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 12 of this Act:

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

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

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

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

(2) "Air carriers" has the same meaning as defined in the Federal Aviation Act 49 U.S.C. secs. 40101, et seq., including the Airline Deregulation Act, 49 U.S.C. sec. 41713;

(3) "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 such consumer rights with respect to the personal data at issue;

(4) "Biometric data" means data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that are used to identify a specific individual 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;

(5) "Business associate" has the same meaning as established 45 C.F.R. sec. 160.103 pursuant to the federal Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191;

(6) "Child" has the same meaning as defined in the Children's Online Privacy Protection Act, 15 U.S.C. secs. 6501 et seq.;

(7) "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;

(8) "Consumer" means a natural person who is a resident of Kentucky acting only in an individual or household context but does not include a natural person acting in a commercial or employment context;

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

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

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

(12) "De-identified data" means data that cannot reasonably be used to infer

information about, or otherwise associated with, an identified or identifiable natural person, or a device linked to such 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 such 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 12 of this Act;

(13) "Fund" means the consumer privacy fund established in Section 11 of this Act;

(14) "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;

(15) "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 Chapters 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;

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

(17) "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, an identification number, location data, an 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;

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

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

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

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

(d) Is a public or other nonprofit institution.

(19) "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;

(20) "Personal data" means any information, including pseudonymous data and sensitive data, that relates to an identified or identifiable natural person. "Personal data" does not include de-identified data or publicly available information;

(21) "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;

(22) "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, such as the collection, use, storage, disclosure, analysis, deletion, or modification of personal data;

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

(24) "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;

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

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

(27) "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;

(28) "Sale," "sell," or "sold" means the exchange of personal data for monetary or other valuable 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 purposes of facilitating the consumer's exercising his or her right to opt out, as provided in Section 3 of this Act;

(29) "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 such data is used in order to avoid discrimination on the basis of a protected class that would violate a federal or state anti-discrimination

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;

(30) "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 purposes of facilitating the consumer's exercising their right to opt out, as provided in Section 3 of this Act:

(31) "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;

(32) "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 Web sites 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 Web sites or online applications when such 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 Web site or online application; or

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

(33) "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;

(34) "Tracking" means combining personal data obtained from a consumer's activities within a controller's own commonly branded Web sites 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 Web sites or online applications with personal data obtained from a third party solely on a consumer's device such that the personal data is not permitted to leave the device in a manner that permits it to be attributed to a consumer; and

(35) "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 12 of this Act applies 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:

(a) Control or process personal data of at least ten thousand (10,000) consumers; or

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

(2) Sections 1 to 12 of this Act shall not apply to any:

(a) State agency, including any body, authority, board, bureau, commission, district, or agency of the state or of any political subdivision of the state;

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

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

(d) Nonprofit organization; or

(e) Institution of higher education.

(3) The following information and data are exempt from Sections 1 to 12 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 12 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. secs. 11101 et seq.;

(f) Patient safety work product for purposes of the federal Patient Safety and Quality Improvement Act, 42 U.S.C. secs. 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 such activity is regulated by and authorized under the federal Fair Credit Reporting Act, 15 U.S.C. secs. 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. secs. 2721 et seq.;

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

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

(n) Data processed or maintained:

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

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;

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

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

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

(1) A consumer may invoke the consumer rights authorized pursuant to this section

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

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

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

(b) To delete personal data provided by the consumer;

(c) To 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;

(d) To opt out of targeted advertising;

(e) To opt out of tracking; and

(f) To opt out of the sale or sharing of personal data.

(3) Except as otherwise provided in Subsection (4) of this section and Sections 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 thirty (30) days of receipt of the request submitted pursuant to the methods described in this section. The response period may be extended once by fifteen (15) 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 such extension within the initial

thirty (30) 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 thirty (30) 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 requests from a consumer are excessive, repetitive, technically infeasible, or manifestly unfounded, such as when the controller reasonably believes that the primary purpose of the requests 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.

(4) 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.

(5) 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 such 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 e-mail 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 Consumer Protection Division of the Attorney General's office. The controller shall maintain records of all such appeals and how it responded to them for at least twenty-four (24) months and shall, upon request, compile and provide a copy of such 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. Such 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 this Section 3 of this Act, including denying goods or services, charging different prices or rates for goods or services, or providing a different level of quality of goods and services to the consumer. However, nothing in this paragraph shall be construed to require a controller to provide a product or service that requires the personal data of a consumer that the controller does not collect or maintain or to prohibit a controller from offering a different price, rate, level, quality, or selection of goods or services to a consumer, including offering goods or services for no fee, if the consumer has 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) Not process sensitive data concerning a consumer for a non-exempt purpose without the consumer having been presented with clear and conspicuous notice and an opportunity to opt out of such processing, or, in the case of the processing of sensitive data collected from a child, for purposes of delivering a product or service requested by the parent of such child, without processing such data in accordance with the federal Children's Online Privacy Protection Act, 15 U.S.C. secs. 6501 et seq.; and

(d) Upon a request made by the Office of the Attorney General pursuant to any investigation or action taken under Section 9 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.

