SENATE

KENTUCKY GENERAL ASSEMBLY AMENDMENT FORM

2023 REGULAR SESSION

Amend printed copy of **SB 15**

On page 2, lines 4 to 12, delete in their entirety and insert in lieu thereof:

"***(6) "Consent" means a clear affirmative act signifying a consumer's freely given, specific, informed, and unambiguous agreement to the processing of personal data relating to the consumer. "Consent" may include a written statement including a statement written by electronic means or any other unambiguous affirmative action;***"; and

On page 2, lines 22 to 24, delete in their entirety and insert in lieu thereof:

"***(10) "Decisions that produce legal or similarly significant effects concerning a consumer" means decisions made by the controller that results in the provision of denial by the controller of financial and lending services, housing, insurance, education, enrollment, criminal justice, employment opportunities, health care services, or access to basic necessities such as food or water;***"; and

On page 2, lines 25 to 26, delete "***used to infer information about, or otherwise be associated with,***" and insert in lieu thereof "***linked to***"; and

On p. 4, lines 1 to 5, delete in their entirety and insert in lieu thereof:

"***(16) "Identified or identifiable natural person" means a person who can be readily identified directly or indirectly;***"; and

On p. 4, lines 22 to 26, delete in their entirety and insert in lieu thereof:

"***(19) "Personal data" means any information, including sensitive data, that is linked or***

Amendment No. SFA 2 Rep. Sen. Damon Thayer

Committee Amendment Signed:

Floor Amendment LRC Drafter:

Adopted: Date:

Rejected: Doc. ID: XXXX

reasonably linkable to an identified or identifiable natural person. "Personal data" does not include deidentified data or publicly available information;"; and

On page 5, lines 13 to 16, delete in their entirety and insert in lieu thereof:

"***(23) "Profiling" means any form of automated processing performed on personal data to evaluate, analyze, or predict personal aspects related to an identified or identifiable natural person's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements;***"; and

On page 6, lines 3 to 21, delete in their entirety and insert in lieu thereof:

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

(a) The disclosure of personal data to a processor that processes the personal data on behalf of the controller;

(b) The disclosure of personal data to a third party for purposes of providing a product or service requested by the consumer;

(c) The disclosure or transfer of personal data to an affiliate of the controller;

(d) The disclosure of information that the consumer intentionally made available to the general public via a channel of mass media and did not restrict to a specific audience; or

(e) The disclosure or transfer of personal data to a third party as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the controller's assets;"; and

Beginning on page 6, lines 22 to 27, and continuing onto page 7, lines 1 to 3, delete in their entirety and insert in lieu thereof:

"***(28) "Sensitive data" means a category of personal data that includes:***

(a) Racial or ethnic origin, religious beliefs, mental or physical health diagnosis,

sexual orientation, or citizenship or immigration status;

(b) Genetic or biometric data that is processed for the purpose of uniquely identifying a natural person;

(c) The personal data collected from a known child; or

(d) Precise geolocation data;"; and

On page 7, lines 4 to 22, delete in their entirety; and

On page 7, line 23, delete "***30***" and insert "***29***"; and'

Beginning on page 7, line 27, and continuing onto page 8, lines 1 to 11, delete in their entirety and insert in lieu thereof:

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

(a) Advertisements based on activities within a controller's websites or online applications;

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

(c) Advertisements directed to a consumer in response to the consumer's request for information or feedback; or

(d) Processing personal data processed solely for measuring or reporting advertising performance, reach, or frequency;"; and

On page 8, line 12, delete "***32***" and insert "***31***"; and'

On page 8, lines 15 to 22, delete in their entirety; and

On page 8, line 23, delete "***34***" and insert "***32***"; and'

On page 10, line 2, delete "***, their affiliates,***"; and

On page 11, line 1 delete "***or***"; and

On page 11, line 4, after "***thereunder***", insert "***; or***

(i) Small telephone utility as defined in KRS 278.516 or a Tier III CMRS provider as defined in KRS 65.7621 that does not sell or share personal data with any third-party processor"; and

Beginning on page 13 and continuing to page 23, delete Sections 3, 4, and 5 in their entirety and insert in lieu thereof:

"➔SECTION 3. A NEW SECTION OF KRS CHAPTER 367 IS CREATED TO READ AS FOLLOWS:

(1) A consumer may invoke the consumer rights authorized pursuant to this section at any time by submitting a request to a controller, via the means specified by the controller pursuant to Section 4 of this Act, specifying the consumer rights the consumer wishes to invoke. A child's parent or legal guardian may invoke such consumer rights on behalf of the child regarding processing personal data belonging to the child.

