

1 AN ACT relating to consumer data privacy.

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 11 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 under Section 3 of this Act is the*
18 *same consumer exercising such consumer rights with respect to the personal data*
19 *at 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, but does not include a physical or digital*
24 *photograph, a video or audio recording, or data generated therefrom, or*
25 *information collected, used, or stored for health care treatment, payment, or*
26 *operations under HIPAA;*
- 27 *(4) "Business associate" has the same meaning as established in 45 C.F.R. sec.*

- 1 160.103 pursuant to the federal Health Insurance Portability and Accountability
2 Act of 1996, Pub. L. No. 104-191;
- 3 (5) "Child" has the same meaning as in 15 U.S.C. sec. 6501;
- 4 (6) "Consent" means any freely given, specific, informed, and unambiguous
5 indication of the consumer's wishes by which the consumer signifies agreement
6 to the processing of personal data relating to the consumer for a narrowly
7 defined, particular purpose. "Consent" does not include:
- 8 (a) Acceptance of a general or broad terms of use or similar document that
9 contains descriptions of personal data processing along with other,
10 unrelated information;
- 11 (b) Hovering over, muting, pausing, or closing a given piece of content; or
- 12 (c) Agreement obtained through the use of dark patterns;
- 13 (7) "Consumer" means a natural person who is a resident of Kentucky acting only in
14 an individual or household context. "Consumer" does not include a natural
15 person acting:
- 16 (a) In a commercial or employment context; or
- 17 (b) As an independent contractor;
- 18 (8) "Controller" means a natural or legal person that, alone or jointly with others,
19 determines the purpose and means of processing personal data;
- 20 (9) "Covered entity" has the same meaning as established in 45 C.F.R. sec. 160.103
21 pursuant to HIPAA;
- 22 (10) "Dark pattern" means a user interface designed or manipulated with the
23 substantial effect of subverting or impairing consumer autonomy, decision
24 making, or choice;
- 25 (11) "De-identified data" means data that cannot reasonably be used to infer
26 information about, or otherwise be associated with, an identified or identifiable
27 natural person, or a device linked to such person, provided that the controller that

1 possesses the data:

2 (a) Takes reasonable measures to ensure that the data cannot be associated
3 with an identified or identifiable natural person, household, or device linked
4 to such person or household;

5 (b) Publicly commits to maintain and use the data only in de-identified form
6 and not attempt to re-identify the data, except as reasonably required for the
7 controller to test their methods of de-identification; and

8 (c) Contractually obligates any recipients of the de-identified data to comply
9 with Sections 1 to 11 of this Act;

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

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

15 (14) "Health care provider" means:

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

17 (b) Any person or entity providing health care or health services, including
18 those licensed, certified, or registered under, or subject to, KRS 194A.700 to
19 194A.729 or KRS Chapter 310, 311, 311A, 311B, 312, 313, 314, 314A, 315,
20 319, 319A, 319B, 319C, 320, 327, 333, 334A, or 335;

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

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

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

- 1 (16) "Identified or identifiable natural person" means a person who can be readily
2 identified directly or indirectly, in particular by reference to an identifier such as
3 a name, identification number, location data, online identifier, or to one (1) or
4 more factors specific to the physical, physiological, genetic, mental, economic,
5 cultural, or social identity of that natural person;
- 6 (17) "Institution of higher education" means an educational institution which:
7 (a) Admits as regular students only individuals having a certificate of
8 graduation from a high school, or the recognized equivalent of such a
9 certificate;
10 (b) Is legally authorized in this state to provide a program of education beyond
11 high school;
12 (c) Provides an educational program for which it awards a bachelor's or higher
13 degree, or provides a program which is acceptable for full credit toward
14 such a degree, a program of postgraduate or postdoctoral studies, or a
15 program of training to prepare students for gainful employment in a
16 recognized occupation; and
17 (d) Is a public or other nonprofit institution;
- 18 (18) "Nonprofit organization" means an incorporated or unincorporated entity that:
19 (a) Is operating for religious, charitable, or educational purposes; and
20 (b) Does not provide net earnings to, or operate in any manner that inures to
21 the benefit of, any officer, employee, or shareholder of the entity;
- 22 (19) "Personal data" means any information, including sensitive data, that relates to
23 an identified or identifiable natural person. "Personal data" does not include de-
24 identified data, pseudonymous data, or publicly available information but does
25 include data generated, recorded, or transmitted by a vehicle belonging to an
26 identified or identifiable natural person;
- 27 (20) "Precise geolocation data" means information derived from technology,

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

7 (21) "Process" or "processing" means any operation or set of operations performed,
8 whether by manual or automated means, on personal data or on sets of personal
9 data, such as the collection, use, storage, disclosure, analysis, deletion, or
10 modification of personal data;

