GENERAL ASSEMBLY
COMMONWEALTH OF KENTUCKY

2024 REGULAR SESSION

HOUSE BILL NO. 15

AS ENACTED

Wednesday, March 27, 2024

RECEIVED AND FILED
DATE 4/4/2024
4:57p
MICHAEL G. ADAMS
SECRETARY OF STATE
COMMONWEALTH OF KENTUCKY
BY Katherine Ellis

AN ACT relating to consumer data privacy and making an appropriation therefor.

Be it enacted by the General Assembly of the Commonwealth of Kentucky:

➔SECTION 1. A NEW SECTION OF KRS CHAPTER 367 IS CREATED TO READ AS FOLLOWS:

As used in Sections 1 to 10 of this Act:

(1) "Affiliate" means a legal entity that controls, is controlled by, or is under common control with another legal entity or shares common branding with another legal entity. For the purposes of this definition, "control" or "controlled" means:

(a) Ownership of, or the power to vote, more than fifty percent (50%) of the outstanding shares of any class of voting security of a company;

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

(c) The power to exercise controlling influence over the management of a company;

(2) "Authenticate" means verifying through reasonable means that the consumer entitled to exercise his or her consumer rights in Section 3 of this Act is the same consumer exercising such consumer rights with respect to the personal data at issue;

(3) "Biometric data" means data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that are used to identify a specific individual. Biometric data does not include a physical or digital photograph, a video or audio recording or data generated therefrom, unless that data is generated to identify a specific individual or information collected, used, or stored for health care treatment, payment, or operations under HIPAA;

(4) "Business associate" has the same meaning as established in 45 C.F.R. sec. 160.103 pursuant to HIPAA;

(5) "Child" has the same meaning as in 15 U.S.C. sec. 6501;

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

(7) "Consumer" means a natural person who is a resident of the Commonwealth of Kentucky acting only in an individual context. Consumer does not include a natural person acting in a commercial or employment context;

(8) "Controller" means the natural or legal person that, alone or jointly with others, determines the purpose and means of processing personal data;

(9) "Covered entity" has the same meaning as established in 45 C.F.R. sec. 160.103 pursuant to HIPAA;

(10) "Decisions that produce legal or similarly significant effects concerning a consumer" means a decision made by a controller that results in the provision or 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 like food and water;

(11) "De-identified data" means data that cannot reasonably be linked to an identified or identifiable natural person or a device linked to a person;

(12) "Fund" means the consumer privacy fund established in Section 10 of this Act;

(13) "Health record" means a record, other than for financial or billing purposes, relating to an individual, kept by a health care provider as a result of the professional relationship established between the health care provider and the individual;

(14) "Health care provider" means:

(a) Any health facility as defined in KRS 216B.015;

(b) Any person or entity providing health care or health services, including those licensed, certified, or registered under, or subject to, KRS 194A.700 to 194A.729 or KRS Chapter 310, 311, 311A, 311B, 312, 313, 314, 314A, 315, 319, 319A, 319B, 319C, 320, 327, 333, 334A, or 335;

(c) The current and former employers, officers, directors, administrators, agents, or employees of those entities listed in paragraphs (a) and (b) of this subsection; or

(d) Any person acting within the course and scope of his or her office, employment, or agency relating to a health care provider;

(15) "HIPAA" means the federal Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191;

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

(17) "Institution of higher education" means an educational institution which:

(a) Admits as regular students only individuals having a certificate of graduation from a high school, or the recognized equivalent of such a certificate;

(b) Is legally authorized in this state to provide a program of education beyond high school;

(c) Provides an educational program for which it awards a bachelor's or higher degree, or provides a program which is acceptable for full credit toward such a degree, a program of postgraduate or postdoctoral studies, or a program of training to prepare students for gainful employment in a recognized occupation; and

(d) Is a public or other nonprofit institution;

(18) "Nonprofit organization" means any incorporated or unincorporated entity that:

(a) Is operating for religious, charitable, or educational purposes; and

(b) Does not provide net earnings to, or operate in any manner that inures to the benefit of, any officer, employee, or shareholder of the entity;

(19) "Personal data" means any information that is linked or reasonably linkable to an identified or identifiable natural person. Personal data does not include de-identified data or publicly available information;

