HINSHAW

Alerts

Q&A: How Businesses Must Comply with New Kentucky and Nebraska Privacy Laws

April 23, 2024

Kentucky

On April 4, 2024, Kentucky joined the growing number of states to enact data privacy legislation, becoming the third state to do so in 2024 and the fifteenth state overall at the time of enactment.

Who Does the KCDPA Apply to?

Similar to the Virginia Consumer Data Protection Act (VCDPA), Kentucky's Consumer Data Protection Act (KCDPA) applies to:

- Persons who conduct business that produce products or services that are targeted towards the state's residents; or
- That handle the personal data of at least 100,000 consumers; or
- That handle the personal data of at least 25,000 consumers and derive over 50 percent of gross revenue from the sale of personal data.

Does Your Business Fall Within an Exception?

The KCDPA provides some familiar exemptions that other states have also exempted from coverage:

- Gramm-Leach-Bliley Act (GLBA) (entity level exception);
- Applicant and employee personal data;
- Business-to-business personal data;
- Non-profits; and
- There are also data-level exemptions for protected health information and personal data collected, processed, sold, or disclosed by a consumer reporting agency under the Family Educational Rights and Privacy Act (FERPA).

Which Key Provisions Should My Business Look Out For?

Data Retention and Data Disposal

Limit the collection of personal data to what is adequate, relevant, and reasonably necessary. In other words, covered entities that have not

Attorneys

Cathy Mulrow-Peattie

Jason J. Oliveri

Service Areas

Privacy, Security & Artificial Intelligence

already implemented a data retention and disposal policy will need to do so in order to comply with the Act's data minimization requirement.

Data Security

Covered entities will need to develop written policies, procedures, and practices to safeguard personal data against unauthorized access and theft. Administrative safeguards include things like password policies and employee background checks.

The statute is specific, and the technical safeguards involve using technology-based measures to control access, such as firewalls and data encryption, whereas physical safeguards include things like visitor management and fire suppression systems.

Sale of Personal Data

Like the other comprehensive privacy laws, you must disclose to consumers if you sell personal data, where "sale" means an exchange of monetary compensation, or if you engage in targeted advertising and provide a mechanism to opt out.

Do not Process "Sensitive Data" Without the Consumer's Expressed Consent

"Sensitive data" includes information about a consumer's race, religious beliefs, sexual orientation, biometric data, precise geolocation, and the personal data of a known child 18 years or younger.

Data Protection Impact Assessments (DPIAs)

Covered entities should conduct data protection impact assessments (DPIAs) on the processing of personal data generated on or after June 1, 2026, that presents a heightened risk of harm to consumers.

Universal Opt Out

In a departure from its sister states, the Kentucky law does not require a universal opt-out mechanism.

How and When is the Act Enforced?

The KCDPA does not go into effect until **January 1, 2026.** The Kentucky Attorney General will enforce the Act, and violators could face fines of up to $7,500 per violation. There is no private right of action, and there is a 30-day cure period prior to an enforcement action.

Nebraska

Nebraska's Legislative passed the Nebraska Data Privacy Act (NEDPA), which is now waiting for Governor Pillen's signature.

Who Would the NEDPA Apply to?

The law has broad applicability and applies to a person who:

- Conducts business in this state or produces a product or service consumed by residents of this state; or
- Processes or engages in the sale of personal data.

Does Your Business Fall Within an Exception?

Key exemptions where the law does not apply include:

- Small businesses under the federal Small Business Act;
- Applicant or employee or business-to-business personal data;
- Nonprofits;
- Gramm-Leach-Bliley Act (GLBA) (entity level exception);
- There are also data level exemptions for protected health information, Family Educational Rights and Privacy Act (FERPA)-related data, and personal data collected, processed, sold, or disclosed by a consumer reporting agency.

Which Key Provisions Should my Business Look out For?

Sensitive Data

NEDPA's definition of Sensitive Data is more limited than other states.

Data Protection Impact Assessments (DPIAs)

The NEDPA requires that a controller conducts a data protection impact assessment on personal data for purposes of targeted advertising, the sale of personal data, and the processing of personal data for purposes of profiling.

Interestingly, the NEDPA requires controllers to factor into the assessment the use of deidentified data, the reasonable expectations of consumers, the context of the processing, and the relationship between the controller and the consumer whose personal data will be processed, all critical provisions to a data impact assessment.

The data protection impact assessment can be requested for review by the NE Attorney General, and it would not be considered a waiver or work product or attorney-client privilege to produce it.

Pseudonymous and Deidentified Data

A controller that discloses pseudonymous data or deidentified data is required to exercise reasonable oversight to monitor compliance with any contractual commitments to which the pseudonymous data or deidentified data is subject and shall take appropriate steps to address any breach of the contractual commitments.

The NEDPA has provisions consistent with other state privacy laws on data subject access rights, consent for the use of sensitive data, service provider contracts, and security requirements.

How and When Would the Act Be Enforced?

The NEDPA would take effect on **January 25, 2025**.

The law is enforced exclusively by the Nebraska Attorney General's office. Civil penalties are $7500 per violation, and the Attorney General can request attorney's fees. There is a permanent 30-day right to cure prior to an enforcement action and no private right of action.

With the 17 state comprehensive laws in place and counting, please reach out to us to help navigate a risk-based approach to data privacy compliance.

Law clerk Sabrina Messar contributed to this post. She is not currently admitted to practice law.