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

13 (23) "Profiling" means any form of automated processing of personal data to
14 evaluate, analyze, or predict personal aspects concerning an identified or
15 identifiable natural person's economic situation, health, personal preferences,
16 interests, reliability, behavior, location, or movements;

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

19 (25) "Pseudonymous data" means personal data that cannot be attributed to a specific
20 natural person without the use of additional information, provided that such
21 additional information is kept separately and is subject to appropriate technical
22 and organizational measures to ensure that the personal data is not attributed to
23 an identified or identifiable natural person;

24 (26) "Publicly available information" means information that is lawfully made
25 available through federal, state, or local government records, or information that
26 a business has a reasonable basis to believe is lawfully made available to the
27 general public through widely distributed media, by the consumer, or by a person

1 to whom the consumer has disclosed the information, unless the consumer has
2 restricted the information to a specific audience;

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

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

8 (b) The disclosure of personal data to a third party with whom the consumer
9 has a direct relationship for purposes of providing a product or service
10 requested by the consumer;

11 (c) The disclosure or transfer of personal data to a commonly branded affiliate
12 of the controller;

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

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

19 (f) The disclosure or transfer of personal data to a third party solely for the
20 purposes of facilitating the consumer's exercise of his or her right to opt
21 out, as provided in Section 3 of this Act;

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

23 (a) Racial or ethnic origin, religious beliefs, mental or physical health
24 diagnosis, sexual orientation, or citizenship or immigration status, except to
25 the extent such data is used in order to avoid discrimination on the basis of
26 a protected class that would violate a federal or state antidiscrimination law;

27 (b) Genetic or biometric data that is processed for the purpose of uniquely

1 identifying a specific natural person;

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

3 (d) Precise geolocation data;

4 (29) "Sharing," "share," or "shared" means sharing, renting, releasing, disclosing,
5 disseminating, making available, transferring, or otherwise communicating
6 orally, in writing, or by electronic or other means, personal data by a controller to
7 a third party for targeted advertising or tracking, whether or not for monetary or
8 other valuable consideration, including transactions between a business and a
9 third party for targeted advertising or tracking for the benefit of the controller or
10 a third party in which no money is exchanged. "Sharing" does not include:

11 (a) The disclosure of personal data to a third party at the consumer's direction;

12 (b) The disclosure or transfer of personal data to a commonly branded affiliate
13 of the controller;

14 (c) The disclosure of information that the consumer intentionally made
15 available to the general public through a channel of mass media and did not
16 restrict to a specific audience;

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

20 (e) The disclosure or transfer of personal data to a third party solely for the
21 purposes of facilitating the consumer's exercise of his or her right to opt
22 out, as provided in Section 3 of this Act;

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

27 (31) "Targeted advertising" means displaying advertisements to a consumer where the

1 advertisement is selected based on personal data obtained from that consumer's
2 activities over time and across one (1) or more distinctly branded websites or
3 online applications to predict the consumer's preferences or interests. "Targeted
4 advertising" does not include advertising:

5 (a) Based on activities within a controller's own commonly branded websites or
6 online applications when such advertisements promote the controller's own
7 products or services;

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

10 (c) To a consumer in response to the consumer's request for information or
11 feedback;

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

15 (33) "Tracking" means combining personal data obtained from a consumer's
16 activities within a controller's own commonly branded websites or online
17 applications with personal data obtained from a third party for targeted
18 advertising. "Tracking" does not include combining personal data obtained from
19 a consumer's activities within a controller's own commonly branded websites or
20 online applications with personal data obtained from a third party solely on a
21 consumer's device such that the personal data is not permitted to leave the device
22 in a manner that permits it to be attributed to a consumer; and

23 (34) "Trade secret" means information, including but not limited to a formula,
24 pattern, compilation, program, device, method, technique, or process that:

25 (a) Derives independent economic value, actual or potential, from not being
26 generally known to, and not being readily ascertainable by proper means by,
27 other persons who can obtain economic value from its disclosure or use;

1 and
2 (b) Is the subject of efforts that are reasonable under the circumstances to
3 maintain its secrecy.

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

6 (1) Sections 1 to 11 of this Act apply to persons that conduct business in this state or
7 produce products or services that are targeted to residents of this state and that
8 during a calendar year:

9 (a) Control or process personal data of at least twenty-five thousand (25,000)
10 consumers; or

11 (b) Derive over forty percent (40%) of gross revenue from the sale of personal
12 data.

