The Regulations Have Landed: A User's Guide to the New Jersey Data Privacy Act's Long-Awaited Draft Regulations

July 1, 2025

By: Alfred Brunetti

What Happened?

The New Jersey Division of Consumer Affairs has issued proposed regulations to further detail and implement the New Jersey Data Privacy Act (NJDPA)—the state's comprehensive data privacy statute which became enforceable nearly five months ago. The 44-page long draft regulatory package aims to clarify and interpret the details and terms of the NJDPA, one of the more exacting data privacy laws in the country.

The proposed regulations address key operational and definitional issues set forth in the NJDPA and drive home the complexity of the compliance concerns that all businesses should keep top of mind. The draft spans topics from how personal data is actually defined to the specificity required for privacy notices, data minimization practices, and granular restrictions on loyalty and discount programs

What Do We Need to Know?

The proposed regulations add depth to numerous important terms of the NJDPA. Among some of the most notable issues addressed in the regulations are:

- **Expanded and New Definitions:** The regulations detail the expansive nature of the NJDPA's definition of “personal data” and clarify that it expressly includes items like IP address, unique device identifiers, place of birth, “employment information,” “username, email address or other account holder identifying information” and “gender identity or expression.” Some freshly defined terms include “access request,” “data right,” “delete,” “essential goods and services,” and “loyalty program benefit.”
- **Universal Opt-Out Mechanisms:** In line with the growing number of other state laws, the NJDPA requires businesses to recognize a digital signal sent from an online visitor to opt out of targeted advertising or the sale of a user's personal data as sent from a user-selected automatic mechanism. The regulations recite and dictate the technical specifications for recognizing and addressing such a signal and address how a business must respond to it.
- **Expanded Privacy Statement Requirements:** A Privacy Statement (i.e., external facing notice frequently referred to as Privacy Policy) must now include specific descriptions of data types, as well as the purpose of processing and retention periods for each category of personal data collected and processed. Notices must also be accessible to people with disabilities, avoid legal or needlessly technical jargon, and be available in languages used to interact with consumers.
- **Loyalty and Discount Program Disclosures:** The draft requires detailed notices when a consumer provides his or her personal data in order to enter a loyalty program or receive certain discounts. A consumer must be able to withdraw

from such a program at any time, penalty free, and the program benefits must be reasonably related to the value of the personal data. If the business cannot provide or calculate such a value on a good-faith basis, it cannot offer the program.

- **Data Minimization and Retention Documentation:** Businesses must justify why each type of data collected is necessary, maintain an up-to-date inventory (including storage locations and access permissions), and document retention and deletion practices—especially for sensitive or biometric data.
- **Consent Refresh Requirements:** After a business receives consent from a consumer, businesses must refresh that consumer consent for processing sensitive data, including teen data, or to continue to process personal data for targeted advertising, profiling, or sale purposes if two years have passed since the last interaction or if the purpose of processing has materially changed.
- **Heightened Requirements for Data Protection (Impact) Assessments (DPIAs):** Businesses engaging in high-risk processing must conduct DPIAs that include a risk-benefit analysis, safeguards to mitigate identified harms, summaries of processing purposes, and retained documentation of internal review and approval.

The formal rulemaking approval and finalization process likely won't be completed until late 2025 or early 2026. Nonetheless, businesses should not delay in preparing for compliance and solidifying—or building out—the necessary data governance. The New Jersey Attorney General's Office is the sole enforcement authority, and it has made clear that it is preparing for the fulsome investigation of and enforcement against potential privacy violations. This is consistent with its strong tradition of consumer protection activity both within the state and nationally through its partnerships with other similarly minded Attorneys General.

What Do We Need to Do?

To best optimize compliance with New Jersey's data privacy statutory and likely regulatory environment, there are a number of steps businesses can take now, including:

1. **Assess Data Inventories and Data Mapping Capabilities:** Ensure that you have a clear, detailed understanding of what personal data you collect, how it is used, where it is stored, how it flows, who has access to it, and for how long it is retained. Pay special attention to the deployment of web-tracking technologies and the signal-reception functionalities of websites, applications, and other consumer-facing platforms. A cross-functional and collaborative approach here is especially important because, regardless of business size, it's become increasingly unlikely that any one person (or department) knows everything about a business's actual data activities.
2. **Review and Revisit Privacy Notices:** Update privacy notices to reflect the NJDPA's clarified and expanded disclosure requirements. Include specific data types collected, retention periods, opt-out mechanism details, and specifications on loyalty programs and consumer profiling practices.
3. **Evaluate Consent Flows:** Review the mechanisms and user experiences for obtaining and providing consent, particularly for sensitive data, children's personal data, and AI training use cases. Design a process for refreshing consent after two years of consumer inactivity or upon material changes in processing purposes.
4. **Implement Robust Data Minimization Practices:** Begin documenting the necessity of each type of data collected and establish a regular schedule to check that internal teams can justify their use of sensitive or biometric data.
5. **Audit Loyalty and Profiling Programs:** Conduct internal audits of any loyalty or automated decision-making programs to ensure full compliance with the new notice, disclosure, and value-justification requirements.

6. **Prepare for Comprehensive DPIA Procedures:** If your business engages in processing activities that touch on consumer profiling or sensitive data, consider how you will detail and address data flow factors like, e.g., what revisions may be required to address risk, safeguarding, lifecycle, and functionality.

7. **Engage in the Process:** If your business has concerns or suggestions regarding any of the proposed rules, consider working with counsel to submit comments during the public comment period, which will close on August 1, 2025.

New Jersey joins California and Colorado as the only states authorized to issue regulations to accompany their respective data privacy statutes, so it is vital for businesses operating in the state or offering products and services to its residents to familiarize themselves with the valuable insights afforded by the draft regulations and ongoing rulemaking activity. The draft regulations are open to public comment and remain a work-in-progress at least until the comment period closes on August 1, 2025.