Kentucky Joins Growing List of States to Enact a Comprehensive Data Privacy Act. What Does It Mean for Your Business?

Apr 18, 2024

Categories:

Publications
Technology Blog

Authors:

Janelle E. Thompson
Lauren E. Cole
Ashley J. Earle

The Kentucky Consumer Data Protection Act, or KCDPA, was signed into law by Governor Andy Beshear on April 4, 2024 (previously House Bill 15). The comprehensive law will go into effect January 1, 2026, and follows the trends of most other U.S. state privacy laws[1] enacted to date, mainly by focusing on standards for processing personal data. The KCDPA codifies many consumer rights relating to personal data, including the right to confirm whether an individual consumer's data is being used or otherwise collected or shared; correct any inaccuracies in your personal data; delete personal data provided; obtain a copy of your personal data; and opt out of targeted advertising, data sales, or profiling measures.

Who Must Comply with the KCDPA?

KCDPA applies to "controllers," which include entities that:

- Conduct business in the Commonwealth of Kentucky; 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:
  - 100,000 consumers; or
  - 25,000 consumers and derive over 50% of gross revenue from the sale of personal data.

The KCDPA exempts law enforcement agencies investigating fraud and first responders collecting information in connection to catastrophic events. In addition, there are several distinct entities that are exempt from the KCDPA, such as cities and municipalities, nonprofit organizations, HIPAA-covered entities, financial institutions, institutions of higher education, and small telephone utilities.

FBT Gibbons

Who Does the KCDPA Protect?

The KCDPA protects "consumers," meaning a natural person who is a resident of the Commonwealth of Kentucky acting only in an individual context. Consumers do not include a natural person acting in a commercial or employment context, and, as such, ***business-to-business (B2B) and employment-related activities are not within the scope of the KCDPA.***

Consumer Rights Under the KCDPA

Under the law, a consumer has the right to:

- Know whether a controller is processing personal data and accessing the personal data;
- Correct inaccuracies in personal data;
- Delete personal data;
- Obtain a copy of personal data previously provided to a controller; and
- Opt out of the processing of personal data for purposes of targeted advertising, the sale of personal data, or profiling.

A consumer can invoke the rights authorized to them by submitting a request to a controller specifying the consumer rights that the consumer wishes to invoke. Consumers have the right to appeal a controller's response to a denied request. If the appeal is denied within 60 days, the controller must provide the consumer with an online mechanism, if available, or another method for the consumer to contact the state attorney general to submit a complaint.

Are Controllers Required to Post Privacy Policies for Consumers?

Controllers are required to give a clear, reasonably accessible, and meaningful privacy policy to consumers. ***If a company triggers the KCDPA, it must provide a privacy policy***, and that policy, at a minimum, must include notice of:

- The categories of personal data processed by the controller;

- The purpose for processing the personal data;
- How consumers may exercise their consumer rights, including how a consumer may appeal a controller's decision regarding a consumer's request;
- The categories of personal data that the controller shares with third parties;
- The categories of third parties with whom the controller shares personal data; and
- Whether the controller engages in targeted advertising, and if so, the right to opt-out.

The privacy policy is a crucial part of data governance for controllers. Failure to provide a comprehensive and effective policy may subject controllers to the penalties and fines described below.

What Type of Data Is Covered by the KCDPA?

Under the KCDPA, personal data is extremely broad in scope, and means any information that is linked or reasonably linkable to an identified or identifiable natural person. Personal data does not include de-identified data or publicly available information (provided that such information has lawfully been made public and not otherwise restricted by the consumer).

The KCDPA requires controllers to get affirmative consent from consumers to process their "sensitive data." Sensitive data is a category of personal data that indicates:

- Personal data indicating racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status;
- The processing of genetic or biometric data that is processed for the purpose of uniquely identifying a specific natural person;
- The personal data collected from a known child; or
- Precise geolocation data.

If you are considering processing sensitive data, a pop-up disclosure "Click to Accept" button or a verification consent

checkbox is recommended to obtain clear, verified consent in advance of the sensitive data collection.

The KCDPA also has separate category for "pseudonymous data." Pseudonymous data means "personal data that cannot be attributed to a specific natural person without the use of additional information, provided that the additional information is kept separately and is subject to appropriate technical and organizational measures to ensure that the personal data is not attributed to an identified or identifiable natural person." To the extent that data can be easily tokenized or otherwise pseudonymized, this is a great option for managing data in compliance with Kentucky's new privacy law.

What Are the Main Types of Activities by Companies Being Regulated?

The "sale of personal data" and "targeted advertising" are some of the main concerns for Kentucky regulators. The sale of personal data is the "exchange of personal data for monetary consideration by the controller to a third party." However, the sale of personal data does not include the following categories:

- The disclosure of personal data to a processor that processes the personal data for the controller;
- The disclosure of personal data to a third party for purposes of providing a product or service requested by the consumer;
- The disclosure or transfer of personal data to an affiliate of the controller;
- The disclosure of information that the consumer has intentionally made available to the public via a channel of mass media, and did not restrict to a specific audience; or
- The disclosure or transfer of personal data to a third party as an asset that is part of a proposed or actual merger, acquisition, bankruptcy, or other transaction where the third party assumes control of all or part of the controller's assets.

Targeted advertising means "displaying advertisements to a consumer where the advertisement is selected based on personal

data obtained or inferred from that consumer's activities over time and across nonaffiliated websites or online applications to predict the consumer's preferences or interests. Targeted advertising does not include the following:

- Advertisements based on activities within a controller's own, or affiliated, websites or online applications;
- Advertisements based on the context of a consumer's current search query, visit to a website, or online application;
- Advertisements directed to a consumer in response to the consumer's request for information or feedback; or
- Processing personal data solely for measuring or reporting advertising performance, reach, or frequency.

Are Privacy Impact Assessments/Data Protection Impact Assessments Needed?

Controllers must conduct and document a data protection impact assessment of each of the following processing activities involving personal data:

- The processing of personal data for the purpose of targeted advertising;
- The processing of personal data for the purpose of selling personal data;
- The processing of personal data for the purpose of profiling, where the profiling presents a reasonably foreseeable risk of:
    - Unfair or deceptive treatment of consumers or disparate impact on consumers;
    - Financial, physical, or reputational injury to consumers;
    - 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
    - Other substantial injury to consumers;
- The processing of sensitive data; and

- Any processing of personal data that presents a heightened risk of harm to consumers

Who Has Enforcement Authority? And Is There a Private Right of Action?

Kentucky's attorney general has exclusive authority to investigate and enforce violations of the KCDPA. If an identified violation is not rectified within 30 days, the attorney general can seek damages of up to $7,500 for each violation.

Unlike privacy laws in other states, however, there is no private right of action for individual consumers under the KCDPA.

For more information and enforcement guidance, to update your privacy policy to comply with the KCDPA, or to conduct a data protection impact assessment, please contact the authors of this article or any member of Frost Brown Todd's Data Security and Privacy practice.

---

[1] Notably, KCDPA very closely mirrors the Virginia Consumer Data Protection Act(VCDPA).

FBT Gibbons