(2) A controller shall comply with an authenticated consumer request to exercise the right to:

(a) Confirm whether or not a controller is processing the consumer's personal data and to access such personal data;

(b) Delete personal data provided by or obtained about the consumer;

(c) Correct inaccuracies in the consumer's personal data, taking into account the nature of the personal data and the purposes of the processing of the consumer's personal data;

(d) Obtain a copy of the consumer's personal data that the consumer previously provided to the controller in a portable and, to the extent technically practicable, readily usable format that allows the consumer to read or transmit the data to

another controller without hindrance, where the processing is carried out by automated means;

(e) Opt out of targeted advertising;

(f) Opt out of profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer; and

(g) Opt out of the sale of personal data.

(3) Except as otherwise provided in subsection (6) of this section and Sections 6 and 7 of this Act, a controller shall comply with a request by a consumer to exercise the consumer rights pursuant to this section as follows:

(a) A controller shall respond to the consumer without undue delay, but in all cases within forty-five (45) days of receipt of the request submitted pursuant to the methods described in this section. The response period may be extended once by forty-five (45) additional days when reasonably necessary, taking into account the complexity and number of the consumer's requests, so long as the controller informs the consumer of any such extension within the initial forty-five (45) day response period, together with the reason for the extension;

(b) If a controller declines to take action regarding the consumer's request, the controller shall inform the consumer without undue delay, but in all cases and at the latest within forty-five (45) days of receipt of the request, of the justification for declining to take action; and

(c) Information provided in response to a consumer request shall be provided by a controller free of charge, at least twice annually per consumer. If a request from a consumer is excessive, repetitive, technically infeasible, or manifestly unfounded, the controller may charge the consumer a reasonable fee to cover the administrative costs of complying with the request or decline to act on the request.

The controller bears the burden of demonstrating the excessive, repetitive, technically infeasible, or manifestly unfounded nature of the request.

(4) A controller shall not be required to comply with a request to exercise any of the rights set forth in this section if the controller is unable to authenticate the request using commercially reasonable efforts. In such a case, the controller may, but is not required to, request the provision of additional information reasonably necessary to authenticate the request.

(5) A controller shall:

(a) Establish an internal process whereby a consumer may appeal a refusal to take action on a request to exercise any of the rights set forth in this section within a reasonable period of time after the controller refuses to take action on such request;

(b) Ensure that the appeal process is conspicuously available and similar to the process for submitting a request to exercise a right under this section;

(c) Inform the consumer of any action taken or not taken in response to the appeal, along with a written explanation of the reasons in support thereof, within sixty (60) days of receipt of an appeal. The controller shall also clearly and prominently provide the consumer with an e-mail address or other online mechanism through which the consumer may contact the Office of Consumer Protection in the Office of the Attorney General to submit a complaint.

(6) A controller that has obtained personal data about a consumer from a source other than the consumer shall be deemed in compliance with the consumer's request to delete the consumer's data pursuant to Sections 1 to 12 of this Act by:

(a) Retaining a record of the deletion request and the minimum data necessary for the purpose of ensuring the consumer's personal data remains deleted

from the controller's records and not using the retained data for any other purpose pursuant to the provisions of Sections 1 to 12 of this Act; or

(b) Opting the consumer out of the processing of personal data for any purpose except for those exempted pursuant to the provisions of Sections 1 to 12 of this Act."

