March 19, 2025

New Jersey Data Protection Act Went Into Effect January 15 — Is Your Company in Compliance?

The New Jersey Data Protection Act (NJDPA), enacted on January 16, 2024, just went into effect on January 15, 2025. This new law establishes comprehensive data privacy protections for New Jersey residents and imposes additional responsibilities on companies doing business in New Jersey.

New Jersey joins the ranks of 13 other states with similar laws. Navigating compliance may present challenges and requires businesses to take action.

Who needs to comply with the NJDPA?

The NJDPA applies to entities, referred to as "controllers" (including nonprofits) that either conduct business in New Jersey or offer products or services to New Jersey residents, acting only in an individual or a household context (versus in an employee or a commercial context) and meet one of the following criteria:

- Control or process the personal data of at least 100,000 consumers, excluding data controlled or processed solely for payment transactions, or
- Control or process the personal data of at least 25,000 consumers and derive revenue or receive discounts from the sale of personal data.

Unlike other state law requirements, there is no specific percentage of revenue that must be derived from the sale of data under the NJDPA.

What rights do consumers have under the NJDPA?

Consumers are granted substantial rights regarding their personal data, including the right to:

- **Access information:** Confirm whether a business is accessing or processing their personal data
- **Correct information:** Correct inaccuracies in their personal data
- **Delete information:** Request deletion of their personal data
- **Obtain a copy of information:** Obtain a copy of their personal data in a portable format
- **Opt out:** Decline the processing of their personal data for targeted advertising or profiling

Businesses are required to respond within 45 days of receipt of a consumer rights request. An additional 45-day extension may be permitted under some circumstances.

What information is considered personal data under the NJDPA? Are there exemptions?

In today's digital age, most businesses collect and process vast amounts of consumer information. However, only some categories of personal data demand heightened protection under the NJDPA. Under the law, "personal data" includes any

information that reveals an individual's race or ethnicity, religious beliefs, mental or physical health conditions, sexual orientation, citizenship status, biometric data, children's data, geolocation or financial information.

However, de-identified and publicly available information, which is not only information lawfully made available from government records but also information that the business has a reasonable basis to believe the consumer has lawfully made available to the general public, does not fall under the law's requirements.

Certain types of data are not subject to NJDPA regulations. For instance, personal information governed by federal laws such as the Health Insurance Portability and Accountability Act, Gramm-Leach-Bliley Act and Fair Credit Reporting Act is exempt. Additionally, secondary market institutions and the state's Motor Vehicle Commission fall outside the law's scope.

How do I comply with the requirements of the NJDPA?

Companies handling personal data are required to implement policies and procedures to safeguard consumer privacy and ensure transparency in their data practices. Key obligations include:

- Providing transparent privacy notices detailing data collection and processing practices
- Conducting assessments for processing activities that present a heightened risk of harm to consumers, such as targeted advertising or profiling
- Obtaining consumer consent before processing sensitive data, including health, financial and biometric data
- Reviewing agreements and relationships with third-party data processors to ensure compliance with the NJDPA
- Updating existing policies and procedures to comply with the new requirements
- Developing business processes to allow consumers to request information about their personal data
- Posting a privacy notice and link on their website that allows consumers to opt out

How is the NJDPA enforced?

Consumers do not have a private right of action under the NJDPA. Enforcement is handled by the New Jersey attorney general. Failure to comply can lead to enforcement actions under the New Jersey Consumer Fraud Act, with penalties of up to $10,000 for an initial violation and $20,000 for each subsequent violation.

How do I navigate compliance with the NJDPA?

Businesses have until 18 months after the effective date (i. e. , July 15, 2026) to comply with the NJDPA. During this transitional period, the New Jersey Attorney General may provide a 30-day notice and cure period for violations before enforcement actions commence. For businesses handling sensitive consumer data, understanding and adhering to the NJDPA is essential. Given the 18-month grace period, now is the best time to conduct a comprehensive review of data privacy policies, internal procedures and third-party vendor agreements to ensure compliance.

If you have questions about your obligations under the NJDPA, the experienced attorneys at Day Pitney are here to help. We can guide you through the complexities of data privacy law, ensuring your business remains compliant while protecting consumers' rights. Reach out to our team today to safeguard your company against potential regulatory risks.

Authors



Fariha Syed
Associate

Parsippany, NJ | (973) 966-8193

fsyed@daypitney.com



William J. Roberts
Partner

Hartford, CT | (860) 275-0184

wroberts@daypitney.com