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

(3) Controllers shall provide consumers with a reasonably accessible, clear, and meaningful privacy notice that includes:

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

(b) The purpose for processing personal data;

(c) How consumers may exercise their consumer rights pursuant to Section 3 of this Act;

(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 (7) of this section;

(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; and

(i) How and where consumers may exercise the rights contained in Section 3

of this Act, including how a consumer may appeal a controller's action with regard to the consumer's request;

(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) A controller shall establish in clear and plain language in a privacy notice one (1) or more secure and reliable means for consumers to submit a request to exercise their consumer rights under Section 3 of this Act. Such means shall take into account the ways in which consumers normally interact with the controller, the need for secure and reliable communication of such requests, and the ability of the controller to authenticate the identity of the consumer making the request. Controllers shall not require a consumer to create a new account in order to exercise consumer rights pursuant to Section 3 of this Act but may require a consumer to use an existing account.

(6) 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; and

(c) Are understandable to the least sophisticated consumer.

(7) 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 all of the following apply:

1. The consumer has provided consent to process his or her personal data for one (1) or more specific purposes or, in the case of processing the personal data of a child, the parent or legal guardian of the child

has provided such consent;

2. The consumer is informed prior to providing consent under this subsection that they may withdraw such consent at any time and how such consent may be withdrawn;

3. The consent provided under this subsection is as easy for the consumer to withdraw as it is to give;

4. 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; and

5. If the consumer grants consent as part of a written declaration that also concerns other matters, the request for consent is clearly distinguishable from the other matters in an intelligible and easily accessible form using clear and plain language;

(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 such legitimate interests are overridden by the fundamental privacy interests of the

consumer, in particular when processing the personal data of a child.

(8) A controller's collection of personal data shall be limited to what is reasonably necessary in relation to the purposes for which the personal data is processed.

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

(10) Except as provided in Sections 1 to 12 of this Act, a controller shall collect and process personal data only for specified and legitimate purposes, and a controller may not further process personal data in a manner that is not reasonably necessary to or compatible with those purposes, unless the controller obtains the consumer's consent and such consent meets the conditions set forth in subsection (7)(a) of this section.

(11) 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.

(12) 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 subsection shall be construed to require a controller to provide a product or service that requires the personal data of a consumer that the controller does not collect or maintain or to prohibit a controller from offering a different price, rate, level, quality, or selection of goods or services to a consumer, including offering goods or services for no fee, if the consumer has exercised his or her right to opt out pursuant to Section 3 of this Act or the offer is related to a consumer's voluntary participation in a bona fide loyalty, rewards, premium features, discounts, or club card program.

(13) 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 such 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 such a benefit to which the consumer is entitled as part of such program; and

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

(14) Except as otherwise provided in Sections 1 to 12 of this Act, a controller shall not process sensitive data concerning a consumer without obtaining the consumer's consent pursuant to subsection (7)(a) of this section 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 Children's Online Privacy Protection Act, 15 U.S.C. secs. 6501 et seq.

(15) Except as otherwise provided in Sections 1 to 12 of this Act, a controller shall not process the personal data of a child for the purposes of targeted advertising or tracking.

(16) Except as otherwise provided in Sections 1 to 12 of this Act, a controller shall not process the personal data of 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 such consumer pursuant to subsection (7)(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 12 of this Act. Such assistance shall include:

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

(b) Taking into account the nature of processing and the information available to the processor, by assisting the controller in meeting the controller's obligations in relation to the security of processing the personal data and in relation to the notification of a breach of the security of the system of the processor pursuant to KRS 365.732 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 12 of this Act shall be construed to require a controller or processor to:

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

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

(c) Collect, obtain, retain, or access any data or technology, in order to be

capable of associating an authenticated consumer request with personal data.

(2) Nothing in Sections 1 to 12 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.

