wiley

ALERT

State Privacy Update: New Jersey Becomes 13th State to Pass a Consumer Privacy Bill

January 12, 2024

The New Jersey Legislature this week passed Senate Bill 332 (SB 332), a comprehensive consumer data privacy bill. Since its conception, the bill has undergone significant revisions that expanded a once narrow bill into a more comprehensive privacy framework. The bill, approved by the legislature on January 8, now awaits final action from Governor Phil Murphy. It will take effect one year after enactment.

While many provisions of this bill track the obligations of existing privacy laws, New Jersey added unique twists to several key provisions. Notably, SB 332 contains some novel definitions, broad rulemaking authority, provisions for universal opt-out mechanisms (UOOMs), and unique children's privacy provisions. Below we highlight those key provisions and differences.

Scope. Once enacted, the law will apply to data controllers conducting business in New Jersey or targeting consumers who are state residents, and that either (1) control or process the data of at least 100,000 consumers, or (2) control or process data of at least 25,000 consumers and derives revenue, or receives a discount on the price of any goods or services from the sale of personal data. The law will not apply to employee or B2B data.

Definitions. The bill contains several unique definitions.

- *Biometric Data:* Includes physical and behavioral characteristics in addition to biological characteristics; data generated by "technological processing" or "analysis"; and specific references to facial mapping, facial geometry, and facial templates.

Authors

Joan Stewart
Partner
202.719.7438
jstewart@wiley.law

Kathleen E. Scott
Partner
202.719.7577
kscott@wiley.law

Kimberly S. Alli
Associate
202.719.4730
kalli@wiley.law

Practice Areas

Privacy, Cyber & Data Governance
State Privacy Laws

- *Sale:* Does not include all of the exceptions to a sale that are found in many other privacy laws, including importantly when the consumer directs the disclosure or uses the Controller to engage with a third party.
- *Sensitive Data:* Includes (1) financial information, defined as a consumer's "account number, account log-in financial account, or credit or debit card number, in combination with any required security code, access code, or password that would permit access to a consumer's financial account"; (2) "mental or physical health condition, treatment or diagnosis"; and (3) "status as transgender or non-binary."

The law also includes certain unique definitions not found in other privacy laws, such as a "designated request address" and "verified request."

Consumer Rights. The law creates several consumer rights consistent with those found in other state privacy laws including:

- The right to know;
- The right to correct;
- The right to delete personal data concerning the consumer;
- The right to data portability; and
- The right to opt out of processing of personal data for the purposes of targeted advertising, sale of personal data, or profiling.

The law does not provide additional rights with respect to third parties, nor does it contain an exemption for pseudonymous data.

Universal Opt-Out Mechanisms. Similar to Colorado, Connecticut, Montana, Oregon, Delaware, Texas, and Washington, the New Jersey law requires controllers to recognize UOOMs no later than six months after the law's effective date. The requirement extends to targeted advertising and sale of personal data.

Rulemaking Authority. Similar to California and Colorado, the law contemplates the initiation of rulemakings to develop implementing regulations. Specifically, the Director of the Division of Consumer Affairs in the Department of Law and Public Safety is tasked with adopting rules and regulations to "effectuate the purposes of this bill." This includes rules that detail the technical specifications for one or more UOOMs.

Children's Data. The law adds unique restrictions to the processing of children's data. It requires opt-in consent to sell, process for purposes of targeted advertising, or engage in profiling in furtherance of decisions that produce legal or similarly significant effects for a child between the ages of 13-17. Notably, New Jersey is the first state to include restrictions on the processing of children's data that includes *both* an opt-in requirement for profiling and applies to minors up to the age of 17.

Data Protection Assessments. Controllers will be required to conduct a data protection assessment prior to engaging in any processing that "presents a *heightened risk of harm* to a consumer." (emphasis added).

Enforcement and Implementation. The New Jersey Attorney General has sole authority to enforce this law. After receiving a notice of violation, companies have a 30-day cure period to fix any violations, after which the AG may bring an enforcement action. The cure period expires 18 months after the law's effective date.

***

Wiley's Privacy, Cyber & Data Governance team has helped entities of all sizes and sectors proactively address risks and compliance with the increasingly complex patchwork of federal and state privacy and cyber laws. Please reach out to any of the authors with questions.