Articles + Publications | June 10, 2025

New Jersey Releases Proposed Privacy Regulations

WRITTEN BY

Kim Phan | Joshua D. Davey | Aileen Ng | Robert Austin Jenkin, II

On June 2, the New Jersey Division of Consumer Affairs announced the publication of new proposed regulations to implement the New Jersey Data Privacy Act (NJDPA), N.J. Stat. §§ 56:8-166.4 *et seq*., which went into effect on January 15. (Please see our prior article on the NJDPA for more details.) Although many of these proposed regulations appear familiar – similar to the finalized regulations under the California Consumer Privacy Act (CCPA) and the Colorado Privacy Act (CPA) – New Jersey introduced several new requirements worth noting.

Written comments on the proposed regulations must be submitted by August 1 to the New Jersey Division of Consumer Affairs, please see instructions here. The New Jersey Attorney General's Office has exclusive authority to enforce violations of the NJDPA.

Clarifying "Personal Data"

The NJDPA is a comprehensive privacy law that grants consumers the right to confirm, correct, delete, and access their "personal data," as well as to opt out of processing for targeted advertising, sale, or profiling. The proposed New Jersey regulations clarify that "personal data" includes any information that is "reasonably linkable" to an identified or identifiable person if it can identify a person or device linked to a person when aggregated with other data, such as a person's full name, mother's maiden name, or telephone number, among other specific data elements. This appears to expand the definition to cover any information which, even if alone may not be reasonably linkable to an identified person, can be reasonably linkable to an identified person if combined with other data elements.

The regulations also include a number of new definitions for terms such as "access request," "correction request," "data broker," "data portability request," "data right," "delete," "deletion request," "essential goods and services," "loyalty program benefit," "loyalty program partner," "opt-out preference signal," and "opt-out request."

No Exemption for Data Used to Train AI for "Internal Research"

Like other state comprehensive privacy laws, the NJDPA contains express exemptions for certain entities, such as financial institutions subject to the federal Gramm-Leach-Bliley Act (GLBA); for certain categories of data, such as financial data subject to the GLBA; and other activity-based exemptions such as to comply with legal obligations and conduct internal research activities. Regarding this last exemption, the proposed regulations clarify that the statutory exemption for the processing of personal data to conduct "internal research" to develop or improve products, services, or technology expressly excludes any internal research conducted: (1) if the data or resulting research is used to train artificial intelligence (AI), unless the consumer has affirmatively consented to such use; or

(2) the data or resulting research is shared with a third party (unless it is de-identified or shared pursuant to one of the permitted exemptions, *e.g*., to comply with applicable laws). Note that the term AI is not further defined.

This exclusion could impact companies that use personal data to train internal AI systems for ordinary business purposes (unless affirmative consent is obtained from consumers). Without providing a definition for AI, this provision may cover a wide range of AI tools and technologies, from machine learning models to generative AI systems for which no personal data may be used for training, even if for internal research purposes.

Privacy Disclosures

The proposed regulations establish new requirements impacting privacy disclosures, notifications, and other communications to be provided under the NJDPA. Such privacy disclosures must be:

1. Understandable and accessible to a controller's target audience;
2. Accessible to consumers with disabilities;
3. Available in and sent to a consumer in the language in which the controller ordinarily interacts with a consumer;
4. Available through a readily accessible interface that consumers regularly use in conjunction with a controller's products or services;
5. Provided in a readable format on all devices that consumers use to regularly interact with the controller;
6. Communicated using methods the controller regularly uses to interact with consumers;
7. Accurate (not written or presented in a way that is unfair, deceptive, or misleading); and
8. Available in a format that allows consumers to print a paper copy.

In such privacy disclosures, to help consumers understand a controller's processing activities, a controller would be prohibited from specifying one broad purpose to justify numerous processing activities, from specifying one broad purpose to cover potential future processing activities, and from specifying so many purposes for which personal data could potentially be processed that the purposes become unclear or uninformative.

Like the CCPA, the proposed rules would also impose a new requirement to provide consumers with a Notice at Collection and prohibit the collection of personal data from consumers unless that notice is provided. The proposed regulations would also include new profiling disclosures in privacy notices.

