

1 AN ACT relating to data privacy.

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

3 ➔Section 1. KRS 367.3611 is amended to read as follows:

4 As used in KRS 367.3611 to 367.3629:

- 5 (1) "Affiliate" means a legal entity that controls, is controlled by, or is under common
6 control with another legal entity or shares common branding with another legal
7 entity. For the purposes of this definition, "control" or "controlled" means:
- 8 (a) Ownership of, or the power to vote, more than fifty percent (50%) of the
9 outstanding shares of any class of voting security of a company;
 - 10 (b) Control in any manner over the election of a majority of the directors or of
11 individuals exercising similar functions; or
 - 12 (c) The power to exercise controlling influence over the management of a
13 company;
- 14 (2) "Authenticate" means verifying through reasonable means that the consumer
15 entitled to exercise his or her consumer rights in KRS 367.3615 is the same
16 consumer exercising such consumer rights with respect to the personal data at issue;
- 17 (3) **"Automatic content recognition data":**
- 18 **(a) Means data about a consumer's content viewing history collected through**
19 **the use of technology that is embedded or operated through a smart**
20 **television or smart monitor, integrated with internet connectivity and an**
21 **operating system that identifies, in real time, the specific content displayed**
22 **by analyzing audio or video fingerprints, including but not limited to**
23 **content received through broadcast, cable, satellite, streaming services, or**
24 **external inputs, through digital fingerprinting, watermark detection, or**
25 **similar comparison techniques; and**
 - 26 **(b) Does not include data:**
 - 27 **1. Collected about a consumer's interactions with content provided by the**

1 *controller's own services;*

2 *2. Generated in the course of providing a feature or service requested by*
3 *a consumer; or*

4 *3. Collected for the purpose of enforcing terms of service;*

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

12 (5)~~(4)~~ "Business associate" has the same meaning as established in 45 C.F.R. sec.
13 160.103 pursuant to HIPAA;

14 (6)~~(5)~~ "Child" has the same meaning as in 15 U.S.C. sec. 6501;

15 (7)~~(6)~~ "Consent" means a clear affirmative act signifying a consumer's freely given,
16 specific, informed, and unambiguous agreement to process personal data relating to
17 the consumer. Consent may include a written statement, written by electronic
18 means or any other unambiguous affirmative action;

19 (8)~~(7)~~ "Consumer" means a natural person who is a resident of the Commonwealth
20 of Kentucky acting only in an individual context. Consumer does not include a
21 natural person acting in a commercial or employment context;

22 (9)~~(8)~~ "Controller" means the natural or legal person that, alone or jointly with
23 others, determines the purpose and means of processing personal data;

24 (10)~~(9)~~ "Covered entity" has the same meaning as established in 45 C.F.R. sec.
25 160.103 pursuant to HIPAA;

26 (11)~~(10)~~ "Decisions that produce legal or similarly significant effects concerning a
27 consumer" means a decision made by a controller that results in the provision or

1 denial by the controller of financial and lending services, housing, insurance,
2 education enrollment, criminal justice, employment opportunities, health care
3 services, or access to basic necessities like food and water;

4 ~~(12)~~~~(11)~~ "De-identified data" means data that cannot reasonably be linked to an
5 identified or identifiable natural person or a device linked to a person;

6 ~~(13)~~~~(12)~~ "Fund" means the consumer privacy fund established in KRS 367.3629;

7 ~~(14)~~~~(13)~~ "Health care provider" means:

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

9 (b) Any person or entity providing health care or health services, including those
10 licensed, certified, or registered under, or subject to, KRS 194A.700 to
11 194A.729 or KRS Chapter 310, 311, 311A, 311B, 312, 313, 314, 314A, 315,
12 319, 319A, 319B, 319C, 320, 327, 333, 334A, or 335;

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

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

18 ~~(15)~~~~(14)~~ "Health record" means a record, other than for financial or billing purposes,
19 relating to an individual, kept by a health care provider as a result of the
20 professional relationship established between the health care provider and the
21 individual;

22 ~~(16)~~~~(15)~~ "HIPAA" means the federal Health Insurance Portability and Accountability
23 Act of 1996, Pub. L. No. 104-191;

24 ~~(17)~~~~(16)~~ "Identified or identifiable natural person" means a person who can be readily
25 identified directly or indirectly;

26 ~~(18)~~~~(17)~~ "Institution of higher education" means an educational institution which:

