Louisville Businesses Must Prepare for New Data Privacy Obligations Effective January 2026

Dalton Cline

On April 4, 2024, Gov. Andy Beshear signed the Kentucky Consumer Data Protection Act (KCDPA, codified at KRS §§ 367.3611 to 3629) into law, making Kentucky the 15th state to pass comprehensive consumer data privacy legislation. Indiana passed a nearly identical Consumer Data Protection Act (ICDPA, codified at Ind. Code § 24-15-1-1 to 24-15-11-2)) last year, which, like the KCDPA, goes into effect Jan. 1, 2026. Although data privacy laws have been proliferating around the country since the passage of the California Consumer Privacy Act in 2018, the growing patchwork is now directly applicable to non-exempt for-profit organizations doing business in Kentucky and Indiana that process the personal data of consumers. Covered businesses in Louisville now have a little more than a year to comply with the requirements imposed by these laws.

Both laws apply to any non-exempt "person that conducts business" in the state or that produces products or services "targeted to residents" of the state, and either 1) processes the data of over 100,000 "consumers" or 2) processes the data of 25,000 "consumers" and derives 50% of its revenue from the "sale" of data. Kentucky and Indiana join the minority of jurisdictions in defining "sale" as "the exchange of personal data for monetary consideration by a controller to a third party."

As with the seventeen other comprehensive state consumer privacy laws, the KCDPA and ICDPA offer numerous entity and data exemptions. Governmental entities, financial institutions, Health Insurance Portability and Accountability Act (HIPAA) covered entities, nonprofits, higher education institutions, small telephone utilities and insurance fraud organizations are among the exempt entities. In addition, certain data, such as data regulated under another major federal privacy law like the Health Insurance Portability and Accountability Act (HIPAA), Fair Credit Reporting Act (FCRA), Family Educational Rights and Privacy Act (FERPA), Gramm-Leach-Bliley Act (GLBA), Driver's Privacy Protection Act, and Farm Credit Act; or employee data, public utility data, and, under the KCDPA, data collected and used "for purposes of federal policy under the Combat Methamphetamine Epidemic Act of 2005" are exempt.

Large businesses in Kentucky and Indiana may already be subject to the comprehensive consumer data privacy laws of other states, and thus already have in place many of the processes and policies necessary to be compliant with these new laws. For businesses that do not fall under an entity exemption or do not already comply with other state data privacy laws, here is what you need to know.

Key Business Responsibilities

Under the new laws, covered businesses will have five key responsibilities: 1) effectuate consumer rights requests, 2) provide a privacy notice with required content, 3) adopt personal data processing principles, 4) execute contracts with third-party processors providing services to the business that have required language, and 5) conduct a data protection impact assessment prior to certain processing activities.

The Indiana or Kentucky Attorney General, as applicable, has exclusive authority to enforce their respective state's law. A covered business must be given notice of alleged violation and provided a 30-day cure period. Uncured violations may lead to damages of up to $7,500 per violation.

Consumer Rights

The KDCPA and ICDPA grant rights to "consumers," i.e., natural persons acting in a personal, individual or household capacity. The law doesn't give rights to persons acting in an employment or commercial capacity. Additionally, recall that that certain types of data are exempt from coverage, like data regulated under another federal privacy law such as HIPAA.

Where applicable, consumers must be given the following rights: Right of Access, Right of Correction, Right of Deletion, Right of Data Portability, Right to Opt-Out, and the Right to Appeal the denial of a consumer rights request. A covered business must also have the consumer's "opt-in" to process "sensitive" personal data.

Those data elements constituting "sensitive" personal data are statutorily defined in KRS § 367.3611(28) and Ind. Code § 24-15-2-28. Although there are slight differences in the definition, "sensitive" personal data includes indicating or revealing racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation or citizenship or immigration status, biometric identifiers, data collected from an individual the business knows is under the age of 16 and "precise" geolocation.

A covered business must respond within 45 days of receipt of a data subject request. This response can either be a substantive response to the request or a notice that the business has received the request and will respond in an additional 45 days and give an explanation for the delay.

Privacy Notice

Covered businesses must post a privacy notice that includes:

- The purposes for processing personal data.
- How consumers may exercise their consumer rights, specifically including the right to appeal.
- The categories of personal data the business shares with "third parties."
- The categories of "third parties" with whom the business shares personal data.
- A clear and conspicuous disclosure of whether the business sells personal data to third parties or processes personal data for "targeted advertising."

The KDCPA and ICDPA define "third parties" as a "natural or legal person … other than the consumer, controller, processor, or an affiliate of the processor or the controller." Therefore, a covered business is not required to disclose the categories of third-party service providers who qualify as a "processor," although they are free to do so voluntarily.