The proposed regulations would further mandate that controllers notify consumers of material changes to their privacy notices and obtain consent, if so required, before any processing of personal data subject to such changes.

Dark Patterns and Consumer Consent

Like other state comprehensive privacy laws, the NJDPA addresses and prohibits the use of "dark patterns" in obtaining consumer consent. The proposed regulations further detail what constitutes "dark patterns," which is described to include presenting choices in a way that shames or pressures a user into making a specific choice. One example provided to illustrate a potential violation of this provision include alternative choices presented to the user such as, "*I accept, I want to help defeat cancer*," and "*No, I don't care about cancer patients*." The proposed regulations also prohibit dark patterns that are confusing, manipulative, or misleading.

Regarding user choice architecture and design for submitting data rights requests and obtaining consent, the proposed regulations would require controllers to test their methods to ensure that they are functional and do not undermine consumers' choices by impairing or interfering with the consumer's ability to make privacy choices. For example, similar to guidance issued by the California Privacy Protection Agency last year regarding dark patterns, the proposed New Jersey regulations expressly incorporate the concept of symmetry-in-choice, which provides that a choice to "Accept All" in one step must also allow consumers to "Decline All" in one step.

In another example provided in the proposed regulations, a consumer navigating forward on a webpage without selecting an option after a consent choice has been presented must not be interpreted as affirmative consent. Importantly, the proposed regulations provide that any method for submitting data rights requests and obtaining consent that does not comply with these regulations would be considered a "dark pattern."

Verification of Data Rights Requests

Like the Colorado regulations, the proposed regulations lay out the factors a controller must consider in determining whether an authentication method for verifying the identity of a consumer is "commercially reasonable" when a consumer submits a data rights request. New Jersey would add a few new factors to consider, including the likelihood that malicious actors would seek personal data and the current available technology for verification.

Loyalty Programs

The NJDPA explicitly states that it does not prohibit businesses from offering consumers discounts, loyalty programs, or other incentives for the collection, processing, and sale of personal data, provided disclosures are provided. Like the CCPA's requirement to provide a Notice of Financial Incentive, the proposed regulations require that consumers be provided with a Notice of the Loyalty Program at or before the point of program enrollment and must offer benefits that are reasonably related to the value of the consumer's personal data.

Notably, the proposed regulation further states that if a controller is unable to calculate a good faith estimate of the value of personal data that forms the basis for offering a loyalty program benefit or cannot show that the benefit is reasonably related to the value of personal data, the controller must not offer the program.

This would require companies to document calculations, assessments, and other financial considerations when determining the value of consumers' personal data, which may include assigning and specifying dollar amounts if personal data is sold to third parties or exchanged for other consideration.

Recordkeeping

Like the CCPA, the proposed regulations require controllers to retain information about data rights requests (*e.g.*, right to access, confirm, correct, delete, opt out of sale, etc.) for at least 24 months, such as the date of the request, the data rights request type, and the substance of the controller's response. In alignment with data minimization principles, a controller would also be required to set reasonable, specific time limits for erasing personal data or for conducting a periodic review so that personal data is not retained for longer than necessary.

Further, the proposed regulations would expressly require that such records be made available at the completion of a merger, acquisition, bankruptcy, or other transaction in which a third party assumes control of personal data to ensure any new controller continues to recognize a consumer's previously exercised data rights.

This would impose privacy obligations on new buyers and third parties that acquire personal data as part of an asset-sale or other transaction to ensure that internal processes are in place to effectively manage and honor consumer opt-outs, among other compliance obligations.

Takeaways

Although many of these proposed regulations generally track the existing California and Colorado privacy regulations, New Jersey has taken additional steps to clarify and outline detailed examples and processes for complying with current privacy requirements. This would impose additional compliance obligations on controllers and processors – something to keep in mind as companies continue to build out and update their websites and internal data management systems to ensure compliance with new privacy laws, while meeting consumers' expectations to better control their data and maintain data autonomy.

RELATED INDUSTRIES + PRACTICES

- Privacy + Cyber