

**367.3619 Data processing responsibilities to controller -- Contract requirements between controller and processor.**

- (1) A processor shall adhere to the instructions of a controller and shall assist the controller in meeting its obligations under KRS 367.3611 to 367.3629. Such assistance shall include:
  - (a) Taking into account the nature of processing and the information available to the processor, by appropriate technical and organizational measures, insofar as this is reasonably practicable, to fulfill the controller's obligation to respond to consumer rights requests pursuant to KRS 367.3615;
  - (b) Taking into account the nature of processing and the information available to the processor, by assisting the controller in meeting the controller's obligations in relation to the security of processing the personal data and in relation to the notification of a breach of the security of the system of the processor pursuant to KRS 365.732; and
  - (c) Providing necessary information to enable the controller to conduct and document data protection assessments pursuant to KRS 367.3621.
- (2) A contract between a controller and a processor shall govern the processor's data processing procedures with respect to processing performed on behalf of the controller. The contract shall be binding and shall clearly set forth instructions for processing personal data, the nature and purpose of processing, the type of data subject to processing, the duration of processing, and the rights and obligations of both parties. The contract shall also include requirements that the processor shall:
  - (a) Ensure that each person processing personal data is subject to a duty of confidentiality with respect to the data;
  - (b) At the controller's direction, delete or return all personal data to the controller as requested at the end of the provision of services, unless retention of the personal data is required by law;
  - (c) Upon the reasonable request of the controller, make available to the controller all information in its possession necessary to demonstrate the processor's compliance with the obligations prescribed in KRS 367.3611 to 367.3629;
  - (d) Allow, and cooperate with, reasonable assessments by the controller or the controller's designated assessor. Alternatively, the processor may arrange for a qualified and independent assessor to conduct an assessment of the processor's policies and technical and organizational measures in support of the obligations in KRS 367.3611 to 367.3629 using an appropriate and accepted control standard or framework and assessment procedure for assessments. The processor shall provide a report of the assessment to the controller upon request; and
  - (e) Engage any subcontractor pursuant to a written contract in accordance with this section that requires the subcontractor to meet the obligations of the processor with respect to the personal data.
- (3) Nothing in this section shall be construed to relieve a controller or processor from the liabilities imposed on it by virtue of its role in a processing relationship as defined by KRS 367.3611 to 367.3629.

- (4) Determining whether a person is acting as a controller or processor with respect to a specific processing of data is a fact-based determination that depends upon the context in which personal data is to be processed. A processor that continues to adhere to a controller's instructions with respect to a specific processing of personal data remains a processor.

**Effective:** January 1, 2026

**History:** Created 2024 Ky. Acts ch. 72, sec. 5, effective January 1, 2026.