



Privacy & Cybersecurity Update

April 2024

Kentucky Poised to Enact Consumer Data Protection Law

On March 27, the Kentucky Legislature sent House Bill 15 to Governor Andy Beshear for his signature and concurrence. Once HB 15 is enacted into law, Kentucky will join the growing number of states that have created comprehensive data privacy laws. HB 15 grants Kentucky residents a broad range of data protection rights and requires covered businesses to comply with new data privacy and information security requirements. While it imposes new compliance obligations on covered businesses, HB 15 notably does not create a private right of action. Rather, the law, which enters into force on January 1, 2026, assigns enforcement authority to the Kentucky attorney general.

Scope of Applicability

HB 15 applies to organizations that conduct business in Kentucky or produce products or services targeted to Kentucky residents and during a calendar year control or process the personal data of at least 100,000 consumers or control or process the personal data of at least 25,000 consumers *and* derive over 50% of gross revenue from the sale of personal data.

HB 15 includes several exemptions that are standard in data privacy frameworks, including exemptions for state and local governments, organizations governed by federal law (e.g., HIPAA, GLBA), and certain nonprofit and educational institutions.

Key Terms

HB 15 primarily regulates how a data “controller,” which it defines as “the natural or legal person that, alone or jointly with others, determines the purpose and means of

processing personal data,” can use and process a consumer’s personal data. The term “consumer” means a Kentucky resident acting only in an individual context and excludes individuals “acting in a commercial or employment context.” As in other state privacy laws, “personal data” is defined as “any information that is linked or reasonably linkable to an identified or identifiable natural person.” It does not, however, include within its scope either “de-identified data” or “publicly available information,” which each have their own unique definitions.

In addition, HB 15 creates additional requirements when an entity processes “sensitive data,” which is defined as a subset of personal data that includes any of the following:

- Personal data indicating racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status
- The processing of certain genetic or biometric data
- The personal data collected from a known child
- Precise geolocation data (i.e., technology-derived data that directly identifies the specific location of a person with precision and accuracy within a radius of 1,750 feet)

Consumer Privacy Rights

As with other state privacy laws, HB 15 grants consumers the following data privacy rights:

- To confirm whether or not a controller is processing the consumer’s personal data and to access the personal data (Know and Access Right)
- To correct inaccuracies in the consumer’s personal data, taking into account the nature of the personal data and the purposes of processing the data

- To delete personal data provided by or obtained about the consumer
- To obtain a copy of the consumer's personal data that the consumer previously provided to the controller in a portable and, to the extent technically practicable, readily usable format that allows the consumer to transmit the data to another controller without hindrance, where the processing is carried out by automated means (Data Portability Right)

The law emphasizes that with respect to both the Know and Access Right and the Data Portability Right, a controller is not required to respond to a request if doing so would cause it to reveal a trade secret. HB 15 creates a framework for how controllers must receive, authenticate, and respond to consumer data privacy requests. It also mandates that organizations establish a process to allow a consumer to appeal a controller's denial of a request.

Opt-Out Rights

In addition, HB 15 grants consumers the right to 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.

HB 15 takes a narrower view of the term "sale of personal data" than other privacy regulations, defining it as "the exchange of personal data for monetary consideration by the controller to a third party" and specifically exempting from its definition the disclosure of personal data to a processor that processes the personal data on behalf of the controller, to a third party for purposes of providing a product or service requested by the consumer, or to an affiliate of the controller. It also exempts the disclosure of information the consumer intentionally made available to the general public via a mass media channel and did not restrict to a specific audience. Certain corporate restructuring and bankruptcy-related transactions are also exempted from the definition.

The term "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 that

consumer's preferences or interests" and includes common exemptions related to online marketing.

Consent and Processing Obligations

HB 15 limits how a controller can use personal data without a consumer's consent. For example, a controller is prohibited from processing a consumer's sensitive data without obtaining the consumer's consent. If processing sensitive data collected from a known child under 13 years of age, the controller must process the data in accordance with the Children's Online Privacy Protection Act. Further, HB 15 provides that controllers cannot process personal data for "purposes that are neither reasonably necessary to nor compatible with the disclosed purposes for which the personal data is processed as disclosed to the consumer," unless the controller obtains the consumer's consent.

HB 15 also adopts more general restrictions, such as requiring controllers to limit the collection of personal data to "what is adequate, relevant, and reasonably necessary in relation to the purposes for which the data is processed as disclosed to the consumer."

Data Protection Assessments

Like other privacy laws, HB 15 requires a controller to conduct and document a data processing assessment for its processing activities that involve targeted advertising, selling personal data, processing sensitive data, profiling that presents certain risks, and any processing activities that present a "heightened risk of harm to consumers."

This data protection impact assessment must 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 law provides that the controller shall factor into this assessment the use of de-identified data, the reasonable expectations of consumers, the context of the processing of personal data, and the relationship between the controller and the consumer whose personal data will be processed. The assessment

must be made available to the Kentucky attorney general upon request.

Privacy Notices and Other Disclaimers

Controllers are required to provide consumers with “a reasonably accessible, clear, and meaningful privacy notice” that addresses:

- The categories of personal data processed by the controller
- The purpose for processing personal data
- How consumers may exercise their privacy rights
- The categories of personal data that the controller shares with third parties, if any
- The categories of third parties, if any, with whom the controller shares personal data

If a controller sells personal data to third parties or processes personal data for targeted advertising, the controller shall clearly and conspicuously disclose these activities, as well as the manner in which a consumer may exercise the right to opt out of processing.

Data Security Requirements

HB 15 places affirmative data security obligations on controllers. Specifically, it requires them to establish, implement, and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data appropriate to the volume and nature of the personal data at issue.

Processor Obligations and Data Processing Agreements

HB 15 also places affirmative obligations on processors, such as those related to compliance with a controller’s instructions and assistance in responding to consumer rights requests. Moreover, the law requires processors to help meet a controller’s obligations related to the security of processing personal data and providing notification of a [data breach](#) occurring within the processor’s system.

The law also requires controllers and processors to execute written agreements that contain certain data protection clauses, which must address, among other things, the

nature and purpose of data processing, the duration of the processing, the types of data subject to processing, parties’ rights and obligations, confidentiality duties, compliance disclosures, and subprocessing.

The law emphasizes that “[d]etermining 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” and a processor that adheres to a controller’s data processing instructions remains a processor.

FOR MORE INFORMATION

For more information, please contact:

Steven G. Stransky

216.566.5646

202.263.4126

Steve.Stransky@ThompsonHine.com

Certified Information Privacy Professional/Government (CIPP/G)

Certified Information Privacy Professional/United States (CIPP/US)

Thomas F. Zych

216.566.5605

Tom.Zych@ThompsonHine.com

Marla M. Izbicky

312.998.4253

Marla.Izbicky@ThompsonHine.com

Certified Information Privacy Professional/United States (CIPP/US)

Thora Knight

212.908.3971

Thora.Knight@ThompsonHine.com

This advisory bulletin may be reproduced, in whole or in part, with the prior permission of Thompson Hine LLP and acknowledgment of its source and copyright. This publication is intended to inform clients about legal matters of current interest. It is not intended as legal advice. Readers should not act upon the information contained in it without professional counsel.

This document may be considered attorney advertising in some jurisdictions.

© 2024 THOMPSON HINE LLP. ALL RIGHTS RESERVED.