Adoption of 'Processing Principles'

The new laws require covered businesses to:

- Limit data collection to what is adequate, relevant and reasonably necessary to the disclosed processing purpose.
- Limit data processing to what is reasonably necessary and relevant to the disclosed processing purpose.
- Establish, implement and maintain reasonable and administrative, technical and physical data security practices to protect the confidentiality, integrity and accessibility of personal data appropriate to the volume and nature of that data.
- Not deny a good or service or charge a difference price or rate if a consumer exercises one of their rights.

Data Protection Impact Assessment

A data protection impact assessment must be conducted before processing "sensitive" data, or prior to processing personal data where the purpose is for targeted advertising, is a "sale," or presents a reasonably foreseeable risk of harm. This assessment must:

- Identify benefits that may flow from the processing to the business, consumer, other stakeholders and public.
- Identify potential risks to the rights of the

(continued on next page)

(continued from previous page)

consumer.

- Identify safeguards that can be employed by the controller to reduce the risk (such as de-identified data).
- Characterize the context of the processing, such as the relationship between the controller and the consumer.
- Weigh the benefit against the mitigated risk and consumer expectations.

Contracts with Third Parties

The new privacy laws require a covered business to execute contracts containing statutorily required language with processors and third parties receiving "de-identified" data.

A contract between a covered business that is a "controller" and their "processor" must:

- Require every person processing personal data to be subject to a duty of confidentiality,
- Require the processor to return or delete all personal data at the end of the contract, unless retention is required by law,
- Require the processor to make available all information necessary to demonstrate the processor's compliance with its obligations,
- Either allow and cooperate with the controller's assessments, or the assessment of a qualified and independent assessor, to demonstrate adequate physical, administrative and technological controls,
- Require the processor to execute a written contract with any subcontractor engaged to process the controller's data that passes down all the above obligations.

A covered business disclosing de-identified data must contractually obligate any recipients of the de-identified data to comply with the KDCPA or IDCPA.

Next Steps

First, determine whether your business meets the jurisdictional threshold under either the KDCPA or ICDPA to be a covered business.

Second, bring together institutional stakeholders that understand the organizational makeup of your business and can help identify where the personal data of consumers is being processed. Although the marketing department may be an easily identifiable risk area, what about the use of historic data by the IT department in test environments? Is there a consumer-facing sales department? Does your business operations center run the customer loyalty program, or receive feedback messages through an email inbox or webform from customers? Learning about each department's collection and use of data will help your organization as it moves toward compliance with the KCDPA and IDCPA.

Third, to the extent your business hasn't already, adopt the required processing principles in your business operations, start amending contracts with third-party service providers, adopt a consumer rights request and data protection impact assessment process and update your online privacy notice.

Conclusion

Because the journey to compliance can be long, covered businesses should begin preparing for the impact of these new laws on their collection, storage and dissemination of consumer data now. Partnering with experienced third parties, whether they be technology vendors or outside counsel, can ensure that the road to compliance with the KCDPA and ICDPA is not just a box ticking exercise, but an investment that protects and increases the value of the personal data the organization holds.

Dalton Cline is an associate at Dentons Bingham Greenebaum in the Data Privacy and Cybersecurity Group. As a Certified Information Privacy Professional (CIPP/US, CIPM, CIPT), Dalton advises clients on a wide range of state and federal privacy and security laws. He graduated from the University of Louisville Brandeis School of Law in 2022 and worked as a privacy analyst for the University of Illinois Urbana Champaign prior to joining Dentons. ■

The LBF Gratefully Recognizes its Foundation Partners for 2024

THE LOUISVILLE BAR FOUNDATION

In 2024, the Louisville Bar Foundation will award more than $175,000 in grants to local non-profits for law-related projects. The LBF is grateful for the generous support from all the attorneys who made this possible and recognizes its 2024 Foundation Partners — those law firms and corporate law departments (with five or more attorneys) where 100% of members made a financial gift to the Foundation to support its grantmaking activities. The combined support from the attorneys represented by these Foundation Partners totals more than $30,000. The generosity of the Foundation Partners and other individual LBA member attorneys makes it possible for the LBF to support and improve legal services for the poor, law-related public education and our judicial system.

The LBF thanks those generous Foundation Partners listed below. For more information about how you can become a Foundation Partner, please contact Jeffrey A. Been at (502) 292-6734 or *jbeen@loubar.org*.

Applegate Fifer Pulliam
Bahe Cook Cantley & Nefzger
Bardenwerper Talbott & Robert
Barnes Maloney
Dentons Bingham Greenebaum
Boehl Stopher & Graves
Dinsmore & Shohl
Frost Brown Todd
Gray Ice Higdon
Kaplan Johnson Abate & Bird
LG&E and KU Energy
McBrayer
O'Bryan, Brown & Toner
Phillips Parker Orberson & Arnett
Stites & Harbison
Stoll Keenon Ogden
Tachau Meek
Thomas Law Offices
Thompson Miller & Simpson
Wyatt, Tarrant & Combs
YUM Brands/KFC