SECOND REGULAR SESSION

SENATE BILL NO. 731

102ND GENERAL ASSEMBLY

INTRODUCED BY SENATOR ROWDEN.

3021S.01I KRISTINA MARTIN, Secretary

AN ACT

To amend chapter 407, RSMo, by adding thereto six new sections relating to the protection of data.

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

Section A. Chapter 407, RSMo, is amended by adding thereto six new sections, to be known as sections 407.2100, 407.2105, 407.2110, 407.2115, 407.2120, and 407.2125, to read as follows:

407.2100. For the purposes of sections 407.2100 to 407.2125, the following terms mean:

(1) "Account", the consumer privacy restricted account established in section 407.2115;

(2) "Affiliate", an entity that:

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

(b) Shares common branding with another entity;

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

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

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

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

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

described in subsection 1 of section 407.2105 is made by the consumer who is entitled to exercise those rights;

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

(b) "Biometric data" does not include:

a. A physical or digital photograph;

b. A video or audio recording;

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

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

e. Information collected, used, or stored for treatment, payment, or health care operations as those terms are defined in 45 CFR Parts 160, 162, and 164;

(7) "Business associate", the same meaning as in 45 CFR Section 160.103;

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

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

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

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

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

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

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

(12) "Covered entity", the same meaning as in 45 CFR Section 160.103;

(13) "Deidentified data", data that:

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

(b) Are possessed by a controller who:

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

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

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

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

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

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

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

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

(19) "Protected health information", the same meaning as in 45 CFR Section 160.103;

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

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

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

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

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

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

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

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

(23) "Right", a consumer right described in subsection 1 of section 407.2105;

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

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

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

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

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

a. Disclose the personal data; or

b. Interact with one or more third parties;

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

(f) The disclosure of information that the consumer:

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

b. Does not restrict to a specific audience; or

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

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

a. Personal data that reveals:

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

(ii) An individual's religious beliefs;

(iii) An individual's sexual orientation;

(iv) An individual's citizenship or immigration status; or

(v) Information regarding an individual's medical history, mental or physical health condition, or medical treatment or diagnosis by a health care professional;

b. The processing of genetic personal data or biometric data, if the processing is for the purpose of identifying a specific individual; or

c. Specific geolocation data.

(b) "Sensitive data" does not include personal data that reveals an individual's racial or ethnic origin, if the personal data are processed by a video communication service;

(26) "Specific geolocation data", information derived from technology, including global position system level latitude and longitude coordinates, that directly identifies an individual's specific location, accurate within a radius of one thousand seven hundred fifty feet or less. "Specific geolocation data" does not include:

(a) The content of a communication; or

(b) Any data generated by or connected to advanced utility metering infrastructure systems or equipment for use by a utility;

(27) "Targeted advertising", displaying an advertisement to a consumer where the advertisement is selected based on personal data obtained from the consumer's activities over time and across nonaffiliated websites or online applications to predict the consumer's preferences or interests. "Targeted advertising" does not include advertising:

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

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

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

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

a. Performance;

b. Reach; or

c. Frequency;

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

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

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

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

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

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

407.2105. 1. A consumer has the right to:

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

(2) Access the consumer's personal data;

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

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

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

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

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

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

(a) Targeted advertising; or

(b) The sale of personal data.

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

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

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

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

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

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

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

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

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

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

b. Provide the reasons the extension is reasonably necessary.

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

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

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

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

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

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

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

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

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

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

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

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

407.2110. 1. (1) A processor shall:

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

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

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

(a) Clearly sets forth instructions for processing personal data, the nature and purpose of the processing, the

type of data subject to processing, the duration of the processing, and the parties' rights and obligations;

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

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

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

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

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

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

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

c. How consumers may exercise a right;

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

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

(b) If a controller sells a consumer's personal data to one or more third parties or engages in targeted advertising, the controller shall clearly and conspicuously

disclose to the consumer the manner in which the consumer may exercise the right to opt out of the:

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

b. Processing for targeted advertising.

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

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

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

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

(3) Except as otherwise provided in sections 407.2100 to 407.2125, a controller may not process sensitive data collected from a consumer without:

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

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

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

a. Denying a good or service to the consumer;

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

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

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

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

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

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

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

(b) The consumer does not:

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

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

(6) Any provision of a contract that purports to waive or limit a consumer's right described in subsection 1 of section 407.2105 is void.

