AN ACT relating to consumer data privacy.

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

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

As used in Sections 1 to 10 of this Act:

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

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

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

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

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

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

(4) "Business associate" has the same meaning as established in 45 C.F.R. sec.

160.103 pursuant to HIPAA;

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

(6) "Consent" means any freely given, specific, informed, and unambiguous indication of the consumer's wishes by which the consumer signifies agreement to the processing of personal data relating to the consumer for a narrowly defined, particular purpose. "Consent" does not include:

(a) Acceptance of a general or broad terms of use or similar document that contains descriptions of personal data processing along with other, unrelated information;

(b) Hovering over, muting, pausing, or closing a given piece of content; or

(c) Agreement obtained through the use of dark patterns;

(7) "Consumer" means a natural person who is a resident of Kentucky acting only in an individual or household context. "Consumer" does not include a natural person acting:

(a) In a commercial or employment context; or

(b) As an independent contractor;

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

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

(10) "Dark pattern" means a user interface designed or manipulated with the substantial effect of subverting or impairing consumer autonomy, decision making, or choice;

(11) "De-identified data" means data that cannot reasonably be used to infer information about, or otherwise be associated with, an identified or identifiable natural person, or a device linked to that person, provided that the controller that possesses the data:

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

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

(c) Contractually obligates any recipients of the de-identified data to comply with Sections 1 to 10 of this Act;

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

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

(14) "Health care provider" means:

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

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

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

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

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

(16) "Identified or identifiable natural person" means a person who can be readily

identified directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, online identifier, or to one (1) or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person;

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

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

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

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

(d) Is a public or other nonprofit organization;

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

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

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

(19) "Personal data" means any information, including sensitive data, that relates to an identified or identifiable natural person. "Personal data" does not include de-identified data, pseudonymous data, or publicly available information but does include data generated, recorded, or transmitted by a vehicle belonging to an identified or identifiable natural person;

(20) "Precise geolocation data" means information derived from technology, including but not limited to global positioning system level latitude and longitude coordinates or other mechanisms, that directly identifies the specific location of a

natural person with precision and accuracy within a radius of one thousand seven hundred fifty (1,750) feet, but does not include the content of communications or any data generated by or connected to advanced utility metering infrastructure systems or equipment for use by a utility;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(d) Precise geolocation data;

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

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

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

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

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

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

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

(31) "Targeted advertising" means displaying advertisements to a consumer where the advertisement is selected based on personal data obtained from that consumer's activities over time and across one (1) or more distinctly branded websites or online applications to predict the consumer's preferences or interests. "Targeted

advertising" does not include advertising:

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

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

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

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

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

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

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

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

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

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

(a) Fifty thousand (50,000) consumers; or

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

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

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

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

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

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

4. Only make a request or demand for individualized data identifying individual consumers from any controller, processor, or other third party in possession of the data upon a showing of probable cause that the individual identified by the data has committed a criminal offense or if a state agency has authority under state or federal law to request or share individualized data;

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

data collected, processed, sold, or disclosed pursuant to the federal Gramm-Leach-Bliley Act, 15 Pub. L. No. 106-102 and any implementing regulations;

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

(d) Nonprofit organization;

(e) Institution of higher education;

(f) Organization that:

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

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

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

b. First responders in connection with catastrophic events;

(g) Legal entity or its affiliate conducting research in accordance with the federal policy for the protection of human subjects under 45 C.F.R. pt. 46, the good clinical practice guidelines issued by the International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use, or the United States Food and Drug Administration protection of human subjects under 21 C.F.R. pts. 50 and 56;

(h) National securities association, registered under Section 15A of the Securities Exchange Act of 1934, 15 U.S.C. sec. 78o-3, as amended, or

regulations adopted thereunder; or

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

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

(a) Protected health information;

(b) Health records;

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

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

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

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

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

(h) Information originating from, and intermingled to be indistinguishable from, or information treated in the same manner as information exempt under this subsection that is maintained by a covered entity or business

associate as defined by HIPAA or a program or a qualified service organization as defined by 42 C.F.R. sec. 2.11;

