 feedback; or

187 (d) Processing personal data solely to measure or
188 report advertising:

189 a. Performance;

190 b. Reach; or

191 c. Frequency;

192 (28) "Third party", a person other than:

193 (a) The consumer, controller, or processor; or

194 (b) An affiliate or contractor of the controller or
195 the processor;

196 (29) "Trade secret", information, including a formula,
197 pattern, compilation, program, device, method, technique, or
198 process, that:

199 (a) Derives independent economic value, actual or
200 potential, from not being generally known to, and not being
201 readily ascertainable by proper means by, other persons who
202 can obtain economic value from the information's disclosure
203 or use; and

204 (b) Is the subject of efforts that are reasonable
205 under the circumstances to maintain the information's
206 secrecy.

407.2005. 1. A consumer has the right to:

2 (1) Confirm whether a controller is processing the
3 consumer's personal data;

4 (2) Access the consumer's personal data;

5 (3) Delete the consumer's personal data that the
6 consumer provided to the controller;

7 (4) Obtain a copy of the consumer's personal data,
8 that the consumer previously provided to the controller, in
9 a format that:

10 (a) To the extent technically feasible, is portable;

11 (b) To the extent practicable, is readily usable; and

12 (c) Allows the consumer to transmit the data to
13 another controller without impediment, where the processing
14 is carried out by automated means;

15 (5) Opt out of the processing of the consumer's
16 personal data for purposes of:

17 (a) Targeted advertising; or

18 (b) The sale of personal data.

19 2. (1) A consumer may exercise a right listed in
20 subsection 1 of this section by submitting a request to a
21 controller, by means prescribed by the controller,
22 specifying the right the consumer intends to exercise.

23 (2) In the case of processing personal data concerning
24 a known child, the parent or legal guardian of the known
25 child shall exercise a right on the child's behalf.

26 (3) In the case of processing personal data concerning
27 a consumer subject to guardianship, conservatorship, or
28 other protective arrangement, the guardian or the
29 conservator of the consumer shall exercise a right on the
30 consumer's behalf.

31 3. (1) Subject to the other provisions of this
32 section, a controller shall comply with a consumer's request
33 under subsection 2 of this section to exercise a right.

34 (2) (a) Within forty-five days after the day on which
35 a controller receives a request to exercise a right listed
36 under subsection 1 of this section, the controller shall:

37 a. Take action on the consumer's request; and

38 b. Inform the consumer of any action taken on the
39 consumer's request.

40 (b) The controller may extend the initial forty-five-
41 day period once by an additional forty-five days if
42 reasonably necessary due to the complexity of the request or
43 the volume of the requests received by the controller.

44 (c) If a controller extends the initial forty-five-day
45 period, before the initial forty-five-day period expires,
46 the controller shall:

47 a. Inform the consumer of the extension, including the
48 length of the extension; and

49 b. Provide the reasons the extension is reasonably
50 necessary.

51 (d) The forty-five-day period shall not apply if the
52 controller reasonably suspects the consumer's request is
53 fraudulent and the controller is not able to authenticate
54 the request before the forty-five-day period expires.

55 (3) If, in accordance with this section, a controller
56 chooses not to take action on a consumer's request, the
57 controller shall, within forty-five days after the day on
58 which the controller receives the request, inform the
59 consumer of the reasons for not taking action.

60 (4) (a) A controller may not charge a fee for
61 information in response to a request.

62 (b) a. Notwithstanding paragraph (a) of this
63 subdivision, a controller may charge a reasonable fee to
64 cover the administrative costs of complying with a request
65 or refuse to act on a request, if:

66 (i) The request is excessive, repetitive, technically
67 infeasible, or manifestly unfounded;

68 (ii) The controller reasonably believes the primary
69 purpose in submitting the request was something other than
70 exercising a right;

71 (iii) The request, individually or as part of an
72 organized effort, harasses, disrupts, or imposes undue
73 burden on the resources of the controller's business; or

74 (iv) The request is the consumer's second or
75 subsequent request during the same twelve-month period.

76 b. A controller that charges a fee or refuses to act
77 in accordance with this paragraph bears the burden of
78 demonstrating the request satisfied one or more of the
79 criteria described in subparagraph a. of this paragraph.

80 (5) If a controller is unable to authenticate a
81 consumer request to exercise a right described in subsection
82 1 of this section using commercially reasonable efforts, the
83 controller:

84 (a) Is not required to comply with the request; and

85 (b) May request that the consumer provide additional
86 information reasonably necessary to authenticate the request.

