

KENTUCKY GENERAL ASSEMBLY AMENDMENT FORM
2023 REGULAR SESSION
Unofficial Document

Amend printed copy of **SB 15/SCS 1**

On page 2, delete lines 4 through 12 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, delete lines 22 through 24 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 result 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 through 26, delete "**used to infer information about, or otherwise be associated with,**" and insert in lieu thereof "**linked to**"; and

On page 4, lines 2 through 5, delete "**, in particular by reference to an identifier such as a name, identification number, location data, online identifier, or to one (1) or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person**"; and

On page 4, line 22, after "**that**" delete "**relates to**" and insert in lieu thereof "**is linked or**

Amendment No. SFA 1

Rep. Sen. Damon Thayer

Committee Amendment _____

Signed: _____

Floor Amendment _____

LRC Drafter: _____

Adopted: _____

Date: _____

Rejected: _____

Doc. ID: XXXX

Not for Filing

Unofficial Document

reasonably linked to"; and

On page 4, line 24, delete "pseudonymous data"; and

On page 4, lines 24 through 26 delete "but does include data generated, recorded, or transmitted by a vehicle belonging to an identified or identifiable natural person"; and

On page 5, line 13, delete the second "of" and insert in lieu thereof "performed on"; and

On page 5, line 14, delete "concerning" and insert in lieu thereof "related to"; and

On page 6, lines 3 and 4, delete "or other valuable"; and

On page 6, lines 8 and 9, delete "with whom the consumer has a direct relationship"; and

On page 6, line 11, delete "a commonly branded" and insert in lieu thereof "an"; and

On page 6, line 15, after ";" insert "or"; and

On page 6, line 18, after ";" delete "or"; and

On page 6, delete lines 19 through 21 in their entirety; and

On page 6, lines 24 through 26, delete "except to the extent such data is used in order to avoid discrimination on the basis of a protected class that would violate a federal or state antidiscrimination law"; and

On page 7, line 1, delete "specific"; and

On page 7, line 2, after "a" insert "known"; and

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

On page 7, line 23, delete "(30)" and insert in lieu thereof "(29)"; and

On page 7, line 27, delete "(31)" and insert in lieu thereof "(30)"; and

On page 8, line 2, delete "across one (1) or more distinctly branded" and insert in lieu thereof "nonaffiliated"; and

On page 8, line 4, delete the second "advertising"; and

On page 8, line 5, delete "Based" and insert in lieu thereof "Advertisements based"; and

On page 8, line 8, delete "Based" and insert in lieu thereof "Advertisements based"; and

On page 8, line 9, after ";" delete "or"; and

On page 8, line 10, delete "To" and insert in lieu thereof "Advertisements directed to"; and

On page 8, line 11, after ";" insert "or"; and

On page 8, between lines 11 and 12, insert the following:

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

On page 8, line 12, delete "(32)" and insert in lieu thereof "(31)"; and

On page 8, line 8, line 14, after ";" insert "and"; and

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

On page 8, line 23, delete "(34)" and insert in lieu thereof "(32)"; and

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

On page 13, line 25, after "by" insert "or obtained about"; and

On page 13, between lines 25 and 26 insert the following:

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

On page 13, line 26, delete "(c)" and insert in lieu thereof "(d)"; and

On page 14, line 4, delete "(d)" and insert in lieu thereof "(e)"; and

On page 14, delete line 5 in its entirety and insert in lieu thereof:

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

On page 14, line 6, delete "(f)" and insert in lieu thereof "(g)"; and

On page 14, line 6, delete "or sharing"; and

On page 14, delete lines 7 through 17 in their entirety; and

On page 14, line 18, delete "(5)" and insert in lieu thereof "(3)"; and

On page 14, line 18, delete "(6)" and insert in lieu thereof "(4)"; and

On page 14, line 24, delete "fifteen (15)" and insert in lieu thereof "forty-five (45)"; and

On page 15, lines 9 through 10, after "unfounded," delete "such as when the controller reasonably believes that the primary purpose of the request is not to exercise a consumer right,"; and

On page 15, line 16, delete "(6)" and insert in lieu thereof "(4)"; and

On page 15, line 21, delete "(7)" and insert in lieu thereof "(5)"; and

On page 15, lines 26 through 27, delete "as easy to use as" and insert in lieu thereof "similar to"; and

On page 15, line 27, after ";" insert "and"; and

On page 16, delete lines 1 through 19 in their entirety and insert in lieu thereof:

"(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."; and

On page 16, between lines 19 and 20, insert the following:

"(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 such personal data for any purpose except for those exempted pursuant to the provisions of Sections 1 to 12 of this Act.**"; and

From page 16, line 20 through page 22, line 17, delete all text in its entirety and insert the following in lieu thereof:

"➔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 not 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. Such means shall take into account the ways in which consumers normally interact with the controller, the need for secure and reliable communication of such 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) Except as otherwise provided in Sections 1 to 12 of this Act, 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.

- (5) Except as otherwise provided in Section 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.
- (6) Except as otherwise provided in Section 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."; and

From page 22, line 20 through page 23, line 4, delete all text in its entirety and insert the following in lieu thereof:

- "(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 taking into account the nature of processing and the information available to the processor by:
- (a) Taking appropriate technical and organizational measures, insofar as this is reasonably practicable, to fulfill the controller's obligation to respond to the 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."; and

On page 23, line 9, delete "specific, fixed"; and

On page 23, lines 9 through 10, delete "for each type of data to be processed"; and

On page 23, line 19, delete "and"; and

On page 23, between lines 19 and 20, insert the following:

"(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 technical 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"; and

On page 23, line 20, delete "(d)" and insert in lieu thereof "(e)"; and

On page 23, after line 27, insert the following:

"(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 Sections 1 to 12 of this Act."

On page 24, line 6, delete "de-identified or pseudonymous data in an identifiable form" and insert in lieu thereof "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, between lines 22 and 23, insert the following:

"(4) The consumer rights contained in subsection (2)(a) to (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, lines 23 and 24, after "(1)" delete "Within thirty (30) days of becoming a controller by beginning to process personal data, controllers" and insert in lieu thereof "Controllers"; and

On page 28, line 26 through 27, delete "or tracking"; and

On page 29, line 1, delete "or sharing"; and

On page 29, delete lines 15 through 18 in their entirety; and

On page 29, line 19, delete "(3)" and insert in lieu thereof "(2)"; and

On page 30, line 1, delete "(4)" and insert in lieu thereof "(3)"; and

On page 30, line 1, delete "in writing" and insert in lieu thereof "pursuant to a civil investigative demand"; and

On page 30, line 4, delete "upon such request"; and

On page 30, line 7, delete "(5)" and insert in lieu thereof "(4)"; and

On page 30, line 9, delete "(6)" and insert in lieu thereof "(5)"; and

On page 30, line 10, delete "(4)" and insert in lieu thereof "(3)"; and

On page 30, lines 12 through 14 delete ", unless otherwise subject to case law regarding the applicability of the attorney-client privilege or work product protections"; and

On page 30, line 15, delete "(7)" and insert in lieu thereof "(6)"; and

On page 30, delete lines 18 through 21 in their entirety and insert the following in lieu thereof:

"(7) Data protection assessments shall apply to processing activities created or generated after January 1, 2025, and are not retroactive."; and

On page 30, line 24, delete "except as provided in Section 10 of this Act,"; and

From page 31, line 21, through page 32, line 4, delete all text in its entirety and insert the following 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 the data.**"; and

From page 32, line 9, through page 33, line 3, delete all text in its entirety and insert the following in lieu thereof:

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