13 (2) Sections 1 to 11 of this Act shall not apply to any:

14 (a) State agency or any body, authority, board, bureau, commission, district, or
15 agency of any political subdivision of the state. However, any state agency
16 that requests, processes, or otherwise collects personal data shall:

17 1. Maintain a reasonably accessible, clear, and meaningful privacy
18 notice;

19 2. Establish, implement, and maintain reasonable administrative,
20 technical, and physical data security practices to protect the
21 confidentiality, integrity, and accessibility of the data;

22 3. Not share that data with a third party unless the data is aggregated
23 consumer information and de-identified; and

24 4. Only make a request or demand for individualized data identifying
25 individual consumers from any controller, processor, or other third
26 party in possession of such data upon a showing of probable cause
27 that the individual identified by the data has committed a criminal

1 offense or if a state agency has authority under state or federal law to
2 request or share individualized data;

3 (b) Financial institutions, their affiliates, or data subject to Title V of the
4 federal Gramm-Leach-Bliley Act, 15 U.S.C. sec. 6801 et seq., and personal
5 data collected, processed, sold, or disclosed pursuant to the federal Gramm-
6 Leach-Bliley Act, 15 Pub. L. No. 106-102 and any implementing
7 regulations;

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

12 (d) Nonprofit organization;

13 (e) Institution of higher education;

14 (f) Organization that:

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

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

21 a. Law enforcement agencies in connection with suspected
22 insurance-related criminal or fraudulent acts; or

23 b. First responders in connection with catastrophic events;

24 (g) Legal entity or its affiliate conducting research in accordance with the
25 federal policy for the protection of human subjects under 45 C.F.R. pt. 46,
26 the good clinical practice guidelines issued by the International Council for
27 Harmonisation of Technical Requirements for Pharmaceuticals for Human

- 1 Use, or the United States Food and Drug Administration protection of
2 human subjects under 21 C.F.R. pts. 50 and 56;
- 3 (h) National securities association, registered under Section 15A of the
4 Securities Exchange Act of 1934, 15 U.S.C. sec. 78o-3, as amended, or
5 regulations adopted thereunder; or
- 6 (i) Small telephone utility as defined in KRS 278.516, a Tier III CMRS
7 provider as defined in KRS 65.7621, or a municipally owned utility that does
8 not sell or share personal data with any third-party processor.
- 9 (3) The following information and data are exempt from Sections 1 to 11 of this Act:
- 10 (a) Protected health information;
- 11 (b) Health records;
- 12 (c) Patient identifying information for purposes of 42 C.F.R. sec. 2.11;
- 13 (d) Identifiable private information for purposes of the federal policy for the
14 protection of human subjects under 45 C.F.R. pt. 46; identifiable private
15 information that is otherwise information collected as part of human
16 subjects research pursuant to the good clinical practice guidelines issued by
17 the International Council for Harmonisation of Technical Requirements
18 for Pharmaceuticals for Human Use; the protection of human subjects
19 under 21 C.F.R. pts. 50 and 56, or personal data used or shared in research
20 conducted in accordance with the requirements set forth in Sections 1 to 11
21 of this Act, or other research conducted in accordance with applicable law;
- 22 (e) Information and documents created for purposes of the federal Health Care
23 Quality Improvement Act of 1986, 42 U.S.C. sec. 11101 et seq.;
- 24 (f) Patient safety work product for purposes of the federal Patient Safety and
25 Quality Improvement Act, 42 U.S.C. sec. 299b-21 et seq.;
- 26 (g) Information derived from any of the health care-related information listed
27 in this subsection that is de-identified in accordance with the requirements

- 1 for de-identification pursuant to HIPAA;
- 2 (h) Information originating from, and intermingled to be indistinguishable
3 from, or information treated in the same manner as information exempt
4 under this subsection that is maintained by a covered entity or business
5 associate as defined by HIPAA or a program or a qualified service
6 organization as defined by 42 C.F.R. sec. 2.11;
- 7 (i) Information used only for public health activities and purposes as
8 authorized by HIPAA;
- 9 (j) The collection, maintenance, disclosure, sale, communication, or use of any
10 personal information bearing on a consumer's creditworthiness, credit
11 standing, credit capacity, character, general reputation, personal
12 characteristics, or mode of living by a consumer reporting agency,
13 furnisher, or user that provides information for use in a consumer report,
14 and by a user of a consumer report, but only to the extent that such activity
15 is regulated by and authorized under the federal Fair Credit Reporting Act,
16 15 U.S.C. sec. 1681 et seq.;
- 17 (k) Personal data collected, processed, sold, or disclosed in compliance with the
18 federal Driver's Privacy Protection Act of 1994, 18 U.S.C. sec. 2721 et seq.;
- 19 (l) Personal data regulated by the federal Family Educational Rights and
20 Privacy Act, 20 U.S.C. sec. 1232g et seq.;
- 21 (m) Personal data collected, processed, sold, or disclosed in compliance with the
22 federal Farm Credit Act, 12 U.S.C. sec. 2001 et seq.;
- 23 (n) Data processed or maintained:
- 24 1. As the emergency contact information of an individual used for
25 emergency contact purposes;
- 26 2. That is necessary to retain to administer benefits for another
27 individual relating to the individual under subparagraph 1. of this

1 paragraph and used for the purposes of administering those benefits;

2 or

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

6 in connection with the gathering, dissemination, or reporting of news or
 7 information to the public by news media;

8 (o) Data processed by a utility as defined by KRS 278.010(3); and

9 (p) Information held by a prescription drug monitoring program.