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

(1) Nothing in Sections 1 to 12 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 such action;

(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 this Sections 1 to 12 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;

(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 such 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 12 of this Act shall not apply where compliance by the controller or processor with Sections 1 to 12 of this Act would violate an evidentiary privilege under the laws of this Commonwealth. Nothing in Sections 1 to 12 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 12 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 12 of this Act.

(6) Personal data processed by a controller pursuant to this section may be processed solely to the extent that such 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 such processing qualifies for the exemption and complies with the requirements in this section.

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

(9) Nothing in Sections 1 to 12 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 12 of Act, shall

not be in violation of Sections 1 to 12 of this Act if the third party controller or processor that receives and processes such personal data is in violation of Sections 1 to 12 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 12 of this Act, is not in violation of Sections 1 to 12 of this Act if the controller or processor that discloses such personal data is in violation of Sections 1 to 12 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.

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

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

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

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

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

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

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

3. A physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of consumers, where such intrusion would

be offensive to a reasonable person; or

4. Any other substantial injury to consumers;

(d) The processing of sensitive data; and

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

(2) Data protection impact assessments conducted under this section shall take into account the type of personal data to be processed by the controller, including the extent to which the personal data are sensitive data, and the context in which the processing is to occur.

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

(4) The Attorney General may request, in writing, that a controller disclose any data protection impact assessment that is relevant to an investigation conducted by the Attorney General, and the controller shall make the requested data protection impact assessment available to the Attorney General upon such request. The Attorney General may evaluate the data protection impact assessments for compliance with the requirements of Sections 1 to 12 of this Act.

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

(6) The disclosure of a data protection impact assessment pursuant to a request from

the Attorney General under subsection (4) of this section does not constitute a waiver of the attorney-client privilege or work product protection with respect to the assessment and any information contained in the assessment, unless otherwise subject to case law regarding the applicability of the attorney-client privilege or work product protections.

(7) Data protection assessments conducted by a controller for the purpose of compliance with other laws or regulations may fulfill a controller's obligations under this section if they have a similar scope and effect.

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

(1) Except as provided in Section 10 of this Act, the Attorney General shall have exclusive authority to enforce the provisions of Sections 1 to 12 of this Act.

(2) The Attorney General may enforce Sections 1 to 12 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 12 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 12 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 12 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 statutory damages shall be initiated against the controller or processor.

(4) If a controller or processor continues to violate Sections 1 to 12 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 continued violation under Sections 1 to 12 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 12 of this Act.

(6) In determining a civil penalty under this section, the court shall consider, as mitigating factors, a controller's or processor's good faith efforts to comply with the requirements of Sections 1 to 12 of this Act and any actions to cure or remedy the violations before an action is filed.

(7) All receipts from the imposition of civil penalties under this section shall be deposited into the consumer privacy fund created in Section 11 of this Act.

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

(1) Except as provided in subsection (3) of this section, nothing in Sections 1 to 12 of this Act creates an independent cause of action, except for those actions brought by the Attorney General to enforce Sections 1 to 12 of this Act.

(2) Except as provided in subsection (3) of this section, no person, except for the Attorney General, may enforce the rights and protections created by Sections 1 to 12 of this Act in any action. However, nothing in Sections 1 to 12 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 12 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 12 of this Act, the person continues to have those rights and protections notwithstanding the existence of

Sections 1 to 12 of this Act.

(3) A consumer alleging a violation of Section 3, subsection (11) of Section 4, or subsections (14) to (16) of Section 4 of this Act may bring a civil action in any court of competent jurisdiction. Remedies shall be limited to appropriate injunctive relief. The court shall also award reasonable attorneys' fees and costs to any prevailing plaintiff.

➔SECTION 11. 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 9 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 12 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 12 of this Act.

➔SECTION 12. A NEW SECTION OF KRS CHAPTER 367 IS CREATED TO READ AS FOLLOWS:

(1) Sections 1 to 12 of this Act is a matter of statewide concern and supersedes and preempts all rules, regulations, codes, ordinances, and other laws adopted by a city, county, city and county, municipality, or local agency regarding the processing of personal data by controllers or processors.

(2) Any reference to federal, state, or local law or statute in Sections 1 to 12 of this Act shall be deemed to include any accompanying rules or regulations or exemptions thereto.

➔Section 13. 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 12 of this Act***, or when he 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 12 of this Act***, he 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 such person to furnish, under oath or otherwise, a report in writing setting forth the relevant facts and circumstances of which he has knowledge, or to appear and testify or to produce relevant documentary material or physical evidence for examination, at 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 has his 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 principal place of business or in the Franklin Circuit Court.

➔Section 14. The provisions of this Act takes effect on January 1, 2024.