367.3625 Construction of KRS 367.3611 to 367.3629 -- Uses of data by controller or processor -- Application of evidentiary privilege -- Disclosure of data to third-party controller -- Limitations on processing of personal data -- Burden of proof.

(1) Nothing in KRS 367.3611 to 367.3629 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 known child;

(f) Perform a contract to which the consumer or parent or guardian of a known child is a party, including fulfilling the terms of a written warranty;

(g) Take steps at the request of the consumer or parent or guardian of a known child prior to entering into a contract;

(h) 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;

(i) 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;

(j) 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 deletion of 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

(k) Assist another controller, processor, or third party with any of the obligations under this subsection.

(2) The obligations imposed on controllers or processors under KRS 367.3611 to 367.3629 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) Effectuate a product recall;

(c) Identify and repair technical errors that impair existing or intended functionality; or

(d) Perform internal operations that are reasonably aligned with the expectations of the consumer or reasonably anticipated based on the consumer's existing relationship with the controller or are otherwise compatible with processing data in furtherance of the provision of a product or service specifically requested by a consumer or a parent or guardian of a known child or the performance of a contract to which the consumer or a parent or guardian of a known child is a party.

(3) The obligations imposed on controllers or processors under KRS 367.3611 to 367.3629 shall not apply to a controller or processor if compliance under KRS 367.3611 to 367.3629 would violate an evidentiary privilege under the laws of this Commonwealth. Nothing in KRS 367.3611 to 367.3629 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) A controller or processor that discloses personal data to a third-party controller or processor, in compliance with the requirements of KRS 367.3611 to 367.3629, is not in violation of KRS 367.3611 to 367.3629 if the third-party controller or processor that receives and processes such personal data is in violation of KRS 367.3611 to 367.3629, 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. A third-party controller or processor receiving personal data from a controller or processor in compliance with the requirements of KRS 367.3611 to 367.3629 is likewise not in violation of KRS 367.3611 to 367.3629 for the transgressions of the controller or processor from which it receives such personal data.

(5) Nothing in KRS 367.3611 to 367.3629 shall be construed as an obligation imposed on controllers and processors that adversely affects the privacy or other rights or freedoms of any persons, including but not limited to the right of free speech pursuant to the First Amendment to the Constitution of the United States, or applies to the processing of personal data by a person in the course of a purely personal or household activity.

(6) 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 KRS 367.3611 to 367.3629. Personal data processed by a controller pursuant to this section may be processed to the extent that such processing is:

(a) Reasonably necessary and proportionate to the purposes listed in this section; and

(b) Adequate, relevant, and limited to what is necessary in relation to the specific purposes listed in this section. Personal data collected, used, or retained pursuant to subsection (2) of this section shall, where applicable, take into account the nature and purpose or purposes of such collection, use, or

retention. The data shall be subject to reasonable administrative, technical, and physical measures to protect the confidentiality, integrity, and accessibility of personal data and to reduce reasonably foreseeable risks of harm to consumers relating to the collection, use, or retention of personal data.

(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.

Effective: January 1, 2026

History: Created 2024 Ky. Acts ch. 72, sec. 8, effective January 1, 2026.