10 (4) Controllers and processors that comply with the verifiable parental consent
 11 requirements of the federal Children's Online Privacy Protection Act, 15 U.S.C.
 12 sec. 6501 et seq., shall be deemed compliant with any obligation to obtain
 13 parental consent under Sections 1 to 11 of this Act.

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

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

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

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

26 (b) Delete personal data provided by the consumer;

27 (c) Obtain a copy of the consumer's personal data that the consumer previously

1 provided to the controller in a portable and, to the extent technically
2 practicable, readily usable format that allows the consumer to read or
3 transmit the data to another controller without hindrance, where the
4 processing is carried out by automated means;

5 (d) Opt out of targeted advertising;

6 (e) Opt out of tracking; and

7 (f) Opt out of the sale or sharing of personal data.

8 (3) A consumer may exercise his or her right to opt out of the selling or sharing of
9 his or her personal data via user-enabled global privacy controls, such as a
10 browser plug-in or privacy setting, device setting, or other mechanism, that
11 communicates or signals the consumer's choice to opt out, and a controller shall
12 comply with such an opt out request.

13 (4) A consumer may authorize another person, acting on the consumer's behalf, to
14 exercise any of the rights set forth in this section. A controller shall comply with a
15 request to exercise a right received from a person authorized to act on a
16 consumer's behalf if the controller is able to authenticate, with commercially
17 reasonable efforts, the identity of the consumer and the authorized agent's
18 authority to act on his or her behalf.

19 (5) Except as otherwise provided in subsection (6) of this section and Sections 6 and
20 7 of this Act, a controller shall comply with a request by a consumer to exercise
21 the consumer rights pursuant to this section as follows:

22 (a) A controller shall respond to the consumer without undue delay, but in all
23 cases within forty-five (45) days of receipt of the request submitted pursuant
24 to the methods described in this section. The response period may be
25 extended once by fifteen (15) additional days when reasonably necessary,
26 taking into account the complexity and number of the consumer's requests,
27 so long as the controller informs the consumer of any such extension within

1 the initial forty-five (45) day response period, together with the reason for
2 the extension;

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

7 (c) Information provided in response to a consumer request shall be provided
8 by a controller free of charge, at least twice annually per consumer. If a
9 request from a consumer is excessive, repetitive, technically infeasible, or
10 manifestly unfounded, such as when the controller reasonably believes that
11 the primary purpose of the request is not to exercise a consumer right, the
12 controller may charge the consumer a reasonable fee to cover the
13 administrative costs of complying with the request or decline to act on the
14 request. The controller bears the burden of demonstrating the excessive,
15 repetitive, technically infeasible, or manifestly unfounded nature of the
16 request.

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

22 (7) A controller shall:

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

27 (b) Ensure that the appeal process is conspicuously available and as easy to use

- 1 as the process for submitting a request to exercise a right under this section;
2 (c) Inform the consumer of any action taken or not taken in response to the
3 appeal, along with a written explanation of the reasons in support thereof,
4 within thirty (30) days of receipt of an appeal. That period may be extended
5 by sixty (60) additional days where reasonably necessary, taking into
6 account the complexity and number of the requests serving as the basis for
7 the appeal. The controller shall inform the consumer of such an extension
8 within thirty (30) days of receipt of the appeal, together with the reasons for
9 the delay. The controller shall also provide the consumer with an e-mail
10 address or other online mechanism through which the consumer may
11 submit the appeal, along with any action taken or not taken by the
12 controller in response to the appeal and the controller's written explanation
13 of the reasons in support thereof, to the Attorney General; and
14 (d) When informing a consumer of any action taken or not taken in response to
15 an appeal pursuant to this subsection, clearly and prominently provide the
16 consumer with information about how to file a complaint with the Office of
17 Consumer Protection in the Office of the Attorney General. The controller
18 shall maintain records of all such appeals and how it responded to them for
19 at least twenty-four (24) months and shall, upon request, compile and
20 provide a copy of such records to the Attorney General.

