

Privacy Comes to the Bluegrass State: Kentucky Enacts a Comprehensive Data Privacy Law

On April 4, Governor Andy Beshear signed the Kentucky Consumer Data Protection Act (KCDPA), making Kentucky the fifteenth state to enact a comprehensive data privacy law. Set to go into effect on January 1, 2026, the KCDPA largely conforms to the majority of other recently enacted state data privacy laws. In particular, the law seems to have been modeled on a neighboring state: Virginia's Consumer Data Protection Act (VCDPA). The KCDPA does, however, deviate from the majority approach in a few notable ways.

Kentucky's applicability thresholds mirror those found in the VCDPA. The KCDPA applies to anyone who does business in Kentucky and controls or processes the personal data of either:

- i. at least 100,000 Kentucky consumers or
- ii. 25,000 Kentucky consumers while deriving over 50% of their gross revenue from the sale of personal data.

Notably, the KCDPA approach to the sale of personal data deviates from that of many other states' privacy laws in that the KCDPA includes only "the exchange of personal data for monetary consideration." In contrast, other states like California also include non-monetary considerations (e.g., assuming obligations to perform services) in their definitions.

The law contains several exemptions common to other states' privacy laws, including exempting all nonprofit organizations and entities regulated by the Gramm-Leach-Bliley Act (GLBA). Additionally, the law's definition of consumer excludes individuals acting in commercial or employment contexts. Notably, however, the KCDPA only offers a data-level exemption for data regulated by the Health Insurance Portability and Accountability Act (HIPAA). ([Click here](#) to read more about the different approaches that states have taken concerning data-level and entity-level exemptions to their privacy laws).

The KCDPA creates many of the same consumer data subject rights found in other state laws: the right to know if a business is collecting their data, the right to access the data a business has collected about them, the right to have that data deleted, and the right to opt out of the sale of their personal data or its processing for targeted advertising or profiling purposes. Unlike some other state laws, however, the KCDPA does not require that businesses honor universal opt-out signals.

As is the case with every other state data privacy law to date, with the notable exception of the California Consumer Privacy Act, the KCDPA does not create a private right of action. Instead, the law vests sole enforcement authority with the state's attorney general. Before implementing any action related to a violation of the KCDPA, the attorney general must provide businesses with 30 days to cure their alleged shortcomings. Unlike the cure period afforded by most other states' privacy laws, which sunsets after a certain period, the KCDPA's cure period is permanent.

As with every state data privacy law, companies should carefully evaluate whether they will be subject to the KCDPA. While enforcement is still a ways off, companies would be wise to begin laying the groundwork for compliance now in order to ease any burden from the eventual transition.



Daniel Kilburn

Associate

DKilburn@cozen.com
Phone: (215) 665-4726
Fax: (215) 665-2013



Benjamin Mishkin

Member

bmishkin@cozen.com
Phone: (215) 665-2171
Fax: (215) 372-2407

Related Practice Areas

- Technology, Privacy & Data Security