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

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

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

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

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

(n) Data processed or maintained:

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

2. That is necessary to retain to administer benefits for another individual relating to the individual under subparagraph 1. of this paragraph and used for the purposes of administering those benefits; or

3. In the course of an individual applying to, employed by, or acting as an agent of a controller, processor, or a third party, to the extent that

the data is collected and used within the context of that role;

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

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

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

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

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

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

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

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

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

(c) Delete personal data provided by the consumer;

(d) Obtain a copy of the consumer's personal data that the consumer previously provided to the controller in a portable and, to the extent technically

practicable, readily usable format that allows the consumer to read or transmit the data to another controller without hindrance, where the processing is carried out by automated means;

(e) Opt out of targeted advertising;

(f) Opt out of tracking; and

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

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

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

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

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

extension;

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

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

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

(7) A controller shall:

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

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

(c) Inform the consumer of any action taken or not taken in response to the appeal, along with a written explanation of the reasons in support thereof, within thirty (30) days of receipt of an appeal. That period may be extended by sixty (60) additional days where reasonably necessary, taking into account the complexity and number of the requests serving as the basis for the appeal. The controller shall inform the consumer of such an extension within thirty (30) days of receipt of the appeal, together with the reasons for the delay. The controller shall also provide the consumer with an email address or other online mechanism through which the consumer may submit the appeal, along with any action taken or not taken by the controller in response to the appeal and the controller's written explanation of the reasons in support thereof, to the Attorney General; and

(d) When informing a consumer of any action taken or not taken in response to an appeal pursuant to this subsection, clearly and prominently provide the consumer with information about how to file a complaint with the Office of Consumer Protection in the Office of the Attorney General. The controller shall maintain records of all appeals and how it responded to them for at least twenty-four (24) months and shall, upon request, compile and provide a copy of the records to the Attorney General.

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

(1) A controller shall:

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

(b) Not process personal data in violation of state and federal laws that prohibit

unlawful discrimination against consumers. A controller shall not discriminate against a consumer for exercising any of the consumer rights contained in Section 3 of this Act, including denying goods or services, charging different prices or rates for goods or services, or providing a different level of quality of goods and services to the consumer. However, nothing in this paragraph shall be construed to require a controller to provide a product or service that requires the personal data of a consumer that the controller does not collect or maintain if the consumer has exercised his or her right to opt out pursuant to Section 3 of this Act or the offer is related to a consumer's informed, voluntary participation in a bona fide loyalty, rewards, premium features, discounts, or club card program;

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

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

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

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

(d) Provide an annual report to the Attorney General as prescribed by the Office of the Attorney General. The annual report form shall include:

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

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

3. The number of identifiable consumers whose personal data the

controller processed in the preceding quarter.

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

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

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

(b) The purpose for processing personal data;

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

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

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

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

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

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

(f) The name and contact information of the controller;

(g) The purposes for which personal data are processed, as well as the basis for processing as provided in subsection (6) of this section; and

(h) The estimated period of time for which the controller will retain the consumer's personal data or, if this is not known, the criteria that the controller will use in determining that period of time.

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

(5) Controllers shall ensure that any privacy notices or disclosures required under this section:

(a) Use clear and plain language;

(b) Are provided in English and any other language in which the controller communicates with the consumer to whom the information pertains;

(c) Are understandable to the least sophisticated consumer; and

(d) Provide an explanation of how the consumer's data will be used by the controller.

