367.3621 Data protection impact assessment -- Requirements -- Disclosure to Attorney General -- Confidentiality and exceptions -- Application. (Effective January 1, 2026)

(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 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.

Effective: January 1, 2026

History: Created 2024 Ky. Acts ch. 72, sec. 6, effective January 1, 2026.