Articles + Publications | April 26, 2024

Nebraska Enacts Comprehensive Privacy Law

WRITTEN BY

Kim Phan | Susie Lloyd | Laura Hamady

On April 12, Nebraska Governor Jim Pillen signed Legislative Bill 1074 into law, making Nebraska the 16th U.S. state to enact a comprehensive privacy law. The Nebraska Data Privacy Act (NEDPA) will take effect on January 1, 2025. Nebraska's law largely mirrors the Texas Data Privacy and Security Act, with some exceptions around required consumer disclosures.

Applicability

The law applies to persons that conduct business in Nebraska or produce products or services targeted at Nebraska residents. It also applies to persons that process or engage in the sale and processing of personal data. Finally, the law applies to any entity not classified as a small business under the Federal Small Business Act, including those that process or sell data. A business qualifies as a "small business" under the act if it employees fewer than 500 people. This approach aligns closely with Texas' data privacy law, marking a departure from the volume and revenue-based thresholds seen in most other states, including New Hampshire, Connecticut, and Maryland.

Exemptions

Like most other comprehensive U.S. state privacy laws, the NEDPA offers certain entity-level exemptions and excludes employee and business-to-business-level personal data. For example, these exemptions include entities subject to Title V of the Gramm-Leach-Bliley Act, nonprofit organizations, institutions of higher education, and state agencies or political subdivisions of Nebraska. Additionally, the law provides data-level exemptions, such as protected health information under HIPAA.

Consumer Rights

The new law provides consumers with a range of comprehensive rights. These include the right to verify if a controller is processing their personal data; the right to rectify inaccuracies; the right to erase personal data; the right to receive a portable and easily usable copy of personal data; and the right to opt out of data processing for targeted advertising, personal data sales, or profiling that solely results in automated decisions with legal or similarly significant implications.

Controller and Processor Obligations

In line with other comprehensive state privacy laws, Nebraska will require that controllers: (1) to recognize universal opt-out mechanisms such as the Global Privacy Control (GPC); (2) only collect data that is adequate,

relevant, and necessary as defined by the law; (3) conduct data protection assessments for any processing activities that involve personal data and present a heightened risk of harm to the consumer, including targeted advertising, the sale of personal data, processing sensitive personal data, or certain profiling; and (4) provide an accessible and clear privacy notice to consumers explaining the purpose of the data collection, how a consumer may exercise his or her rights under the law, and the categories of data being collected.

Under the new law, sensitive data is defined to encompass data revealing racial or ethnic origin, religious beliefs, mental or physical health condition or diagnosis, sex life, sexual orientation, or citizenship or immigration status; the processing of genetic or biometric data for the purpose of uniquely identifying an individual; personal data collected from a known child (under 13 years of age); or precise geolocation data.

A key provision in the law requires controllers to secure a consumer's opt-in consent before processing sensitive data. The law recognizes that advances in technology have created an online environment where consumers can be misled into consenting to the release of sensitive personal information. To counter this, the law specifies that "[a]cceptance of a general or broad term of use or similar document containing a description of personal data processing," or "hovering over … a given piece of consent," does not constitute "consent" under the statute. The law also excludes consent obtained using dark patterns, website design practices that manipulate a consumer into relinquishing rights to personal data.

Enforcement

The NEDPA is enforceable by the Nebraska attorney general (AG) but specifies that before enforcing any alleged violation of the law, the AG "shall" provide notice and offer a 30-day period to cure the alleged compliance violation. Statutory penalties up to $7,500 per violation may be imposed by the AG for noncompliance. The law does not provide a private right of action.

Practice Tips

- Many companies will likely be covered by the Nebraska law. If your organization is not taking a one-size-fits-most approach to honoring data subject rights' requests, evaluate whether your company falls within the small business exemption as a company with fewer than 500 employees, and whether your organization qualifies for an entity-based exemption.
- If your organization has not implemented a privacy risk-assessment procedure to ensure potentially high-risk processing activities are subject to a data protection assessment, consider designing and implementing this process now. Of the 16 states that have enacted privacy legislation, only two states *do not* require controllers to conduct risk assessments for certain types of processing such as engaging in targeted advertising or selling personal data (which are sometimes the same thing).
- Review your current data practices, including data collection, processing, and sharing activities, to ensure compliance with the law's requirements. This includes minimizing data collection to only what is necessary, securing affirmative consent before processing sensitive data, and not using collected data for purposes other than those initially stated without additional consent.

RELATED INDUSTRIES + PRACTICES

- Business Litigation
- Privacy + Cyber