(6) Controllers shall not process the personal data of a consumer unless at least one (1) of the following conditions applies:

(a) The controller is able to demonstrate that the consumer's personal data is being processed for:

1. One (1) or more specific purposes; and

2. The controller does not require the consumer to provide consent as a condition of using the controller's product or service, unless processing the consumer's personal data is required to provide the product or service to the consumer;

(b) The processing is necessary to perform a contract to which the consumer is a party or in order to take steps at the request of the consumer prior to entering into a contract;

(c) The processing is necessary for the controller to comply with a legal obligation to which it is subject;

(d) The processing is necessary to protect the vital interests of the consumer or another natural person, and the processing cannot be manifestly based on another legal basis;

(e) The processing is necessary to perform a task carried out in the public interest or to exercise official authority vested in the controller; or

(f) The processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where the legitimate interests are overridden by the fundamental privacy interests of the consumer, in particular when processing the personal data of a child.

(7) A controller shall store or otherwise retain personal data so that it can be attributed to a consumer for no longer than is necessary for the purposes for which the personal data are processed.

(8) A controller shall not process personal data on the basis of a consumer's or a class of consumers' actual or perceived race, color, ethnicity, religion, national origin, sex, gender, gender identity, sexual orientation, family status, lawful source of income, or disability, in a manner that unlawfully discriminates against the consumer or class of consumers with respect to the offering or provision of:

(a) Housing;

(b) Employment;

(c) Credit;

(d) Education; or

(e) The goods, services, facilities, privileges, advantages, or accommodations of

any place of public accommodation.

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

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

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

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

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

(10) Except as otherwise provided in Sections 1 to 10 of this Act, a controller shall not process sensitive data concerning a consumer without allowing the consumer to opt out pursuant to Sections 1 to 10 of this Act, or in the case of the processing of sensitive data of a child, without obtaining consent from the child's parent or lawful guardian, in accordance with the requirements set forth in the federal Children's Online Privacy Protection Act, 15 U.S.C. sec. 6501 et seq.

(11) Except as otherwise provided in Sections 1 to 10 of this Act, a controller shall not knowingly or intentionally process the personal data of:

(a) A child for the purposes of targeted advertising or tracking; or

(b) A consumer that is not a child and is younger than eighteen (18) years old for the purposes of targeted advertising or tracking or the sale or sharing of personal data without obtaining consent from the consumer pursuant to subsection (6)(a) of this section.

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

(1) A processor shall adhere to the instructions of a controller and shall assist the controller in meeting its obligations under Sections 1 to 10 of this Act. Assistance shall include taking into account the nature of processing and the information available to the processor, by:

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

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

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

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

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

(c) Upon the reasonable request of the controller, make available to the

controller information in its possession necessary to demonstrate the processor's compliance with the obligations in this section; and

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

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

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

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

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

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

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

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

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

(c) The controller does not sell or share the personal data to any third party or

otherwise voluntarily disclose the personal data to any third party other than a processor, except as otherwise permitted in this section.

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

(4) A controller shall conduct and document a data protection assessment of each of the following processing activities involving personal data:

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

(b) The sale of personal data; and

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

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

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

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

4. Other substantial injury to consumers.

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

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

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

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

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

authorities;

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

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

(e) Provide a product or service specifically requested by a consumer or a parent or guardian of a child, perform a contract to which the consumer or parent or guardian of a child is a party, including fulfilling the terms of a written warranty, or take steps at the request of the consumer or parent or guardian of a child prior to entering into a contract;

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

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

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

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

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

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

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

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

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

(b) Effect a product recall, if the data is retained and processed solely for that purpose;

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

(d) Perform solely internal operations that are reasonably aligned and compatible with the purposes of processing as disclosed to the consumer and with the expectations of the consumer based on those purposes, or are otherwise compatible with processing in furtherance of the provision of a product or service specifically requested by the consumer or the performance of a contract to which the consumer is a party when those internal operations are performed during, and not following, the consumer's relationship with the controller.

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

(4) Nothing in Sections 1 to 10 of this Act shall be construed as an obligation

imposed on controllers and processors that:

(a) Adversely affects the privacy or other rights or freedoms of any persons, such as exercising the right of free speech pursuant to the First Amendment to the United States Constitution; or

(b) Applies to personal data by a person in the course of a purely personal or household activity.

