

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

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

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

5 *As used in Sections 1 to 10 of this Act:*

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

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

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

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

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

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

- 1 (4) "Business associate" has the same meaning as established in 45 C.F.R. sec.  
2 160.103 pursuant to HIPAA;
- 3 (5) "Child" has the same meaning as in 15 U.S.C. sec. 6501;
- 4 (6) "Consent" means a clear affirmative act signifying a consumer's freely given,  
5 specific, informed, and unambiguous agreement to process personal data relating  
6 to the consumer. Consent may include a written statement, written by electronic  
7 means or any other unambiguous affirmative action;
- 8 (7) "Consumer" means a natural person who is a resident of the Commonwealth of  
9 Kentucky acting only in an individual context. Consumer does not include a  
10 natural person acting in a commercial or employment context;
- 11 (8) "Controller" means the natural or legal person that, alone or jointly with others,  
12 determines the purpose and means of processing personal data;
- 13 (9) "Covered entity" has the same meaning as established in 45 C.F.R. sec. 160.103  
14 pursuant to HIPAA;
- 15 (10) "Decisions that produce legal or similarly significant effects concerning a  
16 consumer" means a decision made by a controller that results in the provision or  
17 denial by the controller of financial and lending services, housing, insurance,  
18 education enrollment, criminal justice, employment opportunities, health care  
19 services, or access to basic necessities like food and water;
- 20 (11) "De-identified data" means data that cannot reasonably be linked to an identified  
21 or identifiable natural person or a device linked to a person;
- 22 (12) "Fund" means the consumer privacy fund established in Section 10 of this Act;
- 23 (13) "Health record" means a record, other than for financial or billing purposes,  
24 relating to an individual, kept by a health care provider as a result of the  
25 professional relationship established between the health care provider and the  
26 individual;
- 27 (14) "Health care provider" means:

- 1        (a) Any health facility as defined in KRS 216B.015;
- 2        (b) Any person or entity providing health care or health services, including  
3        those licensed, certified, or registered under, or subject to, KRS 194A.700 to  
4        194A.729 or KRS Chapter 310, 311, 311A, 311B, 312, 313, 314, 314A, 315,  
5        319, 319A, 319B, 319C, 320, 327, 333, 334A, or 335;
- 6        (c) The current and former employers, officers, directors, administrators,  
7        agents, or employees of those entities listed in paragraphs (a) and (b) of this  
8        subsection; or
- 9        (d) Any person acting within the course and scope of his or her office,  
10       employment, or agency relating to a health care provider;
- 11       (15) "HIPAA" means the federal Health Insurance Portability and Accountability Act  
12       of 1996, Pub. L. No. 104-191;
- 13       (16) "Identified or identifiable natural person" means a person who can be readily  
14       identified directly or indirectly;
- 15       (17) "Institution of higher education" means an educational institution which:
- 16       (a) Admits as regular students only individuals having a certificate of  
17       graduation from a high school, or the recognized equivalent of such a  
18       certificate;
- 19       (b) Is legally authorized in this state to provide a program of education beyond  
20       high school;
- 21       (c) Provides an educational program for which it awards a bachelor's or higher  
22       degree, or provides a program which is acceptable for full credit toward  
23       such a degree, a program of postgraduate or postdoctoral studies, or a  
24       program of training to prepare students for gainful employment in a  
25       recognized occupation; and
- 26       (d) Is a public or other nonprofit institution;
- 27       (18) "Nonprofit organization" means any incorporated or unincorporated entity that:

- 1        (a) Is operating for religious, charitable, or educational purposes; and
- 2        (b) Does not provide net earnings to, or operate in any manner that inures to
- 3                the benefit of, any officer, employee, or shareholder of the entity;
- 4        (19) "Personal data" means any information that is linked or reasonably linkable to
- 5                an identified or identifiable natural person. Personal data does not include de-
- 6                identified data or publicly available information;
- 7        (20) "Precise geolocation data" means information derived from technology,
- 8                including but not limited to global positioning system level latitude and longitude
- 9                coordinates or other mechanisms, that directly identifies the specific location of a
- 10                natural person with precision and accuracy within a radius of one thousand
- 11                seven hundred fifty (1,750) feet. Precise geolocation data does not include the
- 12                content of communications, or any data generated by or connected to advanced
- 13                utility metering infrastructure systems or equipment for use by a utility;
- 14        (21) "Process" or "processing" means any operation or set of operations performed,
- 15                whether by manual or automated means, on personal data or on sets of personal
- 16                data, including but not limited to the collection, use, storage, disclosure, analysis,
- 17                deletion, or modification of personal data;
- 18        (22) "Processor" means a natural or legal entity that processes personal data on
- 19                behalf of a controller;
- 20        (23) "Profiling" means any form of automated processing performed on personal
- 21                data to evaluate, analyze, or predict personal aspects related to an identified or
- 22                identifiable natural person's economic situation, health, personal preferences,
- 23                interests, reliability, behavior, location, or movements;
- 24        (24) "Protected health information" means the same as established in 45 C.F.R. sec.
- 25                160.103 pursuant to HIPAA;
- 26        (25) "Pseudonymous data" means personal data that cannot be attributed to a specific
- 27                natural person without the use of additional information, provided that the

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

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

10 (27) "Sale of personal data" means the exchange of personal data for monetary  
11 consideration by the controller to a third party. Sale of personal data does not  
12 include:

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

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

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

18 (d) The disclosure of information that the consumer;

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

21 2. Did not restrict to a specific audience; or

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

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

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

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

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

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

6           (d) Precise geolocation data;

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

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

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

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

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

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

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

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

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

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

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

8 (b) Twenty-five thousand (25,000) consumers and derive over fifty percent  
9 (50%) of gross revenue from the sale of personal data.

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

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

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

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

18 (d) Nonprofit organization;

19 (e) Institution of higher education;

20 (f) Organization that:

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

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

27 a. Law enforcement agencies in connection with suspected

- 1                                   insurance-related criminal or fraudulent acts; or
- 2                                   b. First responders in connection with catastrophic events; or
- 3                                   (g) Small telephone utility as defined in KRS 278.516, a Tier III CMRS
- 4                                   provider as defined in KRS 65.7621, or a municipally owned utility that does
- 5                                   not sell or share personal data with any third-party processor.
- 6                                   (3) The following information and data are exempt from Sections 1 to 10 of this Act:
- 7                                   (a) Protected health information under HIPAA;
- 8                                   (b) Health records;
- 9                                   (c) Patient identifying information for purposes of 42 C.F.R. sec. 2.11;
- 10                                  (d) Identifiable private information for purposes of the federal policy for the
- 11                                  protection of human subjects under 45 C.F.R. pt. 46; identifiable private
- 12                                  information that is otherwise information collected as part of human
- 13                                  subjects research pursuant to the good clinical practice guidelines issued by
- 14                                  the International Council for Harmonisation of Technical Requirements
- 15                                  for Pharmaceuticals for Human Use; the protection of human subjects
- 16                                  under 21 C.F.R. pts. 50 and 56, or personal data used or shared in research
- 17                                  conducted in accordance with the requirements set forth in Sections 1 to 10
- 18                                  of this Act, or other research conducted in accordance with applicable law;
- 19                                  (e) Information and documents created for purposes of the federal Health Care
- 20                                  Quality Improvement Act of 1986, 42 U.S.C. sec. 11101 et seq.;
- 21                                  (f) Patient safety work product for purposes of the federal Patient Safety and
- 22                                  Quality Improvement Act, 42 U.S.C. sec. 299b-21 et seq.;
- 23                                  (g) Information derived from any of the health care-related information listed
- 24                                  in this subsection that is de-identified in accordance with the requirements
- 25                                  for de-identification pursuant to HIPAA;
- 26                                  (h) Information originating from, and intermingled to be indistinguishable
- 27                                  from, or information treated in the same manner as information exempt



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

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

6 (j) The collection, maintenance, disclosure, sale, communication, or use of any  
7 personal information bearing on a consumer's creditworthiness, credit  
8 standing, credit capacity, character, general reputation, personal  
9 characteristics, or mode of living by a consumer reporting agency,  
10 furnisher, or user that provides information for use in a consumer report,  
11 and by a user of a consumer report, but only to the extent that such activity  
12 is regulated by and authorized under the federal Fair Credit Reporting Act,  
13 15 U.S.C. sec. 1681 et seq.;

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

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

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

20 (n) Data processed or maintained:

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

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

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

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

4 (o) Data processed by a utility as defined in KRS 278.010.