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

23 (1) A controller shall:

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

1 (b) Not process personal data in violation of state and federal laws that prohibit
2 unlawful discrimination against consumers. A controller shall not
3 discriminate against a consumer for exercising any of the consumer rights
4 contained in Section 3 of this Act, including denying goods or services,
5 charging different prices or rates for goods or services, or providing a
6 different level of quality of goods and services to the consumer. However,
7 nothing in this paragraph shall be construed to require a controller to
8 provide a product or service that requires the personal data of a consumer
9 that the controller does not collect or maintain if the consumer has
10 exercised his or her right to opt out pursuant to Section 3 of this Act or the
11 offer is related to a consumer's informed, voluntary participation in a bona
12 fide loyalty, rewards, premium features, discounts, or club card program;

13 (c) Upon a request made by the Office of the Attorney General pursuant to any
14 investigation or action taken under Section 8 of this Act, provide the
15 Attorney General with the specific third parties, if any, with whom the
16 controller shares or sells personal data relevant to the Attorney General's
17 investigation or action, including:

18 1. Each location, whether domestic or international, at which each third
19 party retains the data;

20 2. The length of time each third party retains the data; and

21 3. The use or uses to which the data is put by each third party; and

22 (d) Provide an annual report to the Attorney General. The report shall include:

23 1. The categories of personal data processed by the controller in the
24 preceding quarter;

25 2. The amount of personal data in each category, identified by specific
26 instances of collection in the preceding quarter; and

27 3. The number of identifiable consumers whose personal data the

1 controller processed in the preceding quarter.

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

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

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

9 (b) The purpose for processing personal data;

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

20 (d) The specific types of personal data that the controller shares with, or sells
21 to, third parties, if any;

22 (e) The categories of third parties, if any, with whom the controller shares or
23 sells personal data, including:

24 1. Each location, whether domestic or international, at which each third
25 party retains the data;

26 2. The length of time each third party retains the data; and

27 3. The use or uses to which the data is put by each third party;

- 1 (f) The name and contact information of the controller;
- 2 (g) The purposes for which personal data are processed, as well as the basis for
- 3 processing as provided in subsection (6) of this section; and
- 4 (h) The estimated period of time for which the controller will retain the
- 5 consumer's personal data or, if this is not known, the criteria that the
- 6 controller will use in determining that period of time.
- 7 (4) If a controller sells or shares personal data to third parties or processes personal
- 8 data for targeted advertising or tracking, the controller shall clearly and
- 9 conspicuously disclose the processing, as well as the manner in which a
- 10 consumer may exercise the right to opt out of the processing.
- 11 (5) Controllers shall ensure that any privacy notices or disclosures required under
- 12 this section:
- 13 (a) Use clear and plain language;
- 14 (b) Are provided in English and any other language in which the controller
- 15 communicates with the consumer to whom the information pertains;
- 16 (c) Are understandable to the least sophisticated consumer; and
- 17 (d) Provide an explanation of how the consumer's data will be used by the
- 18 controller.
- 19 (6) Controllers shall not process the personal data of a consumer unless at least one
- 20 (1) of the following conditions applies:
- 21 (a) The controller is able to demonstrate that the consumer's personal data is
- 22 being processed for:
- 23 1. One (1) or more specific purposes; and
- 24 2. The controller does not require the consumer to provide consent as a
- 25 condition of using the controller's product or service, unless
- 26 processing the consumer's personal data is required to provide the
- 27 product or service to the consumer;

- 1 (b) The processing is necessary to perform a contract to which the consumer is
2 a party or in order to take steps at the request of the consumer prior to
3 entering into a contract;
- 4 (c) The processing is necessary for the controller to comply with a legal
5 obligation to which it is subject;
- 6 (d) The processing is necessary to protect the vital interests of the consumer or
7 another natural person, and the processing cannot be manifestly based on
8 another legal basis;
- 9 (e) The processing is necessary to perform a task carried out in the public
10 interest or to exercise official authority vested in the controller; or
- 11 (f) The processing is necessary for the purposes of the legitimate interests
12 pursued by the controller or by a third party, except where such legitimate
13 interests are overridden by the fundamental privacy interests of the
14 consumer, in particular when processing the personal data of a child.
- 15 (7) A controller's collection of personal data shall be limited to what is reasonably
16 necessary in relation to the purposes for which the personal data is processed.
- 17 (8) A controller shall store or otherwise retain personal data such that it can be
18 attributed to a consumer for no longer than is necessary for the purposes for
19 which the personal data are processed.
- 20 (9) Except as provided in Sections 1 to 11 of this Act, a controller shall collect and
21 process personal data only for specified and legitimate purposes, and a controller
22 may not further process personal data in a manner that is not reasonably
23 necessary to or compatible with those purposes, unless the controller obtains the
24 consumer's consent and such consent meets the conditions set forth in subsection
25 (6)(a) of this section.
- 26 (10) A controller shall not process personal data on the basis of a consumer's or a
27 class of consumers' actual or perceived race, color, ethnicity, religion, national

1 origin, sex, gender, gender identity, sexual orientation, family status, lawful
2 source of income, or disability, in a manner that unlawfully discriminates against
3 the consumer or class of consumers with respect to the offering or provision of:

4 (a) Housing;

5 (b) Employment;

6 (c) Credit;

7 (d) Education; or

8 (e) The goods, services, facilities, privileges, advantages, or accommodations of
9 any place of public accommodation.