(20) "Precise geolocation data" means information derived from technology, including but not limited to global positioning system level latitude and longitude coordinates or other mechanisms, that directly identifies the specific location of a natural person with precision and accuracy within a radius of one thousand seven hundred fifty (1,750) feet. Precise geolocation data does not include the content of communications, or any data generated by or connected to advanced utility metering infrastructure systems or equipment for use by a utility;

(21) "Process" or "processing" means any operation or set of operations performed, whether by manual or automated means, on personal data or on sets of personal data, including but not limited to the collection, use, storage, disclosure, analysis, deletion, or modification of personal data;

(22) "Processor" means a natural or legal entity that processes personal data on behalf of a controller;

(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;

(24) "Protected health information" means the same as established in 45 C.F.R. sec. 160.103 pursuant to HIPAA;

(25) "Pseudonymous data" means personal data that cannot be attributed to a specific natural person without the use of additional information, provided that the

additional information is kept separately and is subject to appropriate technical and organizational measures to ensure that the personal data is not attributed to an identified or identifiable natural person;

(26) "Publicly available information" means information that is lawfully made available through federal, state, or local government records, or information that a business has a reasonable basis to believe is lawfully made available to the general public through widely distributed media, by the consumer, or by a person to whom the consumer has disclosed the information, unless the consumer has restricted the information to a specific audience;

(27) "Sale of personal data" means the exchange of personal data for monetary consideration by the controller to a third party. Sale of personal data 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:

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

2. 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 proposed or actual merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the controller's assets;

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

(a) Personal data indicating racial or ethnic origin, religious beliefs, mental or

physical health diagnosis, sexual orientation, or citizenship or immigration status;

(b) The processing of genetic or biometric data that is processed for the purpose of uniquely identifying a specific natural person;

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

(d) Precise geolocation data;

(29) "State agency" means all departments, offices, commissions, boards, institutions, and political and corporate bodies of the state, including the offices of the clerk of the Supreme Court, clerks of the appellate courts, the several courts of the state, and the legislature, its committees, or commissions;

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

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

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

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

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

(31) "Third party" means a natural or legal person, public authority, agency, or body other than the consumer, controller, processor, or an affiliate of the processor or the controller; and

(32) "Trade secret" has the same meaning as in KRS 365.880.

➔SECTION 2. A NEW SECTION OF KRS CHAPTER 367 IS CREATED TO READ AS FOLLOWS:

(1) Sections 1 to 10 of this Act apply to persons that conduct business in the Commonwealth or produce products or services that are targeted to residents of the Commonwealth and that during a calendar year control or process personal data of at least:

(a) One hundred thousand (100,000) consumers; or

(b) Twenty-five thousand (25,000) consumers and derive over fifty percent (50%) of gross revenue from the sale of personal data.

(2) Sections 1 to 10 of this Act shall not apply to any:

(a) City, state agency, or any political subdivision of the state;

(b) Financial institutions, their affiliates, or data subject to Title V of the federal Gramm-Leach-Bliley Act, 15 U.S.C. sec. 6801 et seq.;

(c) Covered entity or business associate governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services, 45 C.F.R. pts. 160 and 164 established pursuant to HIPAA;

(d) Nonprofit organization;

(e) Institution of higher education;

(f) Organization that:

1. Does not provide net earnings to, or operate in any manner that inures to the benefit of, any officer, employee, or shareholder of the entity; and

2. Is an entity such as those recognized under KRS 304.47-060(1)(e), so long as the entity collects, processes, uses, or shares data solely in relation to identifying, investigating, or assisting:

a. Law enforcement agencies in connection with suspected

insurance-related criminal or fraudulent acts; or

b. First responders in connection with catastrophic events; or

(g) Small telephone utility as defined in KRS 278.516, a Tier III CMRS provider as defined in KRS 65.7621, or a municipally owned utility that does not sell or share personal data with any third-party processor.

