

Understanding the Implications of the Kentucky Consumer Data Privacy Act



ARTICLE 08.26.24 KEVIN CORNWELL

In the digital age, where data drives much of our daily lives, protecting consumer privacy has become paramount. With the introduction of the Kentucky Consumer Data Privacy Act (KCDPA), the state takes a significant step towards safeguarding the personal information of its residents. This act, akin to similar legislation emerging across the United States, reflects a growing recognition of the importance of privacy in the digital economy. Let's delve into the key aspects and implications of the KCDPA.

What is the Kentucky Consumer Data Privacy Act?

Enacted to enhance consumer privacy rights, the KCDPA empowers Kentucky residents with greater control over their personal data. Signed into law on April 4, 2024, and set to take effect on January 1, 2026, the act imposes obligations on businesses handling consumer data, outlining transparency requirements, data access provisions, and guidelines for data processing practices.

Scope

- control or process personal data of at least 100,000 Kentucky consumers; or
- control or process personal data of at least 25,000 Kentucky consumers and derive over 50% of gross revenue from the "sale" of personal data

Exemptions in the KCDPA

- Regulated Industries:
 - Certain industries are subject to existing federal or state privacy regulations that preempt the application of the KCDPA.
 - For example, healthcare providers or business associates governed by HIPAA or financial institutions regulated by GLBA are exempt from provisions of the KCDPA.
- Entity Types:
 - Certain entity exemptions commonly seen in other state privacy laws exist.
 - For example, any city, state agency, or political subdivision of the state; nonprofit organizations; higher education institutions; certain entities collecting data for specific law enforcement activities; first responders in connection with catastrophic events; and small telephone or municipally owned utilities.

- Data Types:
 - Certain data are exempt.
 - For example, protected health information and various other health-related data, certain types of consumer reporting data, data regulated by the Family Educational Rights and Privacy Act, and emergency contact information of an individual used for emergency contact purposes.

Key Provisions

- Consumer Rights:
 - Under the KCDPA, consumers have the right to request disclosure of what personal data businesses collect about them.
 - Consumers have the right to request correction of inaccuracies in the consumer's personal data.
 - Consumers are entitled to request deletion of their data.
 - Consumers may obtain a copy of their personal data in a readily usable format for transmission to another business.
 - Consumers may opt out of the processing of personal data for purposes of targeted advertising, the sale of personal data, or profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer.
- Transparency Requirements
 - Covered businesses must disclose their data collection and processing practices, including the purposes for which data is used.
 - They must notify consumers about their privacy rights and how to exercise them.
- Data Processing Restrictions:
 - The act imposes limitations on how businesses handle sensitive personal information, such as health or financial data.
 - It prohibits businesses from processing data in ways that would discriminate against consumers.
- Data Security Measures:
 - Covered businesses are required to implement reasonable security measures to safeguard consumer data from breaches or unauthorized access.
- Enforcement and Compliance:
 - The Kentucky Attorney General is tasked with enforcing the KCDPA, with penalties for non-compliance.

Implications for Businesses

- Compliance Burden:
 - Businesses must establish, implement, and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data.
 - Businesses must provide consumers with a reasonably accessible, clear, and meaningful privacy notice that includes the categories of personal data processed, the purpose for processing personal data, how consumers may exercise their consumer rights, the categories of personal data that the controller shares with third parties, and the categories of third parties, if any, with whom the controller shares personal data.
 - Consumer requests must be responded to within 45 days of the request. The act provides guidelines for extensions and refusal to respond.
 - Businesses must establish a process for consumers to submit requests and appeal refusals to respond. This process must be conspicuously available.
 - Information provided to a consumer must be free of charge, up to twice annually per consumer.
 - Businesses must conduct and document a data protection impact assessment of processing personal data for the following activities: targeted advertising, selling personal data, profiling, processing sensitive data, and any processing that presents a heightened risk of harm to consumers.
- Data Responsibility:
 - Limit the collection of personal data to what is adequate, relevant, and reasonably necessary.

- Do not process personal data for purposes that are neither reasonably necessary nor compatible with the disclosed purposes.
- Do not process personal data in violation of state and federal laws that prohibit unlawful discrimination against consumers.
- Do not process sensitive data concerning a consumer without obtaining the consumer's consent.
- Legal and Compliance Risks:
 - The Attorney General may request a data protection risk assessment to evaluate its effectiveness.
 - The Attorney General has exclusive authority to enforce violations of this Act. This can include prosecuting any violations.
 - The Attorney General may demand any information, documentary material, or physical evidence from any controller or processor believed to be engaged in or about to engage in any violation.
 - Businesses may receive a written notice from the Attorney General when a violation is noticed. If the violation is remediated within thirty days, no action for damages will be initiated.
 - If violations are not remediated within thirty days, The Attorney General may initiate an action to seek damages for up to \$7,500 for each continued violation.
 - The Attorney General may recover reasonable expenses incurred in investigating and preparing the case, court costs, attorney's fees, and any other relief ordered by the court of any action initiated

Implications for Compliance

- Assessment and Documentation:
 - Businesses must carefully assess whether they fall within any of the exempt categories outlined in the KCDPA.
 - Documenting the basis for exemptions and ensuring compliance with other privacy laws are essential steps in the compliance process.
- Risk Mitigation
 - While exemptions provide relief from certain compliance obligations, they also introduce potential risks, such as reputational harm or legal challenges.
 - Businesses should conduct thorough risk assessments to evaluate the implications of relying on exemptions and implement appropriate risk mitigation strategies.
- Transparency and Consumer Communication:
 - Even when exemptions apply, businesses should maintain transparency and communicate clearly with consumers about their data processing practices.
 - Providing accessible privacy notices and mechanisms for consumers to exercise their rights remains essential for building trust and accountability.

Navigating Complexity

As businesses adapt to the evolving privacy landscape, proactive compliance efforts, robust risk management practices, and transparent communication with consumers are critical for success. By embracing privacy as a fundamental value and integrating it into their operations, businesses can navigate the complexities of the KCDPA while fostering trust and loyalty among their customer base.

Looking Ahead

The passage of the Kentucky Consumer Data Privacy Act reflects a broader trend toward enhanced consumer privacy protections at the state level. As more states consider similar legislation, businesses face a complex regulatory landscape that demands proactive compliance measures.

Moving forward, businesses must prioritize privacy as a fundamental aspect of their operations, integrating privacy by design principles into their products and services. By prioritizing transparency, accountability, and consumer empowerment, businesses can navigate the evolving privacy landscape while building trust and loyalty among their customer base.

In conclusion, the Kentucky Consumer Data Privacy Act represents a significant milestone in the journey toward empowering consumers and enhancing privacy protections in the digital age. By embracing the principles outlined in the act, businesses can not only comply with regulatory requirements but also foster a culture of privacy and trust in their interactions with consumers.