10 (11) If a consumer exercises his or her right to opt out pursuant to Section 3 of this
11 Act, a controller shall not sell or share personal data to a third party as part of a
12 bona fide loyalty, rewards, premium features, discounts, or club card program in
13 which the consumer voluntarily participates unless:

14 (a) The sale or sharing of personal data to third parties is reasonably necessary
15 to enable the third party to provide a benefit to which the consumer is
16 entitled as part of such program;

17 (b) The sale or sharing of personal data to third parties is clearly disclosed in
18 the program's terms;

19 (c) The third party uses the personal data only for purposes of facilitating such
20 a benefit to which the consumer is entitled as part of such program; and

21 (d) The third party does not retain or use, transfer, or disclose the personal data
22 for any other purpose.

23 (12) Except as otherwise provided in Sections 1 to 11 of this Act, a controller shall not
24 process sensitive data concerning a consumer without allowing the consumer to
25 opt out pursuant to Sections 1 to 11 of this Act, or in the case of the processing of
26 sensitive data of a child, without obtaining consent from the child's parent or
27 lawful guardian, in accordance with the requirements set forth in the federal

1 *Children's Online Privacy Protection Act, 15 U.S.C. sec. 6501 et seq.*

2 *(13) Except as otherwise provided in Sections 1 to 11 of this Act, a controller shall not*
3 *process the personal data of a child for the purposes of targeted advertising or*
4 *tracking.*

5 *(14) Except as otherwise provided in Sections 1 to 11 of this Act, a controller shall not*
6 *process the personal data of a consumer that is not a child and is younger than*
7 *eighteen (18) years old for the purposes of targeted advertising or tracking or the*
8 *sale or sharing of personal data without obtaining consent from such consumer*
9 *pursuant to subsection (6)(a) of this section.*

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

12 *(1) A processor shall adhere to the instructions of a controller and shall assist the*
13 *controller in meeting its obligations under Sections 1 to 11 of this Act. Such*
14 *assistance shall include taking into account the nature of processing and the*
15 *information available to the processor, by:*

16 *(a) Taking appropriate technical and organizational measures, insofar as this*
17 *is reasonably practicable, to fulfill the controller's obligation to respond to*
18 *consumer rights requests pursuant to Section 3 of this Act; and*

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

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

1 data subject to processing, the specific, fixed duration of processing for each type
 2 of data to be processed, and the rights and obligations of both parties. The
 3 contract shall also include requirements that the processor shall:

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

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

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

12 (d) Engage any subcontractor pursuant to a written contract in accordance
 13 with this subsection that requires the subcontractor to meet the obligations
 14 of the processor with respect to the personal data.

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

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

22 (1) Nothing in Sections 1 to 11 of this Act shall be construed to require a controller
 23 or processor to:

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

25 (b) Maintain de-identified or pseudonymous data in an identifiable form.

26 (2) Nothing in Sections 1 to 11 of this Act shall be construed to require a controller
 27 or processor to comply with an authenticated consumer rights request, pursuant

1 to Section 3 of this Act, if all of the following are true:

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

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

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

12 (3) A controller that discloses pseudonymous data or de-identified data shall exercise
13 reasonable oversight to monitor compliance with any contractual commitments to
14 which the pseudonymous data or de-identified data is subject.

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

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

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

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

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

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

27 (e) Provide a product or service specifically requested by a consumer or a

- 1 parent or guardian of a child, perform a contract to which the consumer or
2 parent or guardian of a child is a party, including fulfilling the terms of a
3 written warranty, or take steps at the request of the consumer or parent or
4 guardian of a child prior to entering into a contract;
- 5 (f) Take immediate steps to protect an interest that is essential for the life or
6 physical safety of the consumer or of another natural person, and where the
7 processing cannot be manifestly based on another legal basis;
- 8 (g) Prevent, detect, protect against, or respond to security incidents, identity
9 theft, fraud, harassment, malicious or deceptive activities, or any illegal
10 activity; preserve the integrity or security of systems; or investigate, report,
11 or prosecute those responsible for any such action;
- 12 (h) Engage in public or peer-reviewed scientific or statistical research in the
13 public interest that adheres to all other applicable ethics and privacy laws
14 and is approved, monitored, and governed by an institutional review board,
15 or similar independent oversight entities that determine:
- 16 1. If the information is likely to provide substantial benefits that do not
17 exclusively accrue to the controller;
- 18 2. The expected benefits of the research outweigh the privacy risks; and
- 19 3. If the controller has implemented reasonable safeguards to mitigate
20 privacy risks associated with research, including any risks associated
21 with re-identification; or
- 22 (i) Assist another controller, processor, or third party with any of the
23 obligations under this subsection.
- 24 (2) The obligations imposed on controllers or processors under Sections 1 to 11 of
25 this Act shall not restrict a controller's or processor's ability to collect, use, or
26 retain data to:
- 27 (a) Conduct internal research to develop, improve, or repair products, services,