5 (4) Controllers and processors that comply with the verifiable parental consent  
6 requirements of the Children's Online Privacy Protection Act, 15 U.S.C. sec.  
7 6501 et seq., shall be deemed compliant with any obligation to obtain parental  
8 consent under Sections 1 to 10 of this Act.

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

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

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

19 (a) Confirm whether or not a controller is processing the consumer's personal  
20 data and to access the personal data, unless the confirmation and access  
21 would require the controller to reveal a trade secret;

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

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

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

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

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

8 (3) Except as otherwise provided in Sections 1 to 10 of this Act, a controller shall  
9 comply with a request by a consumer to exercise the consumer rights pursuant to  
10 this section as follows:

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

19 (b) If a controller declines to take action regarding the consumer's request, the  
20 controller shall inform the consumer without undue delay, but no later than  
21 forty-five (45) days after receipt of the request, of the justification for  
22 declining to take action and instructions on how to appeal the decision;

23 (c) Information provided in response to a consumer request shall be provided  
24 by a controller free of charge, up to twice annually per consumer. If  
25 requests from a consumer are excessive, repetitive, technically infeasible, or  
26 manifestly unfounded, the controller may charge the consumer a  
27 reasonable fee to cover the administrative costs of complying with the

1           request or decline to act on the request. The controller bears the burden of  
2           demonstrating the excessive, repetitive, technically infeasible, or manifestly  
3           unfounded nature of the request;

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

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

13           1. Retaining a record of the deletion request and the minimum data  
14           necessary for the purpose of ensuring the consumer's personal data  
15           remains deleted from the business' records and not using the retained  
16           data for any other purpose pursuant to the provisions of Sections 1 to  
17           10 of this Act; or

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

21           (4) A controller shall establish a process for a consumer to appeal the controller's  
22           refusal to take action on a request within a reasonable period of time after the  
23           consumer's receipt of the decision pursuant to subsection (3)(b) of this section.  
24           The appeal process shall be conspicuously available and similar to the process for  
25           submitting requests to initiate action pursuant to this section. Within sixty (60)  
26           days of receipt of an appeal, a controller shall inform the consumer in writing of  
27           any action taken or not taken in response to the appeal, including a written

1 explanation of the reasons for the decisions. If the appeal is denied, the controller  
2 shall also provide the consumer with an online mechanism, if available, or other  
3 method through which the consumer may contact the Attorney General to submit  
4 a complaint.

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

7 (1) A controller shall:

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

11 (b) Except as otherwise provided in this section, not process personal data for  
12 purposes that are neither reasonably necessary to nor compatible with the  
13 disclosed purposes for which the personal data is processed as disclosed to  
14 the consumer, unless the controller obtains the consumer's consent;

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

19 (d) Not process personal data in violation of state and federal laws that prohibit  
20 unlawful discrimination against consumers. A controller shall not  
21 discriminate against a consumer for exercising any of the consumer rights  
22 contained in Section 3 of this Act, including denying goods or services,  
23 charging different prices or rates for goods or services, or providing a  
24 different level of quality of goods and services to the consumer. However,  
25 nothing in this paragraph shall be construed to require a controller to  
26 provide a product or service that requires the personal data of a consumer  
27 that the controller does not collect or maintain, or to prohibit a controller