(3) The following information and data are exempt from Sections 1 to 10 of this Act:

(a) Protected health information under HIPAA;

(b) Health records;

(c) Patient identifying information for purposes of 42 C.F.R. sec. 2.11;

(d) Identifiable private information for purposes of the federal policy for the protection of human subjects under 45 C.F.R. pt. 46; identifiable private information that is otherwise information collected as part of human subjects research pursuant to the good clinical practice guidelines issued by the International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use; the protection of human subjects under 21 C.F.R. pts. 50 and 56, or personal data used or shared in research conducted in accordance with the requirements set forth in Sections 1 to 10 of this Act, or other research conducted in accordance with applicable law;

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

(f) Patient safety work product for purposes of the federal Patient Safety and Quality Improvement Act, 42 U.S.C. sec. 299b-21 et seq.;

(g) Information derived from any of the health care-related information listed in this subsection that is de-identified in accordance with the requirements for de-identification pursuant to HIPAA;

(h) Information originating from, and intermingled to be indistinguishable from, or information treated in the same manner as information exempt

under this subsection that is maintained by a covered entity or business associate, or a program or qualified service organization as defined by 42 C.F.R. sec. 2.11;

(i) Information used only for public health activities and purposes as authorized by HIPAA;

(j) The collection, maintenance, disclosure, sale, communication, or use of any personal information bearing on a consumer's creditworthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living by a consumer reporting agency, furnisher, or user that provides information for use in a consumer report, and by a user of a consumer report, but only to the extent that such activity is regulated by and authorized under the federal Fair Credit Reporting Act, 15 U.S.C. sec. 1681 et seq.;

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

(l) Personal data regulated by the federal Family Educational Rights and Privacy Act, 20 U.S.C. sec. 1232g et seq.;

(m) Personal data collected, processed, sold, or disclosed in compliance with the federal Farm Credit Act, 12 U.S.C. sec. 2001 et seq.;

(n) Data processed or maintained:

1. In the course of an individual applying to, employed by, or acting as an agent or independent contractor of a controller, processor, or third party, to the extent that the data is collected and used within the context of that role;

2. As the emergency contact information of an individual used for emergency contact purposes; or

3. That is necessary to retain to administer benefits for another

individual relating to the individual under subparagraph 1. of this paragraph and used for the purposes of administering those benefits;

(o) Data processed by a utility, an affiliate of a utility, or a holding company system organized specifically for the purpose of providing goods or services to a utility as defined in KRS 278.010. For purposes of this paragraph, "holding company system" means two (2) or more affiliated persons, one (1) or more of which is a utility; and

(p) Personal data collected and used for purposes of federal policy under the Combat Methamphetamine Epidemic Act of 2005.

(4) Controllers and processors that comply with the verifiable parental consent requirements of the Children's Online Privacy Protection Act, 15 U.S.C. sec. 6501 et seq., shall be deemed compliant with any obligation to obtain parental consent under Sections 1 to 10 of this Act.

➔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 the personal data, unless the confirmation and access would require the controller to reveal a trade secret;

(b) Correct inaccuracies in the consumer's personal data, taking into account

the nature of the personal data and the purposes of processing the data;

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

(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 transmit the data to another controller without hindrance, where the processing is carried out by automated means. The controller shall not be required to reveal any trade secrets; and

(e) Opt out of the processing of personal data for purposes of targeted advertising, the sale of personal data, or profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer.

(3) Except as otherwise provided in Sections 1 to 10 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 consideration the complexity and number of the consumer's requests, so long as the controller informs the consumer of any 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 no later than forty-five (45) days after receipt of the request, of the justification for declining to take action and instructions on how to appeal the decision;

(c) Information provided in response to a consumer request shall be provided by a controller free of charge, up to twice annually per consumer. If requests from a consumer are 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;

(d) If a controller is unable to authenticate the request using commercially reasonable efforts, the controller shall not be required to comply with a request to initiate an action under subsection (1) of this section and may request that the consumer provide additional information reasonably necessary to authenticate the consumer and the consumer's request; and

(e) A controller that has obtained personal data about a consumer from a source other than the consumer shall be deemed in compliance with a consumer's request to delete such data pursuant to subsection (2)(c) of this section by:

1. 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 business' records and not using the retained data for any other purpose pursuant to the provisions of Sections 1 to 10 of this Act; or

2. Opting the consumer out of the processing of the personal data for any purpose except for those exempted pursuant to Section 2 of this Act.

(4) A controller shall establish a process for a consumer to appeal the controller's refusal to take action on a request within a reasonable period of time after the

consumer's receipt of the decision pursuant to subsection (3)(b) of this section. The appeal process shall be conspicuously available and similar to the process for submitting requests to initiate action pursuant to this section. Within sixty (60) days of receipt of an appeal, a controller shall inform the consumer in writing of any action taken or not taken in response to the appeal, including a written explanation of the reasons for the decisions. If the appeal is denied, the controller shall also provide the consumer with an online mechanism, if available, or other method through which the consumer may contact the Attorney General to submit a complaint.

