New Jersey, New Privacy Law

On January 16, New Jersey joined the list of states with comprehensive consumer privacy statutes when Governor Phil Murphy signed into law Senate Bill 332 (the New Jersey Data Privacy Act or NJDPA). The bill has undergone major revisions since passing in the Senate in early 2023 but contains many of the terms commonly included in other recently enacted consumer privacy laws. The New Jersey Data Privacy Act will take effect on **January 15, 2025**. Below, we discuss the overall framework of the NJDPA and highlight some notable differences from popular consumer privacy law models.

Threshold Requirements and Exemptions

The NJDPA mirrors a common applicability standard for many consumer privacy laws by applying to "controllers," i.e., any persons or entities that conduct business in the State of New Jersey or produce products or services that are targeted to residents of the state *and*, during the preceding calendar year, controlled or processed the personal data of either:

100,000 consumers.

25,000 consumers *and* derives revenue or receives a discount on the price of any goods or services from the sale of personal data.

"Consumer" is defined exclusively as an "identified person who is a resident of New Jersey acting only in an *individual or household context*." It thus excludes employee and contractor information. The NJDPA also excludes personal data controlled or processed solely for the purpose of completing a payment transaction from its threshold requirement.

NJDPA exemptions are narrower than exemptions in many other states' laws. While the NJDPA contains some typical exemptions for Gramm–Leach–Bliley Act (GLBA) financial institutions (both entity and data level), state agencies and related institutions, and an exemption for protected health information under HIPAA, it does *not* contain a broad covered entity or business associate entity exemption. Unlike many other privacy laws, the NJDPA also does not contain exemptions for nonprofits, institutions of higher education, or any Family Educational Rights and Privacy Act (FERPA) exemptions. It also does not contain an exemption for pseudonymous data.

Treatment of Children's Data and Sensitive Data

Many recently enacted state privacy laws have prioritized protecting children's data, including requiring consent for certain types of processing of data relating to children. The NJDPA contains

language, similar to other state laws, prohibiting controllers from selling personal data, processing data for targeted advertising, or using the data for profiling in furtherance of decisions that produce legal or similarly significant effects concerning a consumer without the consumer's consent under circumstances where a controller has actual knowledge, or willfully disregards, that the consumer is at least 13 years of age but younger than 17 years of age. Notably, New Jersey is the first state to include restrictions on the processing of children's data that include *both* an opt-in requirement for profiling and apply to minors up to the age of 17.

Another notable difference is the NJDPA's definition of "sensitive data." The NJDPA has several additions to its definition of sensitive data that make it unique. Namely, the definition includes "financial information," similar to the California Consumer Privacy Act (CCPA) and 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." The CCPA, however, only requires the right to opt out and does not require consent in order to process such financial information.

The NJDPA's definition also includes "mental or physical health condition, treatment or diagnosis" and "status as transgender or non-binary," which have been included in definitions under other recent state privacy laws like Delaware and Oregon. The NJDPA requires consent for a controller to process any sensitive data (or a parent's consent, in the case of a known child under the age of 13), which makes New Jersey the first state to require consent in order to process financial information.

Universal Opt-Out Mechanisms

The NJDPA also joins the list of laws that require 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. UOOMs include browser settings that notify websites that the user has opted out of such uses of personal data. Controllers have until July 15, 2025, to meet this requirement, which extends to both targeted advertising and sales of personal data. The NJDPA also authorizes the New Jersey Division of Consumer Affairs in the Department of Law and Public Safety to adopt rules and regulations that detail the technical specifications for one or more UOOMs, including any regulations permitting authentication of the requests by controllers.

Consumer Rights

The NJDPA provides consumers with many of the same standard rights regarding personal data as provided under other recent state law frameworks, including:

The right to **access** personal data processed by a controller.

The right to **correct** inaccuracies in the personal data.

The right to **delete** the personal data concerning that consumer.

The right to **obtain** a copy of the data retained by a controller in a portable data format.

The right to **opt out of** targeted advertising, sales of personal data, and profiling "in furtherance of decisions that produce legal or similarly significant effects concerning the consumer."

Additionally, under the NJDPA, consumers can transfer their respective "opt out rights" to another person. That person will be considered an "authorized agent" and can act on the consumer's behalf to opt out of the processing and sale of the consumer's personal data. Unlike other state privacy laws passed last year, the NJDPA provides no additional rights with respect to third parties.

Data Protection Assessments

The NJDPA requires controllers to undertake 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 or physical 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.

Enforcement

The NJDPA will be solely enforceable by the Office of the New Jersey Attorney General and explicitly excludes any private right of action. The NJDPA contains a 30-day right to cure upon notice that a controller is in violation of the statute. This right to cure sunsets, however, on July 15, 2026, 18 months after the NJDPA's effective date. The Director of the Division of Consumer Affairs in the Department of Law and Public Safety is required to promulgate rules and regulations necessary to "effectuate the purposes" of the NJDPA but there is currently no timeframe for when such rules and regulations must be issued.

Notable Dates

January 15, 2025: The NJDPA goes into effect.

July 15, 2025: UOOM recognition deadline.

July 15, 2026: The notice/right to cure period sunsets.

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