- 1           from offering a different price, rate, level, quality, or selection of goods or  
2           services to a consumer, including offering goods or services for no fee, if  
3           the offer is related to a consumer's voluntary participation in a bona fide  
4           loyalty, rewards, premium features, discounts, or club card program; and  
5           (e) Not process sensitive data concerning a consumer without obtaining the  
6           consumer's consent, or, in the case of the processing of sensitive data  
7           collected from a known child, process the data in accordance with the  
8           federal Children's Online Privacy Protection Act 15 U.S.C. sec. 6501 et seq.  
9           (2) Any provision of a contract or agreement of any kind that purports to waive or  
10           limit in any way consumer rights pursuant to Section 3 of this Act shall be  
11           deemed contrary to public policy and shall be void and unenforceable.  
12           (3) Controllers shall provide consumers with a reasonably accessible, clear, and  
13           meaningful privacy notice that includes:  
14           (a) The categories of personal data processed by the controller;  
15           (b) The purpose for processing personal data;  
16           (c) How consumers may exercise their consumer rights pursuant to Section 3  
17           of this Act, including how a consumer may appeal a controller's decision  
18           with regard to the consumer's request;  
19           (d) The categories of personal data that the controller shares with third parties,  
20           if any; and  
21           (e) The categories of third parties, if any, with whom the controller shares  
22           personal data.  
23           (4) If a controller sells personal data to third parties or processes personal data for  
24           targeted advertising, the controller shall clearly and conspicuously disclose such  
25           activity, as well as the manner in which a consumer may exercise the right to opt  
26           out of processing.  
27           (5) A controller shall establish, and shall describe in a privacy notice, one (1) or

1 more secure and reliable means for consumers to submit a request to exercise  
2 their consumer rights under Section 3 of this Act. The different ways to submit a  
3 request by a consumer shall take into account the ways in which consumers  
4 normally interact with the controller, the need for secure and reliable  
5 communication of such requests, and the ability of the controller to authenticate  
6 the identity of the consumer making the request. Controllers shall not require a  
7 consumer to create a new account in order to exercise consumer rights pursuant  
8 to Section 3 of this Act but may require a consumer to use an existing account.

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

11 (1) A processor shall adhere to the instructions of a controller and shall assist the  
12 controller in meeting its obligations under Section 1 to 10 of this Act. Such  
13 assistance shall include:

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

18 (b) Taking into account the nature of processing and the information available  
19 to the processor, by assisting the controller in meeting the controller's  
20 obligations in relation to the security of processing the personal data and in  
21 relation to the notification of a breach of the security of the system of the  
22 processor pursuant to KRS 365.732; and

23 (c) Providing necessary information to enable the controller to conduct and  
24 document data protection assessments pursuant to Section 6 of this Act.

25 (2) A contract between a controller and a processor shall govern the processor's data  
26 processing procedures with respect to processing performed on behalf of the  
27 controller. The contract shall be binding and shall clearly set forth instructions

1 for processing personal data, the nature and purpose of processing, the type of  
2 data subject to processing, the duration of processing, and the rights and  
3 obligations of both parties. The contract shall also include requirements that the  
4 processor shall:

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

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

10 (c) Upon the reasonable request of the controller, make available to the  
11 controller all information in its possession necessary to demonstrate the  
12 processor's compliance with the obligations prescribed in Sections 1 to 10 of  
13 this Act;

14 (d) Allow, and cooperate with, reasonable assessments by the controller or the  
15 controller's designated assessor. Alternatively, the processor may arrange  
16 for a qualified and independent assessor to conduct an assessment of the  
17 processor's policies and technical and organizational measures in support  
18 of the obligations in Sections 1 to 10 of this Act using an appropriate and  
19 accepted control standard or framework and assessment procedure for  
20 assessments. The processor shall provide a report of the assessment to the  
21 controller upon request; and

22 (d) Engage any subcontractor pursuant to a written contract in accordance  
23 with this section that requires the subcontractor to meet the obligations of  
24 the processor with respect to the personal data.

25 (3) Nothing in this section shall be construed to relieve a controller or processor  
26 from the liabilities imposed on it by virtue of its role in a processing relationship  
27 as defined by Sections 1 to 10 of this Act.



1 (4) Determining whether a person is acting as a controller or processor with respect  
2 to a specific processing of data is a fact-based determination that depends upon  
3 the context in which personal data is to be processed. A processor that continues  
4 to adhere to a controller's instructions with respect to a specific processing of  
5 personal data remains a processor.

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

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

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

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

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

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

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

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

20 4. Other substantial injury to consumers;

21 (d) The processing of sensitive data; and

22 (e) Any processing of personal data that presents a heightened risk of harm to  
23 consumers.

