

**367.3617 Limitations on the collection and use of personal data by a controller -- Waiver of consumer rights contrary to public policy -- Privacy notice -- Notice for sale of personal data to third party -- Process for consumers to exercise consumer rights requirement.**

- (1) A controller shall:
  - (a) Limit the collection of personal data to what is adequate, relevant, and reasonably necessary in relation to the purposes for which the data is processed as disclosed to the consumer;
  - (b) Except as otherwise provided in this section, not process personal data for purposes that are neither reasonably necessary to nor compatible with the disclosed purposes for which the personal data is processed as disclosed to the consumer, unless the controller obtains the consumer's consent;
  - (c) Establish, implement, and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data. The data security practices shall be appropriate to the volume and nature of the personal data at issue;
  - (d) 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 KRS 367.3615, 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 offer is related to a consumer's voluntary participation in a bona fide loyalty, rewards, premium features, discounts, or club card program; and
  - (e) Not process sensitive data concerning a consumer without obtaining the consumer's consent, or, in the case of the processing of sensitive data collected from a known child, process the data in accordance with the federal Children's Online Privacy Protection Act, 15 U.S.C. sec. 6501 et seq.
- (2) Any provision of a contract or agreement of any kind that purports to waive or limit in any way consumer rights pursuant to KRS 367.3615 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 categories of personal data processed by the controller;
  - (b) The purpose for processing personal data;
  - (c) How consumers may exercise their consumer rights pursuant to KRS 367.3615, including how a consumer may appeal a controller's decision with regard to the consumer's request;
  - (d) The categories of personal data that the controller shares with third parties, if

any; and

- (e) The categories of third parties, if any, with whom the controller shares personal data.
- (4) If a controller sells personal data to third parties or processes personal data for targeted advertising, the controller shall clearly and conspicuously disclose such activity, as well as the manner in which a consumer may exercise the right to opt out of processing.
- (5) A controller shall establish, and shall describe in a privacy notice, one (1) or more secure and reliable means for consumers to submit a request to exercise their consumer rights under KRS 367.3615. The different ways to submit a request by a consumer 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 KRS 367.3615 but may require a consumer to use an existing account.

**Effective:** January 1, 2026

**History:** Created 2024 Ky. Acts ch. 72, sec. 4, effective January 1, 2026.