

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 (Effective January 1, 2026) is amended to read as
4 follows:

5 As used in KRS 367.3611 to 367.3629:

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

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

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

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

15 (2) "Authenticate" means verifying through reasonable means that the consumer
16 entitled to exercise his or her consumer rights in KRS 367.3615 is the same
17 consumer exercising such consumer rights with respect to the personal data at issue;

18 (3) **"Automated-decision system":**

19 (a) **Means a computational process, including one derived from algorithms,**
20 **machine learning, artificial intelligence, statistics, and other data**
21 **processing techniques, that processes personal data to make a decision or**
22 **facilitate human decision-making regarding surveillance pricing; and**

23 (b) **Excludes word processing software, spreadsheet software, map navigation**
24 **systems, web hosting, domain registration, networking, caching, website-**
25 **loading, data storage, firewalls, anti-virus, anti-malware, spam- and**
26 **robocall-filtering, spellchecking, calculators, database, or similar**
27 **technologies, provided that these technologies do not make decisions**

1 *regarding surveillance pricing;*

2 **(4) "Base price"** means the lowest price for a specific good or service offered by a
3 *controller to any consumer in Kentucky;*

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

11 **(6){(4)}** "Business associate" has the same meaning as established in 45 C.F.R. sec.
12 160.103 pursuant to HIPAA;

13 **(7){(5)}** "Child" has the same meaning as in 15 U.S.C. sec. 6501;

14 **(8){(6)}** "Consent" means a clear affirmative act signifying a consumer's freely given,
15 specific, informed, and unambiguous agreement to process personal data relating to
16 the consumer. Consent may include a written statement, written by electronic
17 means or any other unambiguous affirmative action;

18 **(9){(7)}** "Consumer" means a natural person who is a resident of the Commonwealth
19 of Kentucky acting only in an individual context. Consumer does not include a
20 natural person acting in a commercial or employment context;

21 **(10){(8)}** "Controller" means the natural or legal person that, alone or jointly with
22 others, determines the purpose and means of processing personal data;

23 **(11){(9)}** "Covered entity" has the same meaning as established in 45 C.F.R. sec.
24 160.103 pursuant to HIPAA;

25 **(12){(10)}** "Decisions that produce legal or similarly significant effects concerning a
26 consumer" means a decision made by a controller that results in the provision or
27 denial by the controller of financial and lending services, housing, insurance,

1 education enrollment, criminal justice, employment opportunities, health care
2 services, or access to basic necessities like food and water;

3 (13)~~(11)~~ "De-identified data" means data that cannot reasonably be linked to an
4 identified or identifiable natural person or a device linked to a person;

5 (14)~~(12)~~ "Fund" means the consumer privacy fund established in KRS 367.3629;

6 (15)~~(13)~~ "Health care provider" means:

7 (a) Any health facility as defined in KRS 216B.015;
8 (b) Any person or entity providing health care or health services, including those
9 licensed, certified, or registered under, or subject to, KRS 194A.700 to
10 194A.729 or KRS Chapter 310, 311, 311A, 311B, 312, 313, 314, 314A, 315,
11 319, 319A, 319B, 319C, 320, 327, 333, 334A, or 335;

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

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

17 (16)~~(14)~~ "Health record" means a record, other than for financial or billing purposes,
18 relating to an individual, kept by a health care provider as a result of the
19 professional relationship established between the health care provider and the
20 individual;

21 (17)~~(15)~~ "HIPAA" means the federal Health Insurance Portability and Accountability
22 Act of 1996, Pub. L. No. 104-191;

23 (18)~~(16)~~ "Identified or identifiable natural person" means a person who can be readily
24 identified directly or indirectly;

25 (19) "*Individualized data*" means *personal data collected through electronic*
26 *surveillance technology, observation, inference, or tracking of a consumer's*
27 *online activity or device characteristics, including but not limited to browsing*

1 **history, search history, precise geolocation data, device hardware characteristics,**
2 **or operating system;**

3 **(20){(17)}** "Institution of higher education" means an educational institution which:
4 (a) Admits as regular students only individuals having a certificate of graduation
5 from a high school or the recognized equivalent of such a certificate;
6 (b) Is legally authorized in this state to provide a program of education beyond
7 high school;
8 (c) Provides an educational program for which it awards a bachelor's or higher
9 degree, or provides a program which is acceptable for full credit toward such
10 a degree, a program of postgraduate or postdoctoral studies, or a program of
11 training to prepare students for gainful employment in a recognized
12 occupation; and
13 (d) Is a public or other nonprofit institution;

14 **(21){(18)}** "Nonprofit organization" means any incorporated or unincorporated entity
15 that:
16 (a) Is operating for religious, charitable, or educational purposes; and
17 (b) Does not provide net earnings to, or operate in any manner that inures to the
18 benefit of, any officer, employee, or shareholder of the entity;

19 **(22){(19)}** "Personal data" means any information that is linked or reasonably linkable to
20 an identified or identifiable natural person. Personal data does not include de-
21 identified data or publicly available information;

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

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

14 (31)¶(28) "Sensitive data" means a category of personal data that includes:

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

22 (32)¶(29) "State agency" means all departments, offices, commissions, boards,
23 institutions, and political and corporate bodies of the state, including the offices of
24 the clerk of the Supreme Court, clerks of the appellate courts, the several courts of
25 the state, and the legislature, its committees, or commissions;

