Hüskers Dü Privacy

On April 17, Nebraska Governor Jim Pillen signed into law the Nebraska Data Privacy Act (the Act), making Nebraska the seventeenth state to enact general consumer data privacy legislation. The Act largely, but not completely, tracks the Texas Data Privacy and Security Act (TDPSA), which was signed into law last June. The Nebraska Act will take effect **January 1, 2025**.

Threshold Requirements and Exemptions

Whereas most prior state privacy laws have limited their applicability to legal entities that process the personal data of a large number of individuals or obtain significant revenue from the sale of personal data, the Act mirrors the TDPSA's applicability standards and applies to any person that meet the following criteria:

1. Conducts business in Nebraska or produces a product or service consumed by residents of Nebraska.
2. Processes or engages in the sale of personal data.
3. Is not a small business as defined by the United States Small Business Administration (SBA).

The Act requires small businesses to obtain consumer consent prior to selling personal data, despite not falling into the applicability standards above. The Act also contains typical exemptions seen in other states' laws, including entity exemptions for nonprofit organizations, Gramm–Leach–Bliley Act (GLBA) financial institutions (both entity and data level), institutions of higher education, and HIPAA-covered entities and business associates. The Act also contains data level exemptions generally seen in other states' laws, including PHI and data controlled or processed in compliance with the Family Education Rights and Privacy Act (FERPA), the Farm Credit Act (FCA), the Fair Credit Reporting Act (FCRA), or the Driver's Privacy Protection Act. Like other privacy statutes, the Act does not cover personal data relating to employment or contracted services.

As with the TDPSA, and unlike other privacy laws, the Act is not focused on whether a business is targeted at Nebraska residents but rather whether any services or products are consumed by a resident of Nebraska. The second standard — whether the person or business engages in the "**processing** or **sale** of personal data" — further expands the applicability of the Act to include individuals and businesses that engage in any operations dealing with personal data, such as the "collection, use, storage, disclosure, analysis, deletion, or modification of personal data." In short, collecting, storing or otherwise handling the personal data of any resident of Nebraska, or transferring that data for any consideration, will likely meet this standard. The third standard allows for an exemption for businesses that meet the SBA definition of a "small business." Consider using the SBA's resources linked here to determine if your business may meet the definition.

Universal Opt-Out Mechanisms

The Act also follows other states in requiring controllers to recognize universal opt-out mechanisms (UOOMs) used by consumers to opt out of the sale of their personal data or the use of such data for targeted advertising. The Act, however, only requires entities to recognize UOOMs if the relevant entity is already processing such requests to comply with another state's privacy law. Furthermore, and unlike the TDPSA, the Act does not appear to include a delayed effective date for recognizing UOOMs, so entities should be ready to begin complying with requests when the Act takes effect on January 1, 2025 (if not already required to do so under other state laws).

Consumer Rights

The Act provides consumers with many of the same standard rights regarding personal data as provided under other recent state law frameworks (and is identical to TDPSA):

- The **right to know** whether a controller is processing the consumer's personal data.
- The **right to receive a portable copy**, in digital format, of the consumer's personal data processed by the controller.
- The **right to request deletion** of personal data provided by or obtained about the consumer.
- The **right to request a correction** of inaccurate personal data.
- The **right to opt out** of sales of personal data, targeted advertising, and profiling in furtherance of a decision that produces a legal or similarly significant effect concerning the consumer.
- The **right to appeal** any refusal to take action on any of the above requests.

Controller Obligations

Like the TDPSA, the Act requires controllers to comply with certain obligations, including practicing data minimization (only using personal data as reasonably necessary), avoiding secondary uses, and undertaking a "Data Protection Assessment" prior to any processing that involves:

- The processing of personal data for the purpose of targeted advertising or profiling "if the profiling presents a reasonably foreseeable risk of: unfair or deceptive treatment of, or unlawful disparate impact on, consumers; financial physical, or reputational injury to consumers; a physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of consumers if the intrusion would be offensive to a reasonable person; or other substantial injury to consumers."
- The selling of personal data.
- The processing of sensitive data.
- Any processing activity that involves personal data that presents a heightened risk of harm to consumers.

Additionally, a controller that is in possession of "deidentified" or "pseudonymous" data should take reasonable measures to ensure that the data cannot be associated with an individual, in addition to publicly committing to not re-identify the data. The controller also must contractually obligate any recipient of the deidentified data to comply with the terms of the Act.

Furthermore, the Act requires that controllers maintain both Data Processing Agreements and Privacy Policies. As with the TDPSA, the Act requires controllers to obtain consumer consent before processing sensitive personal data. Unlike under the TDPSA, however, controllers are not required to specify whether they sell sensitive personal data and/or biometric data.

The Act is also missing specific provisions regarding children's data and does not specify whether consent can be later revoked by consumers.

Enforcement

The Act will be solely enforceable by the Office of the Nebraska Attorney General and explicitly excludes any private right of action. The Act contains a 30-day right to cure upon notice that a

controller is in violation of the statute, and like the TDPSA, this right to cure does not sunset. The Act also expressly states that the Act does not provide a private right of action.

Notable Date

- **January 1, 2025:** The Act goes into effect, and controllers must begin recognizing UOOMs.

Our team will continue to monitor the Act. If you have any questions about the Act or any other state or international privacy laws and how they could affect your business, please contact the authors.