27 (a) Admits as regular students only individuals having a certificate of graduation

1 from a high school or the recognized equivalent of such a certificate;

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

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

9 (d) Is a public or other nonprofit institution;

10 (19)~~(18)~~ "Nonprofit organization" means any incorporated or unincorporated entity
11 that:

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

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

15 (20)~~(19)~~ "Personal data" means any information that is linked or reasonably linkable to
16 an identified or identifiable natural person. Personal data does not include de-
17 identified data or publicly available information;

18 (21)~~(20)~~ "Precise geolocation data" means information derived from technology,
19 including but not limited to global positioning system level latitude and longitude
20 coordinates or other mechanisms, that directly identifies the specific location of a
21 natural person with precision and accuracy within a radius of one thousand seven
22 hundred fifty (1,750) feet. Precise geolocation data does not include the content of
23 communications or any data generated by or connected to advanced utility metering
24 infrastructure systems or equipment for use by a utility;

25 (22)~~(21)~~ "Process" or "processing" means any operation or set of operations performed,
26 whether by manual or automated means, on personal data or on sets of personal
27 data, including but not limited to the collection, use, storage, disclosure, analysis,

1 deletion, or modification of personal data;

2 ~~(23)~~~~(22)~~ "Processor" means a natural or legal entity that processes personal data on
3 behalf of a controller;

4 ~~(24)~~~~(23)~~ "Profiling" means any form of automated processing performed on personal
5 data to evaluate, analyze, or predict personal aspects related to an identified or
6 identifiable natural person's economic situation, health, personal preferences,
7 interests, reliability, behavior, location, or movements;

8 ~~(25)~~~~(24)~~ "Protected health information" means the same as established in 45 C.F.R.
9 sec. 160.103 pursuant to HIPAA;

10 ~~(26)~~~~(25)~~ "Pseudonymous data" means personal data that cannot be attributed to a
11 specific natural person without the use of additional information, provided that the
12 additional information is kept separately and is subject to appropriate technical and
13 organizational measures to ensure that the personal data is not attributed to an
14 identified or identifiable natural person;

15 ~~(27)~~~~(26)~~ "Publicly available information" means information that is lawfully made
16 available through federal, state, or local government records, or information that a
17 business has a reasonable basis to believe is lawfully made available to the general
18 public through widely distributed media, by the consumer, or by a person to whom
19 the consumer has disclosed the information, unless the consumer has restricted the
20 information to a specific audience;

21 ~~(28)~~~~(27)~~ "Sale of personal data" means the exchange of personal data for monetary
22 consideration by the controller to a third party. Sale of personal data does not
23 include:

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

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

- 1 (c) The disclosure or transfer of personal data to an affiliate of the controller;
- 2 (d) The disclosure of information that the consumer:
- 3 1. Intentionally made available to the general public via a channel of mass
- 4 media; and
- 5 2. Did not restrict to a specific audience; or
- 6 (e) The disclosure or transfer of personal data to a third party as an asset that is
- 7 part of a proposed or actual merger, acquisition, bankruptcy, or other
- 8 transaction in which the third party assumes control of all or part of the
- 9 controller's assets;

10 **(29)**~~[(28)]~~ "Sensitive data" means a category of personal data that includes:

- 11 (a) Personal data indicating racial or ethnic origin, religious beliefs, mental or
- 12 physical health diagnosis, sexual orientation, or citizenship or immigration
- 13 status;
- 14 (b) The processing of genetic or biometric data that is processed for the purpose
- 15 of uniquely identifying a specific natural person;
- 16 (c) The personal data collected from a known child; or
- 17 (d) Precise geolocation data;

18 **(30) "Smart monitor":**

19 **(a) Means a digital, display device that integrates hardware and software**

20 **components to enable:**

21 **1. Internet connectivity;**

22 **2. Application execution; and**

23 **3. Media content streaming independently of an external computer or**

24 **media source; and**

25 **(b) Does not include a voice assistant device or mobile device;**

26 **(31)**~~[(29)]~~ "State agency" means all departments, offices, commissions, boards,

27 institutions, and political and corporate bodies of the state, including the offices of

1 the clerk of the Supreme Court, clerks of the appellate courts, the several courts of
2 the state, and the legislature, its committees, or commissions;

3 ~~(32)~~~~(30)~~ "Targeted advertising" means displaying advertisements to a consumer where
4 the advertisement is selected based on personal data obtained or inferred from that
5 consumer's activities over time and across nonaffiliated websites or online
6 applications to predict that consumer's preferences or interests. "Targeted
7 advertising" does not include:

- 8 (a) Advertisements based on activities within a controller's own or affiliated
9 websites or online applications;
- 10 (b) Advertisements based on the context of a consumer's current search query,
11 visit to a website, or online application;
- 12 (c) Advertisements directed to a consumer in response to the consumer's request
13 for information or feedback; or
- 14 (d) Processing personal data solely for measuring or reporting advertising
15 performance, reach, or frequency;

16 ~~(33)~~~~(31)~~ "Third party" means a natural or legal person, public authority, agency, or
17 body other than the consumer, controller, processor, or an affiliate of the processor
18 or the controller; and

19 ~~(34)~~~~(32)~~ "Trade secret" has the same meaning as in KRS 365.880.

20 ➔Section 2. KRS 367.3617 is amended to read as follows:

21 (1) A controller shall:

- 22 (a) Limit the collection of personal data to what is adequate, relevant, and
23 reasonably necessary in relation to the purposes for which the data is
24 processed as disclosed to the consumer;
- 25 (b) Except as otherwise provided in this section, not process personal data for
26 purposes that are neither reasonably necessary to nor compatible with the
27 disclosed purposes for which the personal data is processed as disclosed to the

- 1 consumer, unless the controller obtains the consumer's consent;
- 2 (c) Establish, implement, and maintain reasonable administrative, technical, and
3 physical data security practices to protect the confidentiality, integrity, and
4 accessibility of personal data. The data security practices shall be appropriate
5 to the volume and nature of the personal data at issue;
- 6 (d) Not process personal data in violation of state and federal laws that prohibit
7 unlawful discrimination against consumers. A controller shall not discriminate
8 against a consumer for exercising any of the consumer rights contained in
9 KRS 367.3615, including denying goods or services, charging different prices
10 or rates for goods or services, or providing a different level of quality of
11 goods and services to the consumer. However, nothing in this paragraph shall
12 be construed to require a controller to provide a product or service that
13 requires the personal data of a consumer that the controller does not collect or
14 maintain, or to prohibit a controller from offering a different price, rate, level,
15 quality, or selection of goods or services to a consumer, including offering
16 goods or services for no fee, if the offer is related to a consumer's voluntary
17 participation in a bona fide loyalty, rewards, premium features, discounts, or
18 club card program; ~~and~~
- 19 (e) Not process sensitive data concerning a consumer without obtaining the
20 consumer's consent, or, in the case of the processing of sensitive data
21 collected from a known child, process the data in accordance with the federal
22 Children's Online Privacy Protection Act, 15 U.S.C. sec. 6501 et seq.; and
- 23 (f) Not collect automatic content recognition data without a consumer's
24 consent.
- 25 (2) Any provision of a contract or agreement of any kind that purports to waive or limit
26 in any way consumer rights pursuant to KRS 367.3615 shall be deemed contrary to
27 public policy and shall be void and unenforceable.

- 1 (3) Controllers shall provide consumers with a reasonably accessible, clear, and
2 meaningful privacy notice that includes:
- 3 (a) The categories of personal data processed by the controller;
 - 4 (b) The purpose for processing personal data;
 - 5 (c) How consumers may exercise their consumer rights pursuant to KRS
6 367.3615, including how a consumer may appeal a controller's decision with
7 regard to the consumer's request;
 - 8 (d) The categories of personal data that the controller shares with third parties, if
9 any; and
 - 10 (e) The categories of third parties, if any, with whom the controller shares
11 personal data.
- 12 (4) If a controller sells personal data to third parties or processes personal data for
13 targeted advertising, the controller shall clearly and conspicuously disclose such
14 activity, as well as the manner in which a consumer may exercise the right to opt
15 out of processing.
- 16 (5) A controller shall establish, and shall describe in a privacy notice, one (1) or more
17 secure and reliable means for consumers to submit a request to exercise their
18 consumer rights under KRS 367.3615. The different ways to submit a request by a
19 consumer shall take into account the ways in which consumers normally interact
20 with the controller, the need for secure and reliable communication of such
21 requests, and the ability of the controller to authenticate the identity of the
22 consumer making the request. Controllers shall not require a consumer to create a
23 new account in order to exercise consumer rights pursuant to KRS 367.3615 but
24 may require a consumer to use an existing account.
- 25 ➔Section 3. This Act takes effect July 1, 2027.