HINSHAW

Alerts

Lucky Number 13: What to Look Out For in New Jersey's Data Protection Law

January 24, 2024
Privacy, Cyber & AI Decoded

On January 16, 2024, New Jersey's Governor Murphy signed New Jersey's comprehensive state privacy law. New Jersey is the thirteenth state to adopt comprehensive consumer privacy protections.

With Congress unlikely to pass a federal law granting similar protections for consumers this year, the growing number of states enacting their own laws makes compliance obligations for businesses ever more complex. Soon, you will hear from us about New Hampshire's new privacy law, which is waiting for signature before Governor Sununu.

Who Does the Law Apply to?

The applicability of the statute is similar to other state privacy laws. It applies to entities doing business in New Jersey or that produce products or services that are targeting New Jersey consumers that:

> (1) control or process the personal data of at least 100,000 New Jersey residents, or
>
> (2) process the personal data of at least 25,000 New Jersey residents and derive revenue or provide a discount from/for the sale of personal data.

Sale of personal data is defined, similar to the CCPA, as monetary and other valuable consideration. The law applies to the personal data of consumers and households in New Jersey.

Does Your Business Fall Within an Exception?

- New Jersey's law contains an exception for employment, business-to-business data, and nonprofits.
- It has exceptions for organizations otherwise regulated under:
  - HIPPA (data related exception)
  - GLBA
  - As an insurance institution under PL 1985, C. 179
  - For personal data processed under FCRA by a consumer reporting agency

Attorneys

Cathy Mulrow-Peattie

John P. Ryan

Service Areas

Privacy, Security & Artificial Intelligence

Key Provisions to Look Out for:

- **Updates to Your Privacy Notice**: Similar to other state data protection laws, businesses must list out the categories of personal data they share with third parties. Specifically, if a business processes personal data for targeted advertising, a sale of personal data for profiling related to the provision or denial of financial or lending services, housing, insurance, education enrollment or opportunity, health care, or access to essential goods and services (e.g., profiling in the furtherance of decisions that produce legal or similarly significant effects) then the business must clearly disclose such sale or processing in its privacy notice and provide the consumer with the right to opt-out.
- **Data Subject Access Rights**: Similar to other state data protection laws, businesses must ensure that consumers have the right to access, delete, correct, data portability, nondiscrimination, and to opt out of targeted advertising, sale of personal data, and profiling in the furtherance of decisions that product legal or similarly significant effects about the consumer. A consumer has the right to appeal these actions.
- **Sensitive Personal Data**: There is an expansive definition of sensitive personal data, which includes financial information and precise geolocation data. The use of this sensitive data by a business requires opt-in consent.
- **Vendor Contracts**: Once again contracts with vendors (data processing agreements) are required to limit the use and processing of the consumer's personal data. Interestingly, vendors are required to delete personal data at the end of the services received from a business unless it can be retained by applicable law.
- **Data Protection Assessments**: Businesses which have not yet implemented a data protection assessment process should prioritize this process in early 2024. New Jersey follows other, in effect, state laws (and federal guidelines) that require data protection assessments for use cases and projects that have a heightened data protection risk of harm. Under this law, the definition of a heightened risk of harm is broad and includes targeted advertising, profiling, selling personal data, and processing sensitive data.
- **Universal Opt-Out:** Six months after the effective date, the statute will require applicable businesses that sell personal data or engage in targeted advertising to allow consumers to exercise the right to opt out of processing through a "universal opt-out mechanism[s]." Implementation of universal opt-out mechanisms should be on businessess' technology plans this year as California already has similar requirements in place, and Colorado's CPA similar requirement is effective as of July 1.
- **Data Security**: The law sets out requirements for data security for businesses' supply chain, ensuring that these businesses establish, implement, and maintain administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data and to secure personal data during both storage and use from unauthorized acquisition. The data security requirements cover both businesses, their vendors, and their vendors' subcontractors.

Enforcement

We expect the law to be actively enforced by the New Jersey Attorney General, given that historically, the New Jersey Attorney General's office has been active in the investigation and enforcement of privacy violations.

The Lucky 13 good news is that there is a 30-day cure period for organizations for violations of the law that will extend for 18 months after the January 15, 2025 effective date, and that there is no private right of action.