407.2010. 1. (1) A processor shall:

2 (a) Adhere to the controller's instructions; and

3 (b) Taking into account the nature of the processing
4 and information available to the processor, by appropriate
5 technical and organizational measures, insofar as reasonably
6 practicable, assist the controller in meeting the
7 controller's obligations.

8 (2) Before a processor performs processing on behalf
9 of a controller, the processor and controller shall enter
10 into a contract that:

11 (a) Clearly sets forth instructions for processing
12 personal data, the nature and purpose of the processing, the
13 type of data subject to processing, the duration of the
14 processing, and the parties' rights and obligations;

15 (b) Requires the processor to ensure each person
16 processing personal data is subject to a duty of
17 confidentiality with respect to the personal data; and

18 (c) Requires the processor to engage any subcontractor
19 pursuant to a written contract that requires the
20 subcontractor to meet the same obligations as the processor
21 with respect to the personal data.

22 (3) (a) Determining whether a person is acting as a
23 controller or processor with respect to a specific
24 processing of data is a fact-based determination that
25 depends upon the context in which personal data are to be
26 processed.

27 (b) A processor that adheres to a controller's
28 instructions with respect to a specific processing of
29 personal data remains a processor.

30 2. (1) (a) A controller shall provide consumers with
31 a reasonably accessible and clear privacy notice that
32 includes:

33 a. The categories of personal data processed by the
34 controller;

35 b. The purposes for which the categories of personal
36 data are processed;

37 c. How consumers may exercise a right;

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

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

42 (b) If a controller sells a consumer's personal data
43 to one or more third parties or engages in targeted
44 advertising, the controller shall clearly and conspicuously
45 disclose to the consumer the manner in which the consumer
46 may exercise the right to opt out of the:

47 a. Sale of the consumer's personal data; or

48 b. Processing for targeted advertising.

49 (2) (a) A controller shall establish, implement, and
50 maintain reasonable administrative, technical, and physical
51 data security practices designed to:

52 a. Protect the confidentiality and integrity of
53 personal data; and

54 b. Reduce reasonably foreseeable risks of harm to
55 consumers relating to the processing of personal data.

56 (b) Considering the controller's business size, scope,
57 and type, a controller shall use data security practices
58 that are appropriate for the volume and nature of the
59 personal data at issue.

60 (3) Except as otherwise provided in sections 407.2000
61 to 407.2025, a controller may not process sensitive data
62 collected from a consumer without:

63 (a) First presenting the consumer with clear notice
64 and an opportunity to opt out of the processing; or

65 (b) In the case of the processing of personal data
66 concerning a known child, processing the data in accordance
67 with the federal Children's Online Privacy Protection Act,
68 15 U.S.C. Section 6501 et seq., and the act's implementing
69 regulations and exemptions.

70 (4) (a) A controller may not discriminate against a
71 consumer for exercising a right by:

72 a. Denying a good or service to the consumer;

73 b. Charging the consumer a different price or rate for
74 a good or service; or

75 c. Providing the consumer a different level of quality
76 of a good or service.

77 (b) This subdivision shall not prohibit a controller
78 from offering a different price, rate, level, quality, or
79 selection of a good or service to a consumer, including
80 offering a good or service for no fee or at a discount, if:

81 a. The consumer has opted out of targeted advertising;
82 or

83 b. The offer is related to the consumer's voluntary
84 participation in a bona fide loyalty, rewards, premium
85 features, discounts, or club card program.

86 (5) A controller is not required to provide a product,
87 service, or functionality to a consumer if:

88 (a) The consumer's personal data are or the processing
89 of the consumer's personal data is reasonably necessary for
90 the controller to provide the consumer the product, service,
91 or functionality; and

92 (b) The consumer does not:

93 a. Provide the consumer's personal data to the
94 controller; or

95 b. Allow the controller to process the consumer's
96 personal data.

97 (6) Any provision of a contract that purports to waive
98 or limit a consumer's right described in subsection 1 of
99 section 407.2005 is void.

100 3. (1) The provisions of sections 407.2000 to
101 407.2025 do not require a controller or processor to:

102 (a) Reidentify deidentified data or pseudonymous data;

103 (b) Maintain data in identifiable form or obtain,
104 retain, or access any data or technology for the purpose of

105 allowing the controller or processor to associate a consumer
106 request with personal data; or

107 (c) Comply with an authenticated consumer request to
108 exercise a right described in subsection 1 of section
109 407.2005, if:

110 a. (i) The controller is not reasonably capable of
111 associating the request with the personal data; or

112 (ii) It would be unreasonably burdensome for the
113 controller to associate the request with the personal data;

114 b. The controller does not:

115 (i) Use the personal data to recognize or respond to
116 the consumer who is the subject of the personal data; or

117 (ii) Associate the personal data with other personal
118 data about the consumer; and

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

122 (2) The rights described in subsection 1 of section
123 407.2005 do not apply to pseudonymous data if a controller
124 demonstrates that any information necessary to identify a
125 consumer is kept:

126 (a) Separately; and

127 (b) Subject to appropriate technical and
128 organizational measures to ensure the personal data are not
129 attributed to an identified individual or an identifiable
130 individual.