- 1 or technology;
- 2 (b) Effect a product recall, if the data is retained and processed solely for that
- 3 purpose;
- 4 (c) Identify and repair technical errors that impair existing or intended
- 5 functionality; or
- 6 (d) Perform solely internal operations that are reasonably aligned and
- 7 compatible with the purposes of processing as disclosed to the consumer
- 8 and with the expectations of the consumer based on such purposes, or are
- 9 otherwise compatible with processing in furtherance of the provision of a
- 10 product or service specifically requested by the consumer or the
- 11 performance of a contract to which the consumer is a party when those
- 12 internal operations are performed during, and not following, the
- 13 consumer's relationship with the controller.
- 14 (3) The obligations imposed on controllers or processors under Sections 1 to 11 of
- 15 this Act shall not apply where compliance by the controller or processor with
- 16 Sections 1 to 11 of this Act would violate an evidentiary privilege under the laws
- 17 of this Commonwealth. Nothing in Sections 1 to 11 of this Act shall be construed
- 18 to prevent a controller or processor from providing personal data concerning a
- 19 consumer to a person covered by an evidentiary privilege under the laws of this
- 20 Commonwealth as part of a privileged communication.
- 21 (4) Nothing in Sections 1 to 11 of this Act shall be construed as an obligation
- 22 imposed on controllers and processors that:
- 23 (a) Adversely affects the privacy or other rights or freedoms of any persons,
- 24 such as exercising the right of free speech pursuant to the First Amendment
- 25 to the United States Constitution; or
- 26 (b) Applies to personal data by a person in the course of a purely personal or
- 27 household activity.

- 1 (5) Personal data processed by a controller pursuant to this section shall not be
2 processed for any purpose other than those expressly listed in this section unless
3 otherwise allowed by Sections 1 to 11 of this Act.
- 4 (6) Personal data processed by a controller pursuant to this section may be processed
5 solely to the extent that such processing is:
- 6 (a) Reasonably necessary and proportionate to the purposes listed in this
7 section;
- 8 (b) Adequate, relevant, and limited to what is necessary in relation to the
9 specific purposes listed in this section; and
- 10 (c) Insofar as possible, taking into account the nature and purpose of
11 processing the personal data, subjected to reasonable administrative,
12 technical, and physical measures to protect the confidentiality, integrity,
13 and accessibility of the personal data and to reduce reasonably foreseeable
14 risks of harm to consumers.
- 15 (7) If a controller processes personal data pursuant to an exemption in this section,
16 the controller bears the burden of demonstrating that such processing qualifies
17 for the exemption and complies with the requirements in this section.
- 18 (8) Processing personal data for the purposes expressly identified in subsection (1) of
19 this section shall not by itself make an entity a controller with respect to such
20 processing.
- 21 (9) Nothing in Sections 1 to 11 of this Act shall require a controller, processor, third
22 party, or consumer to disclose trade secrets.
- 23 (10) A controller or processor that discloses personal data to a third party controller or
24 processor, in compliance with the requirements of Sections 1 to 11 of this Act,
25 shall not be in violation of Sections 1 to 11 of this Act if the third party controller
26 or processor that receives and processes such personal data is in violation of
27 Sections 1 to 11 of this Act, provided that, at the time of disclosing the personal

1 data, the disclosing controller or processor did not have actual knowledge that the
2 recipient intended to commit a violation.

3 (11) A third party controller or processor that receives personal data from a controller
4 or processor, in compliance with the requirements of Sections 1 to 11 of this Act,
5 is not in violation of Sections 1 to 11 of this Act if the controller or processor that
6 discloses such personal data is in violation of Sections 1 to 11 of this Act,
7 provided that, at the time of receiving the personal data, the receiving controller
8 or processor did not have actual knowledge that the disclosing controller or
9 processor intended to commit a violation.

10 (12) Nothing in Sections 1 to 11 of this Act shall be construed as requiring a
11 controller or processor to identify de-identified data in response to a consumer
12 request made under Section 3 of this Act.

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

15 (1) The Attorney General shall have exclusive authority to enforce the provisions of
16 Sections 1 to 11 of this Act.

17 (2) The Attorney General may enforce Sections 1 to 11 of this Act by bringing an
18 action in the name of the Commonwealth, or on behalf of persons residing in the
19 Commonwealth. The Attorney General may issue a civil investigative demand to
20 any controller or processor believed to be engaged in, or about to engage in, any
21 violation of Sections 1 to 11 of this Act. The provisions of KRS 367.240 shall
22 apply to civil investigative demands issued under this section.