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

(1) A controller shall:

(a) Limit the collection of personal data to what is adequate, relevant, and reasonably necessary in relation to the purposes for which the data is processed as disclosed to the consumer;

(b) Except as otherwise provided in this section, 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 consumer, unless the controller obtains the consumer's consent;

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

(d) 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 offer is related to a consumer's voluntary participation in a bona fide loyalty, rewards, premium features, discounts, or club card program; and

(e) Not process sensitive data concerning a consumer without obtaining the consumer's consent, or, in the case of the processing of sensitive data collected from a known child, process the data in accordance with the federal Children's Online Privacy Protection Act 15 U.S.C. sec. 6501 et seq.

(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) Controllers 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) How consumers may exercise their consumer rights pursuant to Section 3 of this Act, including how a consumer may appeal a controller's decision with regard to the consumer's request;

(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 such activity, as well as the manner in which a consumer may exercise the right to opt out of processing.

(5) A controller shall establish, and shall describe in a privacy notice, 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. The different ways to submit a request by a consumer 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.

➔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 10 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) Taking into account the nature of processing and the information available to the processor, by 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; and

(c) Providing necessary information to enable the controller to conduct and document data protection assessments pursuant to Section 6 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 of processing, 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 all information in its possession necessary to demonstrate the processor's compliance with the obligations prescribed in Sections 1 to 10 of this Act;

(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 in Sections 1 to 10 of this Act using an appropriate and accepted control standard or framework and assessment procedure for assessments. The processor shall provide a report of the assessment to the controller upon request; and

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

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

(3) 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 a processing relationship as defined by Sections 1 to 10 of this Act.

(4) 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.

➔SECTION 6. A NEW SECTION OF KRS CHAPTER 367 IS CREATED TO READ AS FOLLOWS:

(1) Controllers shall conduct and document a data protection impact assessment of each of the following processing activities involving personal data:

(a) The processing of personal data for the purposes of targeted advertising;

(b) The processing of personal data for the purposes of selling of personal data;

(c) The processing of personal data for the purposes of profiling, where the profiling presents a reasonably foreseeable risk of:

1. Unfair or deceptive treatment of consumers or disparate impact on consumers;

2. Financial, physical, or reputational injury to consumers;

3. A physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of consumers, where an intrusion would be offensive to a reasonable person; or

4. Other substantial injury to consumers;

(d) The processing of sensitive data; and

(e) Any processing of personal data that presents a heightened risk of harm to

consumers.

(2) Data protection impact assessments conducted under this section shall identify and weigh the benefits that may flow, directly and indirectly, from the processing to the controller, the consumer, other stakeholders, and the public against the potential risks to the rights of the consumer associated with such processing, as mitigated by safeguards that can be employed by the controller to reduce such risk. The use of de-identified data and the reasonable expectations of consumers, as well as the context of the processing of personal data and the relationship between the controller and the consumer whose personal data will be processed, shall be factored into this assessment by the controller.

(3) The Attorney General may request, pursuant to an investigative demand, that a controller disclose any data protection impact assessment that is relevant to an investigation conducted by the Attorney General, and the controller shall make the data protection impact assessment available to the Attorney General. The Attorney General may evaluate the data protection impact assessments for compliance with the requirements of Sections 1 to 10 of this Act.

(4) Data protection impact assessments are confidential and exempt from disclosure, public inspection, and copying under KRS 61.870 to KRS 61.884.

(5) The disclosure of a data protection impact assessment pursuant to a request from the Attorney General under subsection (3) of this section does not constitute a waiver of the attorney-client privilege or work product protection with respect to the assessment and any information contained in the assessment.

(6) A single data protection assessment may address a comparable set of processing operations that include similar activities.

(7) Data protection assessments conducted by a controller for the purpose of compliance with other laws or regulations may comply under this section if the assessments have a reasonably comparable scope and effect.

(8) Data protection assessment requirements shall apply to processing activities created or generated on or after June 1, 2026.

➔SECTION 7. A NEW SECTION OF KRS CHAPTER 367 IS CREATED TO READ AS FOLLOWS:

(1) The controller in possession of de-identified data shall:

(a) Take reasonable measures to ensure the data cannot be associated with a natural person;

(b) Publicly commit to maintaining and using de-identified data without attempting to re-identify the data; and

(c) Contractually obligate any recipients of the de-identified data to comply with all provisions of Sections 1 to 10 of this Act.

