CHAPTER 13

(HB 473)

AN ACT relating to consumer data privacy.

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

➔Section 1. KRS 367.3613 (Effective January 1, 2026) is amended to read as follows:

(1) KRS 367.3611 to 367.3629 apply to persons that conduct business in the Commonwealth or produce products or services that are targeted to residents of the Commonwealth and that during a calendar year control or process personal data of at least:

(a) One hundred thousand (100,000) 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) KRS 367.3611 to 367.3629 shall not apply to any:

(a) City, state agency, or any political subdivision of the state;

(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.;

(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; or

(g) 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 KRS 367.3611 to 367.3629:

(a) Protected health information under HIPAA;

(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 KRS 367.3611 to 367.3629, 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, or a program or qualified service organization as defined by 42 C.F.R. sec. 2.11;

(i) ***Information collected by a health care provider who is a covered entity that maintains protected health information in accordance with HIPAA and related regulations, 45 C.F.R. pts. 160, 162, and 164;***

(j) Information included in a limited data set as described in 45 C.F.R. 164.514(e), to the extent the information is used, disclosed, and maintained as specified in 45 C.F.R. sec. 164.514(e);

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

(l) ~~[(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. sec. 1681 et seq.;

(m) ~~[(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.;

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

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

(p) ~~[(n)]~~ Data processed or maintained:

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

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

3. 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;

(q) ~~[(o)]~~ Data processed by a utility, an affiliate of a utility, or a holding company system organized specifically for the purpose of providing goods or services to a utility as defined in KRS 278.010. For purposes of this paragraph, "holding company system" means two (2) or more affiliated persons, one (1) or more of which is a utility; and

(r) ~~[(p)]~~ Personal data collected and used for purposes of federal policy under the Combat Methamphetamine Epidemic Act of 2005.

(4) Controllers and processors that comply with the verifiable parental consent requirements of the 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 KRS 367.3611 to 367.3629.

➔Section 2. KRS 367.3621 (Effective January 1, 2026) is amended 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;

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

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

1. Unfair or deceptive treatment of consumers 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, where an intrusion would be offensive to a reasonable person; or

4. 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 identify and weigh the benefits that may flow, directly and indirectly, from the processing to the controller, the 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.

(3) The Attorney General may request, pursuant to an investigative demand, 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 data protection impact assessment available to the Attorney General. The Attorney General may evaluate the data protection impact assessments for compliance with the requirements of KRS 367.3611 to 367.3629.

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

(5) The disclosure of a data protection impact assessment pursuant to a request from the Attorney General under subsection (3) 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.

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

(7) Data protection assessments conducted by a controller for the purpose of compliance with other laws or regulations may comply under this section if the assessments have a reasonably comparable scope and effect.

(8) Data protection assessment requirements shall apply to processing activities created or generated on or after June 1, 2026.

Signed by Governor March 15, 2025.