131 (3) A controller who uses pseudonymous data or
132 deidentified data shall take reasonable steps to ensure the
133 controller:

134 (a) Complies with any contractual obligations to which
135 the pseudonymous data or deidentified data are subject; and

136 (b) Promptly addresses any breach of a contractual
137 obligation described in paragraph (a) of this subdivision.

138 4. (1) The requirements described in sections
139 407.2000 to 407.2025 do not restrict a controller's or
140 processor's ability to:

141 (a) Comply with a federal, state, or local law, rule,
142 or regulation;

143 (b) Comply with a civil, criminal, or regulatory
144 inquiry, investigation, subpoena, or summons by a federal,
145 state, or local entity;

146 (c) Cooperate with a law enforcement agency concerning
147 activity that the controller or processor reasonably and in
148 good faith believes may violate federal, state, or local
149 laws, rules, or regulations;

150 (d) Investigate, establish, exercise, prepare for, or
151 defend a legal claim;

152 (e) Provide a product or service requested by a
153 consumer or a parent or legal guardian of a child;

154 (f) Perform a contract to which the consumer or the
155 parent or legal guardian of a child is a party, including
156 fulfilling the terms of a written warranty or taking steps
157 at the request of the consumer or parent or legal guardian
158 before entering into the contract with the consumer;

159 (g) Take immediate steps to protect an interest that
160 is essential for the life or physical safety of the consumer
161 or of another individual;

162 (h) a. Detect, prevent, protect against, or respond
163 to a security incident, identity theft, fraud, harassment,
164 malicious or deceptive activity, or any illegal activity; or

165 b. Investigate, report, or prosecute a person
166 responsible for an action described in subparagraph a of
167 this paragraph;

168 (i) a. Preserve the integrity or security of systems;
169 or

170 b. Investigate, report, or prosecute a person
171 responsible for harming or threatening the integrity or
172 security of systems, as applicable;

173 (j) If the controller discloses the processing in a
174 notice described in subsection 2 of this section, engage in
175 public or peer-reviewed scientific, historical, or
176 statistical research in the public interest that adheres to
177 all other applicable ethics and privacy laws;

178 (k) Assist another person with an obligation described
179 in this subsection;

180 (l) Process personal data to:

181 a. Conduct internal analytics or other research to
182 develop, improve, or repair a controller's or processor's
183 product, service, or technology;

184 b. Identify and repair technical errors that impair
185 existing or intended functionality; or

186 c. Effectuate a product recall;

187 (m) Process personal data to perform an internal
188 operation that is:

189 a. Reasonably aligned with the consumer's expectations
190 based on the consumer's existing relationship with the
191 controller; or

192 b. Otherwise compatible with processing to aid the
193 controller or processor in providing a product or service
194 specifically requested by a consumer or a parent or legal
195 guardian of a child or the performance of a contract to
196 which the consumer or a parent or legal guardian of a child
197 is a party; or

198 (n) Retain a consumer's email address to comply with
199 the consumer's request to exercise a right.

200 (2) Sections 407.2000 to 407.2025 shall not apply if a
201 controller's or processor's compliance with such sections:

202 (a) Violates an evidentiary privilege under Missouri
203 law or supreme court rules;

204 (b) As part of a privileged communication, prevents a
205 controller or processor from providing personal data
206 concerning a consumer to a person covered by an evidentiary
207 privilege under Missouri law or supreme court rules; or

208 (c) Adversely affects the privacy or other rights of
209 any person.

210 (3) A controller or processor is not in violation of
211 sections 407.2000 to 407.2025 if:

212 (a) The controller or processor discloses personal
213 data to a third party controller or processor in compliance
214 with sections 407.2000 to 407.2025;

215 (b) The third party processes the personal data in
216 violation of sections 407.2000 to 407.2025; and

217 (c) The disclosing controller or processor did not
218 have actual knowledge of the third party's intent to commit
219 a violation of sections 407.2000 to 407.2025.

220 (4) If a controller processes personal data pursuant
221 to an exemption described in subdivision (1) of this
222 subsection, the controller bears the burden of demonstrating
223 that the processing qualifies for the exemption.

