Kilpatrick

Insights: Alerts

New Jersey Proposes Rules for Implementing New Jersey Data Privacy Act

June 26, 2025

Written by **Meghan K. Farmer,**

The New Jersey Division of Consumer Affairs has released proposed rules to implement the New Jersey Data Privacy Act (NJDPA). For covered businesses, these proposed rules demand close attention—not only for their substantive requirements, but also for the procedural steps that must be taken in the coming months.

Public Comment Window: Act Before August 1, 2025

The Division of Consumer Affairs has provided a 60-day comment period on the proposed rules. Interested parties—including businesses, privacy professionals, and consumer advocates—must submit any written comments by August 1, 2025. After this period, a summary of public comments will be published in a Notice of Adoption and then the rules will become final.

Implementation Timeline: Prepare for Near-Term Compliance

The NJDPA became effective on January 15, 2025, and the proposed rules are designed to operationalize its key provisions. While the precise effective date of the regulations will depend on the final rulemaking process, the draft rules make clear that compliance obligations will attach as soon as the rules become effective. Notably, some provisions—including requirements related to data protection assessments—apply prospectively to processing activities initiated after the effective date of the rules. Organizations should use the comment period not only to engage with the Division, but also to begin internal compliance assessments, as the transition period may be limited, and the rules are comprehensive in scope.

Significant Compliance Impact: Heightened Standards and Broad Applicability

The proposed rules impose robust compliance obligations on both controllers and processors. Some key issues are highlighted below:

- Comprehensive Data Rights and Notice Requirements: Businesses must provide clear, accessible privacy notices before collecting personal data. If a required notice is not provided, businesses are barred from collecting personal data from the consumer.
- Prohibition of Dark Patterns and Enhanced Consent: The New Jersey rules mirror California's approach. All mechanisms for submitting data rights requests and obtaining consumer consent must avoid manipulative “dark patterns.” Consent must be a clear, affirmative act and cannot be bundled into broad

terms of use. Specific, granular consent must be obtained for processing activities unrelated to the purposes for which the data was initially collected.

- Universal Opt-Out and Swift Response: Businesses must honor user-selected universal opt-out signals (i.e., a browser setting) for the sale of data and targeted advertising. Opt-out requests must be implemented within 15 days, and businesses must notify third parties and maintain detailed records of the requests.
- Stringent Data Minimization and Security: Controllers are required to limit the collection and retention of personal data to what is adequate, relevant, and reasonably necessary in relation to the disclosed processing purposes (see related provisions above). New processing purposes require revised notice and, if not reasonably necessary or compatible, fresh consent. Controllers must implement, maintain, and document comprehensive data security measures tailored to the nature, sensitivity, and amount of data processed, and must protect against unauthorized access, loss, destruction, or damage. Controllers must also conduct periodic reviews of stored data and set reasonable retention periods.
- Special Protections for Children and High-Risk Processing: The rules impose heightened requirements for processing children's data and for processing activities that present a heightened risk of harm (such as profiling with significant effects, targeted advertising, or sale of sensitive data). Controllers with actual knowledge of processing data from children under 13 must obtain verifiable parental consent and ensure parents are notified of their opt-out rights. For processing activities that present heightened risk, controllers must conduct and document detailed data protection assessments before initiating such processing, regularly review and update these assessments, and retain them for at least three years after processing concludes.

Conclusion

The new rules impose significant operational and compliance requirements on businesses subject to the NJDPA. The next few months are critical as affected businesses should review the proposed rules, submit comments by August 1, 2025, and begin preparations for compliance now.

Related People

Meghan K. Farmer

t 404.541.6816

mfarmer@ktslaw.com