(2) Nothing in Sections 1 to 10 of this Act shall be construed to require a controller or processor to:

(a) Re-identify de-identified data or pseudonymous data; or

(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.

(3) Nothing in Sections 1 to 10 of this Act shall be construed to require a controller or processor to comply with an authenticated consumer rights request pursuant to Section 3 of this Act if:

(a) The controller is not reasonably capable of associating the request with the personal data or it would be unreasonably burdensome for the controller to associate the request with the personal data;

(b) The controller does not use the personal data to recognize or respond to the specific consumer who is the subject of the personal data, or associate the personal data with other personal data about the same specific consumer; and

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

(4) The consumer rights contained in Section 3 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 appropriate technical and organizational measures to ensure that the personal data is not attributed to an identified or identifiable natural person.

(5) A controller that discloses pseudonymous data or de-identified data shall exercise reasonable oversight to monitor compliance with any contractual commitments to which the pseudonymous data or de-identified data is subject and shall take appropriate steps to address any breaches of those contractual commitments.

➔SECTION 8. A NEW SECTION OF KRS CHAPTER 367 IS CREATED TO READ AS FOLLOWS:

(1) Nothing in Sections 1 to 10 of this Act shall be construed to restrict a controller's or processor's ability to:

(a) Comply with federal, state, or local laws or regulations;

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

(c) Cooperate with law enforcement agencies concerning conduct or 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 legal claims;

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

(f) Perform a contract to which the consumer or parent or guardian of a

known child is a party, including fulfilling the terms of a written warranty;

(g) Take steps at the request of the consumer or parent or guardian of a known child prior to entering into a contract;

(h) Take immediate steps to protect an interest that is essential for the life or physical safety of the consumer or of another natural person, and where the processing cannot be manifestly based on another legal basis;

(i) Prevent, detect, protect against, or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities, or any illegal activity; preserve the integrity or security of systems; or investigate, report, or prosecute those responsible for any such action;

(j) Engage in public or peer-reviewed scientific or statistical research in the public interest that adheres to all other applicable ethics and privacy laws and is approved, monitored, and governed by an institutional review board, or similar independent oversight entities that determine:

1. If the deletion of the information is likely to provide substantial benefits that do not exclusively accrue to the controller;

2. The expected benefits of the research outweigh the privacy risks; and

3. If the controller has implemented reasonable safeguards to mitigate privacy risks associated with research, including any risks associated with re-identification; or

(k) Assist another controller, processor, or third party with any of the obligations under this subsection.

(2) The obligations imposed on controllers or processors under Sections 1 to 10 of this Act shall not restrict a controller's or processor's ability to collect, use, or retain data to:

(a) Conduct internal research to develop, improve, or repair products, services, or technology;

(b) Effectuate a product recall;

(c) Identify and repair technical errors that impair existing or intended functionality; or

(d) Perform internal operations that are reasonably aligned with the expectations of the consumer or reasonably anticipated based on the consumer's existing relationship with the controller or are otherwise compatible with processing data in furtherance of the provision of a product or service specifically requested by a consumer or a parent or guardian of a known child or the performance of a contract to which the consumer or a parent or guardian of a known child is a party.

(3) The obligations imposed on controllers or processors under Sections 1 to 10 of this Act shall not apply to a controller or processor if compliance under Sections 1 to 10 of this Act would violate an evidentiary privilege under the laws of this Commonwealth. Nothing in Sections 1 to 10 of this Act shall be construed to prevent a controller or processor from providing personal data concerning a consumer to a person covered by an evidentiary privilege under the laws of this Commonwealth as part of a privileged communication.

(4) A controller or processor that discloses personal data to a third-party controller or processor, in compliance with the requirements of Sections 1 to 10 of this Act, is not in violation of Sections 1 to 10 of this Act if the third-party controller or processor that receives and processes such personal data is in violation of Sections 1 to 10 of this Act, provided that, at the time of disclosing the personal data, the disclosing controller or processor did not have actual knowledge that the recipient intended to commit a violation. A third-party controller or processor receiving personal data from a controller or processor in compliance with the requirements of Sections 1 to 10 of this Act is likewise not in violation of Sections 1 to 10 of this Act for the transgressions of the controller or processor from which

it receives such personal data.