224 (5) Nothing in sections 407.2000 to 407.2025 shall
225 require a controller, processor, third party, or consumer to
226 disclose a trade secret.

227 5. A violation of sections 407.2000 to 407.2025 does
228 not provide a basis for, nor is a violation of such sections
229 subject to, a private right of action under such sections or
230 any other law.

407.2015. 1. (1) The attorney general shall
2 establish and administer a system to receive consumer
3 complaints regarding a controller's or processor's alleged
4 violation of sections 407.2000 to 407.2025.

(2) The attorney general may investigate a consumer
6 complaint to determine whether the controller or processor
7 violated or is violating sections 407.2000 to 407.2025.

2. (1) The attorney general has the exclusive
9 authority to enforce sections 407.2000 to 407.2025.

(2) The attorney general may initiate an enforcement
11 action against a controller or processor for a violation of
12 sections 407.2000 to 407.2025 at any time.

(3) (a) At least thirty days before the day on which
14 the attorney general initiates an enforcement action against
15 a controller or processor, the attorney general shall
16 provide the controller or processor:

a. Written notice identifying each provision of
18 sections 407.2000 to 407.2025 the attorney general alleges
19 the controller or processor has violated or is violating; and

b. An explanation of the basis for each allegation.

(b) The attorney general may not initiate an action if
22 the controller or processor:

a. Cures the noticed violation within thirty days
24 after the day on which the controller or processor receives
25 the written notice described in paragraph (a) of this
26 subdivision; and

b. Provides the attorney general an express written
28 statement that:

(i) The violation has been cured; and

(ii) No further violation of the cured violation will
31 occur.

32 (c) The attorney general may initiate an action in
33 circuit court against a controller or processor who:

34 a. Fails to cure a violation after receiving the
35 notice described in paragraph (a) of this subdivision; or

36 b. After curing a noticed violation and providing a
37 written statement in accordance with paragraph (b) of this
38 subdivision, continues to violate sections 407.2000 to
39 407.2025.

40 (d) In an action described in paragraph (c) of this
41 subdivision, the attorney general may recover:

42 a. Actual damages to the consumer; and

43 b. For each violation described in paragraph (c) of
44 this subdivision, an amount not to exceed seven thousand
45 five hundred dollars.

46 (4) All money received from an action under this
47 chapter shall be deposited into the consumer privacy account
48 established in subsection 3 of this section.

49 (5) If more than one controller or processor are
50 involved in the same processing in violation of sections
51 407.2000 to 407.2025, the liability for the violation shall
52 be allocated among the controllers or processors according
53 to the principles of comparative fault.

54 3. (1) There is hereby created in the state treasury
55 a fund to be known as the "Consumer Privacy Fund". The
56 state treasurer shall be custodian of the fund. In
57 accordance with sections 30.170 and 30.180, the state
58 treasurer may approve disbursements. The fund shall be a
59 dedicated fund and money in the fund shall be used solely by
60 the office of administration for the purposes of protection
61 of data.

62 (2) Notwithstanding the provisions of section 33.080
63 to the contrary, any moneys remaining in the fund at the end

64 of the biennium shall not revert to the credit of the
65 general revenue fund.

66 (3) The state treasurer shall invest moneys in the
67 fund in the same manner as other funds are invested. Any
68 interest and moneys earned on such investments shall be
69 credited to the fund.

70 4. (1) The attorney general shall compile a report:

71 (a) Evaluating the liability and enforcement
72 provisions of this section, including the effectiveness of
73 the attorney general's efforts to enforce sections 407.2000
74 to 407.2025; and

75 (b) Summarizing the data protected and not protected
76 by sections 407.2000 to 407.2025 including, with reasonable
77 detail, a list of the types of information that are publicly
78 available from local, state, and federal government sources.

79 (2) The attorney general shall submit the report to
80 the speaker of the house of representatives and president
81 pro tempore of the senate not later than July first in each
82 odd-numbered year.

407.2020. No political subdivision shall establish,
2 implement, or otherwise enforce any law or ordinance that
3 conflicts with the provisions of sections 407.2000 to
4 407.2025.

407.2025. 1. Sections 407.2000 to 407.2025 applies to
2 any controller or processor that:

3 (1) (a) Conducts business in this state; or

4 (b) Produces a product or service that is targeted to
5 consumers who are residents of this state;

6 (2) Has annual revenue of twenty-five million dollars
7 or more; and

8 (3) Satisfies at least one of the following:

9 (a) During a calendar year, controls or processes the
10 personal data of one hundred thousand or more consumers; or

11 (b) Derives over fifty percent of its gross revenue
12 from the sale of personal data and controls or processes
13 personal data of twenty-five thousand or more consumers.