26 (33) "Surveillance pricing":

27 (a) Means offering or setting a customized price increase for a good or service

1 for a specific consumer or group of consumers, based in whole or in part,
2 on individualized data collected through electronic surveillance technology;
3 and

4 **(b) Includes the use of technological methods, systems, or tools including, but**
5 **not limited to sensors, cameras, device tracking, biometric monitoring, or**
6 **other forms of observation or data collection that are capable of gathering**
7 **personally identifiable information about a consumer's behavior,**
8 **characteristics, location, or other personal attributes, whether in physical or**
9 **digital environments;**

10 (34)¶(30) "Targeted advertising" means displaying advertisements to a consumer where
11 the advertisement is selected based on personal data obtained or inferred from that
12 consumer's activities over time and across nonaffiliated websites or online
13 applications to predict that consumer's preferences or interests. "Targeted
14 advertising" does not include:

- 15 (a) Advertisements based on activities within a controller's own or affiliated
16 websites or online applications;
- 17 (b) Advertisements based on the context of a consumer's current search query,
18 visit to a website, or online application;
- 19 (c) Advertisements directed to a consumer in response to the consumer's request
20 for information or feedback; or
- 21 (d) Processing personal data solely for measuring or reporting advertising
22 performance, reach, or frequency;

23 (35)¶(31) "Third party" means a natural or legal person, public authority, agency, or
24 body other than the consumer, controller, processor, or an affiliate of the processor
25 or the controller; and

26 (36)¶(32) "Trade secret" has the same meaning as in KRS 365.880.

27 ➔Section 2. KRS 367.3617 (Effective January 1, 2026) is amended to read as

1 follows:

2 (1) A controller shall:

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

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

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

14 (d) Not process personal data in violation of state and federal laws that prohibit
15 unlawful discrimination against consumers. A controller shall not discriminate
16 against a consumer for exercising any of the consumer rights contained in
17 KRS 367.3615, including denying goods or services, charging different prices
18 or rates for goods or services, or providing a different level of quality of
19 goods and services to the consumer. However, nothing in this paragraph shall
20 be construed to require a controller to provide a product or service that
21 requires the personal data of a consumer that the controller does not collect or
22 maintain, or to prohibit a controller from offering a different price, rate, level,
23 quality, or selection of goods or services to a consumer, including offering
24 goods or services for no fee, if the offer is related to a consumer's voluntary
25 participation in a bona fide loyalty, rewards, premium features, discounts, or
26 club card program;[and]

27 (e) Not process sensitive data concerning a consumer without obtaining the

1 consumer's consent, or, in the case of the processing of sensitive data
2 collected from a known child, process the data in accordance with the federal
3 Children's Online Privacy Protection Act, 15 U.S.C. sec. 6501 et seq.; and

4 (f) Not engage in surveillance pricing, or offer, set, or display a price for a
5 purchasable good or service to a consumer using an automated-decision
6 system that is based, in whole or in part, on individualized data. The base
7 price for all purchasable goods and services shall be the same for all
8 prospective consumers regardless of their individualized data. However, this
9 paragraph shall not be construed to prohibit any of the following:

10 1. An adjustment of the base price based on a real-time, non-
11 individualized factor, such as current market demand, inventory
12 levels, competitor pricing, or time-of-day, provided that the adjusted
13 price is applied uniformly to all consumers seeking the good or service
14 at that time and in that region, regardless of the consumer's
15 individualized data;

16 2. An offer of a different price, rate, level, or quality of goods or services
17 to a consumer who is a bona fide participant in a voluntary loyalty,
18 rewards, premium features, discounts, or club card program where the
19 difference is clearly disclosed and does not rely on individualized data
20 beyond what is necessary for program operation; or

21 3. Price differences based solely on legitimate, verifiable costs, such as
22 shipping costs to different geographical zones or costs related to the
23 method of service delivery.

24 (2) Any provision of a contract or agreement of any kind that purports to waive or limit
25 in any way consumer rights pursuant to KRS 367.3615 shall be deemed contrary to
26 public policy and shall be void and unenforceable.

27 (3) Controllers shall provide consumers with a reasonably accessible, clear, and

1 meaningful privacy notice that includes:

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

3 (b) The purpose for processing personal data;

4 (c) How consumers may exercise their consumer rights pursuant to KRS
5 367.3615, including how a consumer may appeal a controller's decision with
6 regard to the consumer's request;

7 (d) The categories of personal data that the controller shares with third parties, if
8 any; and

9 (e) The categories of third parties, if any, with whom the controller shares
10 personal data.

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

15 (5) A controller shall establish, and shall describe in a privacy notice, one (1) or more
16 secure and reliable means for consumers to submit a request to exercise their
17 consumer rights under KRS 367.3615. The different ways to submit a request by a
18 consumer shall take into account the ways in which consumers normally interact
19 with the controller, the need for secure and reliable communication of such
20 requests, and the ability of the controller to authenticate the identity of the
21 consumer making the request. Controllers shall not require a consumer to create a
22 new account in order to exercise consumer rights pursuant to KRS 367.3615 but
23 may require a consumer to use an existing account.

24 ➔Section 3. This Act may be cited as the Kentucky Price Fairness Act.