24 (2) Data protection impact assessments conducted under this section shall identify  
25 and weigh the benefits that may flow, directly and indirectly, from the processing  
26 to the controller, the consumer, other stakeholders, and the public against the  
27 potential risks to the rights of the consumer associated with such processing, as

1 mitigated by safeguards that can be employed by the controller to reduce such  
2 risk. The use of de-identified data and the reasonable expectations of consumers,  
3 as well as the context of the processing of personal data and the relationship  
4 between the controller and the consumer whose personal data will be processed,  
5 shall be factored into this assessment by the controller.

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

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

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

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

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

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

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

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

- 1        (a) Take reasonable measures to ensure the data cannot be associated with a  
2                natural person;
- 3        (b) Publicly commit to maintaining and using de-identified data without  
4                attempting to re-identify the data; and
- 5        (c) Contractually obligate any recipients of the de-identified data to comply  
6                with all provisions of Sections 1 to 10 of this Act.
- 7        (2) Nothing in Sections 1 to 10 of this Act shall be construed to require a controller  
8                or processor to:
- 9                (a) Re-identify de-identified data or pseudonymous data; or  
10                (b) Maintain data in identifiable form, or collect, obtain, retain, or access any  
11                data or technology, in order to be capable of associating an authenticated  
12                consumer request with personal data.
- 13        (3) Nothing in Sections 1 to 10 of this Act shall be construed to require a controller  
14                or processor to comply with an authenticated consumer rights request pursuant to  
15                Section 3 of this Act if:
- 16                (a) The controller is not reasonably capable of associating the request with the  
17                personal data or it would be unreasonably burdensome for the controller to  
18                associate the request with the personal data;
- 19                (b) The controller does not use the personal data to recognize or respond to the  
20                specific consumer who is the subject of the personal data, or associate the  
21                personal data with other personal data about the same specific consumer;  
22                and
- 23                (c) The controller does not sell the personal data to any third party or otherwise  
24                voluntarily disclose the personal data to any third party other than a  
25                processor, except as otherwise permitted in this section.
- 26        (4) The consumer rights contained in Section 3 of this Act shall not apply to  
27                pseudonymous data in cases where the controller is able to demonstrate any

1 information necessary to identify the consumer is kept separately and is subject to  
2 appropriate technical and organizational measures to ensure that the personal  
3 data is not attributed to an identified or identifiable natural person.

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

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

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

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

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

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

19 (d) Investigate, establish, exercise, prepare for, or defend legal claims;

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

22 (f) Perform a contract to which the consumer or parent or guardian of a  
23 known child is a party, including fulfilling the terms of a written warranty;

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

26 (f) Take immediate steps to protect an interest that is essential for the life or  
27 physical safety of the consumer or of another natural person, and where the

- 1 processing cannot be manifestly based on another legal basis;
- 2 (g) Prevent, detect, protect against, or respond to security incidents, identity
- 3 theft, fraud, harassment, malicious or deceptive activities, or any illegal
- 4 activity; preserve the integrity or security of systems; or investigate, report,
- 5 or prosecute those responsible for any such action;
- 6 (h) Engage in public or peer-reviewed scientific or statistical research in the
- 7 public interest that adheres to all other applicable ethics and privacy laws
- 8 and is approved, monitored, and governed by an institutional review board,
- 9 or similar independent oversight entities that determine:
- 10 1. If the deletion of the information is likely to provide substantial
- 11 benefits that do not exclusively accrue to the controller;
- 12 2. The expected benefits of the research outweigh the privacy risks; and
- 13 3. If the controller has implemented reasonable safeguards to mitigate
- 14 privacy risks associated with research, including any risks associated
- 15 with re-identification; or
- 16 (i) Assist another controller, processor, or third party with any of the
- 17 obligations under this subsection.
- 18 (2) The obligations imposed on controllers or processors under Sections 1 to 10 of
- 19 this Act shall not restrict a controller's or processor's ability to collect, use, or
- 20 retain data to:
- 21 (a) Conduct internal research to develop, improve, or repair products, services,
- 22 or technology;
- 23 (b) Effectuate a product recall;
- 24 (c) Identify and repair technical errors that impair existing or intended
- 25 functionality; or
- 26 (d) Perform internal operations that are reasonably aligned with the
- 27 expectations of the consumer or reasonably anticipated based on the

1           consumer's existing relationship with the controller or are otherwise  
2           compatible with processing data in furtherance of the provision of a product  
3           or service specifically requested by a consumer or a parent or guardian of a  
4           known child or the performance of a contract to which the consumer or a  
5           parent or guardian of a known child is a party.