➔SECTION 4. A NEW SECTION OF KRS CHAPTER 367 IS CREATED TO READ AS FOLLOWS:

(1) A controller shall:

(a) Establish, implement, and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data. Such data security practices shall be appropriate to the volume and nature of the personal data at issue; and

(b) Not process personal data in violation of state and federal laws that prohibit unlawful discrimination against consumers. A controller shall not discriminate against a consumer for exercising any of the consumer rights contained in Section 3 of this Act, including denying goods or services, charging different prices or rates for goods or services, or providing a different level of quality of goods and services to the consumer. However, nothing in this paragraph shall be construed to require a controller to provide a product or service that requires the personal data of a consumer that the controller does not collect or maintain or to prohibit a controller from offering a different price, rate, level quality, or selection of goods or services to a consumer, including offering goods or services for no fee, if the consumer has exercised his or her right to opt out pursuant to Section 3 of this Act or the offer is related to a consumer's informed, voluntary participation in a bona fide loyalty, rewards, premium features, discounts, or club card program.

(2) Any provision of a contract or agreement of any kind that purports to waive or limit in any way consumer rights pursuant to Section 3 of this Act shall be deemed contrary to public policy and shall be void and unenforceable.

(3) At or before the time that a controller collects personal data, the controller shall provide consumers with a reasonably accessible, clear, and meaningful privacy notice that includes:

(a) The categories of personal data processed by the controller;

(b) The purpose for processing personal data;

(c) One (1) or more secure and reliable means for consumers to submit a request to exercise their consumer rights under Section 3 of this Act, including how a consumer may appeal a controller's action with regard to the consumer's request. The means shall take into account the ways in which consumers normally interact with the controller, the need for secure and reliable communication of the requests, and the ability of the controller to authenticate the identity of the consumer making the request. Controllers shall not require a consumer to create a new account in order to exercise consumer rights pursuant to Section 3 of this Act, but may require a consumer to use an existing account;

(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.

(4) If a controller sells personal data to third parties or processes personal data for targeted advertising, the controller shall clearly and conspicuously disclose the processing, as well as the manner in which a consumer may exercise the right to opt out of the processing.

(5) Except as otherwise provided in KRS Chapter 367, a controller shall not process personal data for purposes that are neither reasonably necessary to nor compatible with the disclosed purposes for which the personal data is processed, as disclosed to the controller, unless the consumer obtains the consumer's consent.

(6) Except as otherwise provided in Sections 1 to 12 of this Act, a controller shall limit the collection of personal data to what is adequate, relevant, and reasonably necessary in relation to the purposes for which data is processed, as disclosed to the consumer.

(7) Except as otherwise provided in Sections 1 to 12 of this Act, a controller shall not process sensitive data concerning a consumer without obtaining the consumer's consent or, in the case of the processing of sensitive data of a child, without obtaining consent from the child's parent or lawful guardian, in accordance with the requirements set forth in the federal Children's Online Privacy Protection Act, 15 U.S.C. sec. 6501 et seq.

➔SECTION 5. A NEW SECTION OF KRS CHAPTER 367 IS CREATED TO READ AS FOLLOWS:

(1) A processor shall adhere to the instructions of a controller and shall assist the controller in meeting its obligations under Sections 1 to 12 of this Act. Such assistance shall include:

(a) Taking into account the nature of processing and the information available to the processor, by appropriate technical and organizational measures, insofar as this is reasonably practicable, to fulfill the controller's obligation to respond to consumer rights requests pursuant to Section 3 of this Act;

(b) Assisting the controller in meeting the controller's obligations in relation to the security of processing the personal data and in relation to the notification of a breach of the security of the system of the processor pursuant to KRS 365.732, or any other applicable state and federal law, in order to meet the controller's

obligations.; and

(c) Providing necessary information to enable the controller to conduct and document data protection assessments pursuant to Sections 1 to 12 of this Act.