(5) Personal data processed by a controller pursuant to this section shall not be processed for any purpose other than those expressly listed in this section unless otherwise allowed by Sections 1 to 10 of this Act.

(6) Personal data processed by a controller pursuant to this section may be processed solely to the extent that the processing is:

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

(b) Adequate, relevant, and limited to what is necessary in relation to the specific purposes listed in this section; and

(c) Insofar as possible, taking into account the nature and purpose of processing the personal data, subjected to reasonable administrative, technical, and physical measures to protect the confidentiality, integrity, and accessibility of the personal data and to reduce reasonably foreseeable risks of harm to consumers.

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

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

(9) Nothing in Sections 1 to 10 of this Act shall require a controller, processor, third

party, or consumer to disclose trade secrets.

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

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

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

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

(1) The Attorney General shall have exclusive authority to enforce the provisions of Sections 1 to 10 of this Act.

(2) The Attorney General may enforce Sections 1 to 10 of this Act by bringing an action in the name of the Commonwealth, or on behalf of persons residing in the Commonwealth. The Attorney General may issue a civil investigative demand to any controller or processor believed to be engaged in, or about to engage in, any violation of Sections 1 to 10 of this Act. The provisions of KRS 367.240 shall

apply to civil investigative demands issued under this section.

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

(4) If a controller or processor does not cure a violation under subsection (3) of this section or violates Sections 1 to 10 of this Act in breach of an express written statement provided to the Attorney General under this section, the Attorney General may initiate an action and seek damages for up to seven thousand five hundred dollars ($7,500) for each violation under Sections 1 to 10 of this Act.

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

(6) In determining a civil penalty under this section, the court shall consider a controller's or processor's good-faith efforts to comply with the requirements of Sections 1 to 10 of this Act.

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

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

(1) Except for those actions brought by the Attorney General to enforce Sections 1 to 10 of this Act, nothing in Sections 1 to 10 of this Act creates an independent cause of action.

(2) No person, except for the Attorney General, may enforce the rights and protections created by Sections 1 to 10 of this Act in any action. However, nothing in Sections 1 to 10 of this Act shall limit any other independent causes of action enjoyed by any person, including any constitutional, statutory, administrative, or common law rights or causes of action. The rights and protections in Sections 1 to 10 of this Act are not exclusive, and to the extent that a person has the rights and protections in this chapter because of another law other than Sections 1 to 10 of this Act, the person continues to have those rights and protections notwithstanding the existence of Sections 1 to 10 of this Act.

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

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

➔Section 11. KRS 367.240 is amended to read as follows:

(1) When the Attorney General has reason to believe that a person has engaged in, is engaging in, or is about to engage in any act or practice declared to be unlawful by KRS 367.110 to 367.300 ***or Sections 1 to 10 of this Act***, or when he ***or she*** believes it to be in the public interest that an investigation should be made to ascertain whether a person in fact has engaged in, is engaging in or is about to engage in, any act or practice declared to be unlawful by KRS 367.110 to 367.300 ***or Sections 1 to***

10 of this Act, he ***or she*** may execute in writing and cause to be served upon any person who is believed to have information, documentary material or physical evidence relevant to the alleged or suspected violation, an investigative demand requiring ***that***~~[such]~~ person to furnish, under oath or otherwise, a report in writing setting forth the relevant facts and circumstances of which he ***or she*** has knowledge, or to appear and testify or to produce relevant documentary material or physical evidence for examination, at ***a***~~[such]~~ reasonable time and place as may be stated in the investigative demand, concerning the advertisement, sale or offering for sale of any goods or services or the conduct of any trade or commerce that is the subject matter of the investigation. Provided however, that no person who has a place of business in Kentucky shall be required to appear or present documentary material or physical evidence outside of the county where he ***or she*** has his ***or her*** principal place of business within the Commonwealth.

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

➔Section 12. This Act may be cited as the Kentucky Consumer Data Protection Act.

➔Section 13. This Act takes effect on January 1, 2026.