6   (3) The obligations imposed on controllers or processors under Sections 1 to 10 of  
7   this Act shall not apply to a controller or processor if compliance under Sections  
8   1 to 10 of this Act would violate an evidentiary privilege under the laws of this  
9   Commonwealth. Nothing in Sections 1 to 10 of this Act shall be construed to  
10   prevent a controller or processor from providing personal data concerning a  
11   consumer to a person covered by an evidentiary privilege under the laws of this  
12   Commonwealth as part of a privileged communication.

13   (4) A controller or processor that discloses personal data to a third-party controller  
14   or processor, in compliance with the requirements of Sections 1 to 10 of this Act,  
15   is not in violation of Sections 1 to 10 of this Act if the third-party controller or  
16   processor that receives and processes such personal data is in violation of  
17   Sections 1 to 10 of this Act, provided that, at the time of disclosing the personal  
18   data, the disclosing controller or processor did not have actual knowledge that the  
19   recipient intended to commit a violation. A third-party controller or processor  
20   receiving personal data from a controller or processor in compliance with the  
21   requirements of Sections 1 to 10 of this Act is likewise not in violation of Sections  
22   1 to 10 of this Act for the transgressions of the controller or processor from which  
23   it receives such personal data.

24   (5) Nothing in Sections 1 to 10 of this Act shall be construed as an obligation  
25   imposed on controllers and processors that adversely affects the privacy or other  
26   rights or freedoms of any persons, including but not limited to the right of free  
27   speech pursuant to the First Amendment to the United States Constitution, or

1 applies to personal data by a person in the course of a purely personal or  
2 household activity.

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

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

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

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

22 (8) Processing personal data for the purposes expressly identified in subsection (1) of  
23 this section shall not by itself make an entity a controller with respect to such  
24 processing.

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

27 (1) The Attorney General shall have exclusive authority to enforce violations of

- 1        Sections 1 to 10 of this Act. The Attorney General may enforce Sections 1 to 10 of  
2        this Act by bringing an action in the name of the Commonwealth of Kentucky or  
3        on behalf of persons residing in this Commonwealth. The Attorney General shall  
4        have all powers and duties granted to the Attorney General under KRS Chapter  
5        15 to investigate and prosecute any violation of Sections 1 to 10 of this Act. The  
6        Attorney General may demand any information, documentary material, or  
7        physical evidence from any controller or processor believed to be engaged in, or  
8        about to engage in, any violation of Sections 1 to 10 of this Act.
- 9        (2) Prior to initiating any action for violation of Sections 1 to 10 of this Act, the  
10       Attorney General shall provide a controller or processor thirty (30) days' written  
11       notice identifying the specific provisions of Sections 1 to 10 of this Act, the  
12       Attorney General alleges have been or are being violated. If within the thirty (30)  
13       days the controller or processor cures the noticed violation and provides the  
14       Attorney General an express written statement that the alleged violations have  
15       been cured and that no further violations shall occur, no action for damages  
16       under subsection (3) of this section shall be initiated against the controller or  
17       processor.
- 18       (3) If a controller or processor continues to violate Sections 1 to 10 of this Act  
19       following the cure period in subsection (2) of this section or breaches an express  
20       written statement provided to the Attorney General under subsection (2) of this  
21       section, the Attorney General may initiate an action and seek damages for up to  
22       seven thousand five hundred dollars (\$7,500) for each continued violation under  
23       Sections 1 to 10 of this Act.
- 24       (4) Nothing in Sections 1 to 10 of this Act or any other law, regulation, or the  
25       equivalent shall be construed as providing the basis for, or give rise to, a private  
26       right of action for violations of Sections 1 to 10 of this Act.
- 27       (5) The Attorney General may recover reasonable expenses incurred in investigating



1        and preparing the case, court costs, attorney's fees, and any other relief ordered  
2        by the court of any action initiated under Sections 1 to 10 of this Act.

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

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

14       ➔Section 11. This Act takes effect January 1, 2026.