(2) A contract between a controller and a processor shall govern the processor's data processing procedures with respect to processing performed on behalf of the controller. The contract shall be binding and shall clearly set forth instructions for processing personal data, the nature and purpose of processing, the type of data subject to processing, the duration, and the rights and obligations of both parties. The contract shall also include requirements that the processor shall:

(a) Ensure that each person processing personal data is subject to a duty of confidentiality with respect to the data;

(b) At the controller's direction, delete or return all personal data to the controller as requested at the end of the provision of services, unless retention of the personal data is required by law;

(c) Upon the reasonable request of the controller, make available to the controller information in its possession necessary to demonstrate the processor's compliance with the obligations in this section;

(d) Allow and cooperate with reasonable assessments by the controller or the controller’s designated assessor; alternatively, the processor may arrange for a qualified and independent assessor to conduct an assessment of the processor’s policies and technicial and organizational measures in support of the obligations under this chapter using an appropriate and accepted control standard or framework and assessment procedure for such assessments. The processor shall provide a report of such assessment to the controller upon request; and

(e) Engage any subcontractor pursuant to a written contract in accordance with this

subsection that requires the subcontractor to meet the obligations of the processor with respect to the personal data.

(3) 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 is to be processed. A processor that continues to adhere to a controller's instructions with respect to a specific processing of personal data remains a processor.

(4) Nothing in this section shall be construed to relieve a controller or processor from the liabilities imposed on it by virtue of its role in the processing relationship as defined in this chapter."; and

On page 24, line 3, delete in its entirety and insert in lieu thereof:

"***(b) Maintain data in identifiable form, or collect, obtain, retain, or access any data or technology in order to be capable of associating an authenticated consumer request with personal data.***"; and

On page 24, after line 19, insert the following:

"***(4) The consumer rights contained in Section 3(2)(a), (b), (c), and (d) of this Act shall not apply to pseudonymous data in cases where the controller is able to demonstrate any information necessary to identify the consumer is kept separately and is subject to effective technical and organizational controls that prevent the controller from accessing such information.***"; and

On page 28, beginning on line 20, delete the following: "***Within thirty (30) days of becoming a controller by beginning to process personal data,***"; and

On page 28, on lines 23 and 24, delete the following: "***or tracking***"; and

On page 28, on line 25, delete the following: "***or sharing***"; and

On page 29, delete lines 12 through 15 in their entirety; and

On page 29, line 16, delete "***(3)***"and insert in lieu of "***(2)***"; and

On page 29, line 25, delete "***(4)***"and insert in lieu of "***(3)***"; and

On page 29, line 25, after "***request***", delete "***in writing***" and insert the following: "***pursuant to a civil investigative demand***"; and

On page 30, line 1, delete the following: "***upon such request***"; and

On page 30, line 4 delete "***(5)***"and insert in lieu of "***(4)***"; and

On page 30, line 6, delete "***(6)***"and insert in lieu of "***(5)***"; and

On page 30, beginning on line 9, delete the following: "***, unless otherwise subject to case law regarding the applicability of the attorney-client privilege or work product protections***"; and

On page 30, line 12, delete "***(7)***"and insert in lieu of "***(6)***"; and

On page 30, line 15 delete "***(8)***"and insert in lieu of "***(7)***"; and

On page 30, line 15, after "***assessments***" delete the following: "***conducted by a controller under this section shall be updated immediately upon any material change in the nature or volume of data controlled, processed, sold, traded, or shared by the controller or, if there is no material change, annually***" and insert the following: "***shall apply processing activities created or generated after January 1, 2025, and are not retroactive***"; and

On page 30, line 21, delete "***Except as provided in Section 10 of this Act***,"; and

Beginning on page 31, lines 18 to 27, and continuing to page 32, line 1, delete in their entirety and insert in lieu thereof;

"***(6) In determining a civil penalty under this section, the court shall consider:***

(a) A controller's or processor's good-faith efforts to comply with the requirements of Sections 1 to 12 of this Act; and

(b) Whether a controller made willful or reckless omissions on the data protection impact assessment required by Section 8 of this Act, the nature of the omissions,

and the nature and volume of data."; and

On page 32, delete Section 10 in its entirety and insert in lieu thereof:

"***Nothing in Sections 1 to 12 of this Act creates the basis for an independent cause of action under Kentucky law.***".