3. (1) The provisions of sections 407.2100 to 407.2125 do not require a controller or processor to:

(a) Reidentify deidentified data or pseudonymous data;

(b) Maintain data in identifiable form or obtain, retain, or access any data or technology for the purpose of allowing the controller or processor to associate a consumer request with personal data; or

(c) Comply with an authenticated consumer request to exercise a right described in subsection 1 of section 407.2105, if:

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

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

b. The controller does not:

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

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

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

(2) The rights described in subsection 1 of section 407.2105 do not apply to pseudonymous data if a controller demonstrates that any information necessary to identify a consumer is kept:

(a) Separately; and

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

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

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

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

4. (1) The requirements described in sections 407.2100 to 407.2125 do not restrict a controller's or processor's ability to:

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

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

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

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

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

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

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

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

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

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

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

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

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

(l) Process personal data to:

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

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

c. Effectuate a product recall;

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

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

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

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

(2) Sections 407.2100 to 407.2125 shall not apply if a controller's or processor's compliance with such sections:

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

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

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

(3) A controller or processor is not in violation of sections 407.2100 to 407.2125 if:

(a) The controller or processor discloses personal data to a third party controller or processor in compliance with sections 407.2100 to 407.2125;

(b) The third party processes the personal data in violation of sections 407.2100 to 407.2125; and

(c) The disclosing controller or processor did not have actual knowledge of the third party's intent to commit a violation of sections 407.2100 to 407.2125.

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

(5) Nothing in sections 407.2100 to 407.2125 shall require a controller, processor, third party, or consumer to disclose a trade secret.

5. A violation of sections 407.2100 to 407.2125 does not provide a basis for, nor is a violation of such sections subject to, a private right of action under such sections or any other law.

407.2115. 1. (1) The attorney general shall establish and administer a system to receive consumer

complaints regarding a controller's or processor's alleged violation of sections 407.2100 to 407.2125.

(2) The attorney general may investigate a consumer complaint to determine whether the controller or processor violated or is violating sections 407.2100 to 407.2125.

2. (1) The attorney general has the exclusive authority to enforce sections 407.2100 to 407.2125.

(2) The attorney general may initiate an enforcement action against a controller or processor for a violation of sections 407.2100 to 407.2125 at any time.

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

a. Written notice identifying each provision of sections 407.2100 to 407.2125 the attorney general alleges 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 the controller or processor:

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

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

(i) The violation has been cured; and

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

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

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

b. After curing a noticed violation and providing a written statement in accordance with paragraph (b) of this subdivision, continues to violate sections 407.2100 to 407.2125.

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

a. Actual damages to the consumer; and

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

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

(5) If more than one controller or processor are involved in the same processing in violation of sections 407.2100 to 407.2125, the liability for the violation shall be allocated among the controllers or processors according to the principles of comparative fault.

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

(2) Notwithstanding the provisions of section 33.080 to the contrary, any moneys remaining in the fund at the end of the biennium shall not revert to the credit of the general revenue fund.

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

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

(a) Evaluating the liability and enforcement provisions of this section, including the effectiveness of the attorney general's efforts to enforce sections 407.2100 to 407.2125; and

(b) Summarizing the data protected and not protected by sections 407.2100 to 407.2125 including, with reasonable detail, a list of the types of information that are publicly available from local, state, and federal government sources.

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

407.2120. No political subdivision shall establish, implement, or otherwise enforce any law or ordinance that conflicts with the provisions of sections 407.2100 to 407.2125.

407.2125. 1. Sections 407.2100 to 407.2125 applies to any controller or processor that:

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

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

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

(3) Satisfies at least one of the following:

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

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

2. Sections 407.2100 to 407.2125 do not apply to the following:

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

(2) An institution of higher education;

(3) A nonprofit corporation;

(4) A covered entity;

(5) A business associate;

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

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

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

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

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

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

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

(13) An air carrier;

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

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

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

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

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

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

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

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

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

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

(h) Information that is:

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

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

(15) Information originating from, and intermingled to be indistinguishable with, information under subdivision (14) of this subsection that is maintained by:

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

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

(16) An activity that meets the following:

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

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

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

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

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

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

a. Credit worthiness;

b. Credit standing;

c. Credit capacity;

d. Character;

e. General reputation;

f. Personal characteristics; or

g. Mode of living;

(17) Data that are processed or maintained:

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

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

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

✓