14 2. Sections 407.2000 to 407.2025 do not apply to the
15 following:

16 (1) A public body or a third party who has contracted
17 with a public body when acting on behalf of a public body;

18 (2) An institution of higher education;

19 (3) A nonprofit corporation;

20 (4) A covered entity;

21 (5) A business associate;

22 (6) Information used solely for public health
23 activities and purposes as described in 45 CFR Section
24 164.512;

25 (7) A financial institution or an affiliate of a
26 financial institution governed by Title V of the Gramm-Leach-
27 Bliley Act, 15 U.S.C. Section 6801, et seq., and related
28 regulations;

29 (8) Personal data collected, processed, sold, or
30 disclosed in accordance with Title V of the Gramm-Leach-
31 Bliley Act, 15 U.S.C. Section 6801, et seq., and related
32 regulations;

33 (9) Personal data collected, processed, sold, or
34 disclosed in accordance with the federal Driver's Privacy
35 Protection Act of 1994, 18 U.S.C. Section 2721, et seq.;

36 (10) Personal data regulated by the federal Family
37 Education Rights and Privacy Act, 20 U.S.C. Section 1232g,
38 and related regulations;

39 (11) Personal data collected, processed, sold, or
40 disclosed in accordance with the federal Farm Credit Act of
41 1971, 12 U.S.C. Section 2001, et seq.;

42 (12) An individual's processing of personal data for
43 purely personal or household purposes;

44 (13) An air carrier;

45 (14) Information that meets any of the following
46 definitions:

47 (a) Protected health information for purposes of the
48 federal Health Insurance Portability and Accountability Act
49 of 1996, 42 U.S.C. Section 1320d, et seq., and related
50 regulations;

51 (b) Patient identifying information for purposes of 42
52 CFR Part 2;

53 (c) Identifiable private information for purposes of
54 the Federal Policy for the Protection of Human Subjects, 45
55 CFR Part 46;

56 (d) Identifiable private information or personal data
57 collected as part of human subjects research pursuant to or
58 under the same standards as:

59 a. The good clinical practice guidelines issued by the
60 International Council for Harmonisation; or

61 b. The Protection of Human Subjects under 21 CFR Part
62 50 and Institutional Review Boards under 21 CFR Part 56;

63 (e) Personal data used or shared in research conducted
64 in accordance with one or more of the requirements described
65 in paragraph (c) of this subdivision;

66 (f) Information and documents created for purposes of
67 the federal Health Care Quality Improvement Act of 1986, 42
68 U.S.C. Section 11101, et seq., and related regulations;

69 (g) Patient safety work product for purposes of 42 CFR
70 Part 3; or

71 (h) Information that is:

72 a. Deidentified in accordance with the requirements
73 for deidentification set forth in 45 CFR Part 164; and

74 b. Derived from any of the health care-related
75 information listed in this subdivision;

76 (15) Information originating from, and intermingled to
77 be indistinguishable with, information under subdivision

78 (14) of this subsection that is maintained by:

79 (a) A health care facility or health care provider; or

80 (b) A program or a qualified service organization as
81 defined in 42 CFR Section 2.11;

82 (16) An activity that meets the following:

83 (a) The activity is by one of the following:

84 a. A consumer reporting agency, as defined in 15
85 U.S.C. Section 1681a;

86 b. A furnisher of information, as set forth in 15
87 U.S.C. Section 1681s-2, who provides information for use in
88 a consumer report, as defined in 15 U.S.C. Section 1681a; or

89 c. A user of a consumer report, as set forth in 15
90 U.S.C. Section 1681b;

91 (b) The activity is subject to regulation under the
92 federal Fair Credit Reporting Act, 15 U.S.C. Section 1681,
93 et seq.; and

94 (c) The activity involves the collection, maintenance,
95 disclosure, sale, communication, or use of any personal data
96 bearing on a consumer's:

97 a. Credit worthiness;

98 b. Credit standing;

99 c. Credit capacity;

100 d. Character;

101 e. General reputation;

102 f. Personal characteristics; or

103 g. Mode of living;

104 (17) Data that are processed or maintained:

105 (a) In the course of an individual applying to, being
106 employed by, or acting as an agent or independent contractor
107 of a controller, processor, or third party, to the extent
108 the collection and use of the data are related to the
109 individual's role;

110 (b) As the emergency contact information of an
111 individual described in paragraph (a) of this subdivision
112 and used for emergency contact purposes; or

113 (c) To administer benefits for another individual
114 relating to an individual described in paragraph (a) of this
115 subdivision and used for the purpose of administering the
116 benefits.

✓