(5) Nothing in Sections 1 to 10 of this Act shall be construed as an obligation imposed on controllers and processors that adversely affects the privacy or other rights or freedoms of any persons, including but not limited to the right of free speech pursuant to the First Amendment to the United States Constitution, or applies to the processing of personal data by a person in the course of a purely personal or household activity.

(6) Personal data processed by a controller pursuant to this section shall not be processed for any purpose other than those expressly listed in this section unless otherwise allowed by Sections 1 to 10 of this Act. Personal data processed by a controller pursuant to this section may be processed to the extent that such processing is:

(a) Reasonably necessary and proportionate to the purposes listed in this section; and

(b) Adequate, relevant, and limited to what is necessary in relation to the specific purposes listed in this section. Personal data collected, used, or retained pursuant to subsection (2) of this section shall, where applicable, take into account the nature and purpose or purposes of such collection, use, or retention. The data shall be subject to reasonable administrative, technical, and physical measures to protect the confidentiality, integrity, and accessibility of personal data and to reduce reasonably foreseeable risks of harm to consumers relating to the collection, use, or retention of personal data.

(7) If a controller processes personal data pursuant to an exemption in this section, the controller bears the burden of demonstrating that such processing qualifies for the exemption and complies with the requirements in this section.

(8) Processing personal data for the purposes expressly identified in subsection (1) of

this section shall not by itself make an entity a controller with respect to such processing.

➔SECTION 9. A NEW SECTION OF KRS CHAPTER 367 IS CREATED TO READ AS FOLLOWS:

(1) The Attorney General shall have exclusive authority to enforce violations of Sections 1 to 10 of this Act. The Attorney General may enforce Sections 1 to 10 of this Act by bringing an action in the name of the Commonwealth of Kentucky or on behalf of persons residing in this Commonwealth. The Attorney General shall have all powers and duties granted to the Attorney General under KRS Chapter 15 to investigate and prosecute any violation of Sections 1 to 10 of this Act. The Attorney General may demand any information, documentary material, or physical evidence from any controller or processor believed to be engaged in, or about to engage in, any violation of Sections 1 to 10 of this Act.

(2) Prior to initiating any action for violation of Sections 1 to 10 of this Act, the Attorney General shall provide a controller or processor thirty (30) days' written notice identifying the specific provisions of Sections 1 to 10 of this Act, the Attorney General alleges have been or are being violated. If within the thirty (30) days the controller or processor cures the noticed violation and provides the Attorney General an express written statement that the alleged violations have been cured and that no further violations shall occur, no action for damages under subsection (3) of this section shall be initiated against the controller or processor.

(3) If a controller or processor continues to violate Sections 1 to 10 of this Act following the cure period in subsection (2) of this section or breaches an express written statement provided to the Attorney General under subsection (2) of this section, the Attorney General may initiate an action and seek damages for up to seven thousand five hundred dollars ($7,500) for each continued violation under

Sections 1 to 10 of this Act.

(4) Nothing in Sections 1 to 10 of this Act or any other law, regulation, or the equivalent shall be construed as providing the basis for, or give rise to, a private right of action for violations of Sections 1 to 10 of this Act.

(5) The Attorney General may recover reasonable expenses incurred in investigating and preparing the case, court costs, attorney's fees, and any other relief ordered by the court of any action initiated under Sections 1 to 10 of this Act.

➔SECTION 10. A NEW SECTION OF KRS CHAPTER 367 IS CREATED TO READ AS FOLLOWS:

There is hereby created a trust and agency account to be known as the consumer privacy fund. The fund shall be administered by the Office of the Attorney General. All civil penalties collected pursuant to Sections 1 to 10 of this Act shall be deposited into the fund. Interest earned on moneys in the fund shall accrue to the fund. Moneys in the fund shall be used by the Office of the Attorney General to enforce Sections 1 to 10 of this Act. Notwithstanding KRS 45.229, any moneys remaining in the fund at the close of the fiscal year shall not lapse but shall be carried forward into the succeeding fiscal year to be used by the Office of the Attorney General for the purposes set forth in Sections 1 to 10 of this Act.

➔Section 11. This Act may be cited as the Kentucky Consumer Data Protection Act.

➔Section 12. This Act takes effect January 1, 2026.

Speaker-House of Representatives

President of Senate

Attest: _____
Chief Clerk of House of Representatives

Approved _____
Governor

Date 4/4/24