23 (3) Prior to initiating any action under Sections 1 to 11 of this Act, the Attorney
24 General shall provide a controller or processor thirty (30) days' written notice
25 identifying the specific provisions of Sections 1 to 11 of this Act the Attorney
26 General, on behalf of a consumer, alleges have been or are being violated. If
27 within the thirty (30) days the controller or processor cures the noticed violation

1 and provides the Attorney General an express written statement that the alleged
2 violations have been cured and that no further violations shall occur, no action
3 for damages shall be initiated against the controller or processor.

4 (4) If a controller or processor does not cure a violation under subsection (3) of this
5 section or violates Sections 1 to 11 of this Act in breach of an express written
6 statement provided to the Attorney General under this section, the Attorney
7 General may initiate an action and seek damages for up to seven thousand five
8 hundred dollars (\$7,500) for each violation under Sections 1 to 11 of this Act.

9 (5) The Attorney General may recover reasonable expenses incurred in investigating
10 and preparing the case, including attorneys' fees, of any action initiated under
11 Sections 1 to 11 of this Act.

12 (6) In determining a civil penalty under this section, the court shall consider a
13 controller's or processor's good-faith efforts to comply with the requirements of
14 Sections 1 to 11 of this Act.

15 (7) Proceeds from the civil penalties imposed under this section shall be deposited
16 into the consumer privacy fund created in Section 10 of this Act.

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

19 (1) Except for those actions brought by the Attorney General to enforce Sections 1 to
20 11 of this Act, nothing in Sections 1 to 11 of this Act creates an independent
21 cause of action.

22 (2) No person, except for the Attorney General, may enforce the rights and
23 protections created by Sections 1 to 11 of this Act in any action. However,
24 nothing in Sections 1 to 11 of this Act shall limit any other independent causes of
25 action enjoyed by any person, including any constitutional, statutory,
26 administrative, or common law rights or causes of action. The rights and
27 protections in Sections 1 to 11 of this Act are not exclusive, and to the extent that

1 *a person has the rights and protections in this chapter because of another law*
2 *other than Sections 1 to 11 of this Act, the person continues to have those rights*
3 *and protections notwithstanding the existence of Sections 1 to 11 of this Act.*

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

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

15 ➔SECTION 11. A NEW SECTION OF KRS CHAPTER 367 IS CREATED TO
16 READ AS FOLLOWS:

17 *(1) Sections 1 to 11 of this Act is a matter of statewide concern and supersedes and*
18 *preempts all rules, regulations, codes, ordinances, and other laws adopted by a*
19 *city, county, charter county, urban-county government, consolidated local*
20 *government, unified local government, municipality, or local agency regarding*
21 *the processing of personal data by controllers or processors.*

22 *(2) Any reference to federal, state, or local law or statute in Sections 1 to 11 of this*
23 *Act shall be deemed to include any accompanying rules or regulations or*
24 *exemptions thereto.*

25 ➔Section 12. KRS 367.240 is amended to read as follows:

26 (1) When the Attorney General has reason to believe that a person has engaged in, is
27 engaging in, or is about to engage in any act or practice declared to be unlawful by

1 KRS 367.110 to 367.300 or Sections 1 to 11 of this Act, or when he or she believes
2 it to be in the public interest that an investigation should be made to ascertain
3 whether a person in fact has engaged in, is engaging in or is about to engage in, any
4 act or practice declared to be unlawful by KRS 367.110 to 367.300 or Sections 1 to
5 11 of this Act, he or she may execute in writing and cause to be served upon any
6 person who is believed to have information, documentary material or physical
7 evidence relevant to the alleged or suspected violation, an investigative demand
8 requiring such person to furnish, under oath or otherwise, a report in writing setting
9 forth the relevant facts and circumstances of which he or she has knowledge, or to
10 appear and testify or to produce relevant documentary material or physical evidence
11 for examination, at such reasonable time and place as may be stated in the
12 investigative demand, concerning the advertisement, sale or offering for sale of any
13 goods or services or the conduct of any trade or commerce that is the subject matter
14 of the investigation. Provided however, that no person who has a place of business
15 in Kentucky shall be required to appear or present documentary material or physical
16 evidence outside of the county where he or she has his or her principal place of
17 business within the Commonwealth.

18 (2) At any time before the return date specified in an investigative demand, or within
19 twenty (20) days after the demand has been served, whichever period is shorter, a
20 petition to extend the return date, or to modify or set aside the demand, stating good
21 cause, may be filed in the Circuit Court where the person served with the demand
22 resides or has his or her principal place of business or in the Franklin Circuit Court.

23 ➔Section 13. This Act may be cited as the Kentucky Consumer Data Protection
24 Act.

25 ➔Section 14. This Act takes effect on January 1, 2025.