Proposed New Jersey Regulations Would Require Major Privacy Compliance Shifts for Businesses

Insights
7.17.25

New Jersey officials recently released proposed privacy regulations that would create several new compliance obligations for businesses above and beyond what existing state law and many other state laws require, meaning you may need to adjust your compliance approach if you do business there. The June 2 release by the Office of Consumer Protection aims to stretch the boundaries of the New Jersey Data Privacy Act (NJDPA) – so much so, in fact, that you should not assume your existing compliance programs would fully satisfy these proposed requirements. They include detailed standards for obtaining **consumer consent**, specific content and timing requirements for **loyalty program notices**, expanded definitions of **personal and sensitive data**, and new restrictions on the use of data for **AI model training**. The public comment period for businesses that want to make their voice heard runs through August 1, 2025. What do you need to know about these proposed rules, and what can you do help shape policy before these take effect without substantive changes?

Quick Background

The NJDPA took effect on January 15, 2025. It applies to any business that conducts business in New Jersey or produces products or services that are targeted to New Jersey residents, and that during a calendar year either:

- Controls or processes the personal data of at least 100,000 New Jersey residents, excluding personal data processed solely for the purpose of completing payment transactions or data collected in the employment or commercial (B-2-B) context; or
- Controls or processes the personal data of at least 25,000 New Jersey residents and the business derives revenue, or receives a discount on the price of any goods or services, from the sale of personal data.

You can read our detailed summary here.

Definitions: Personal and Sensitive Data

The proposed regulations expand two very critical definitions, which would reshape the state's privacy law.

Personal Data

Key to all the consumer privacy laws is the definition of personal data. Under the NJDPA, this is defined as "any information that is linked or reasonably linkable to an identified or identifiable person." The law excludes data collected in the employment or commercial (B-2-B) context.

The proposed regulations include an expanded definition that incorporates personal data that is reasonably linkable to a person. This refers to information that can identify a person or a device associated with a person when cross referenced with other data, including, but not limited to, a person's:

- Full name
- Mother's maiden name
- Telephone number
- IP address or other unique device identifier
- Place of birth
- Date of birth
- Geographical details (for example, zip code, city, state, or country)
- Employment information
- Username, email address, or any other account holder identifying information (including but not limited to identifying information related to social media accounts)
- Mailing address
- Race, ethnicity, sex, sexual orientation, or gender identity or expression

With such a change, this would mean that a business subject to the law may be collecting personal data even if the business itself is not capable of identifying the person with the data and resources it has available, as long as the data is reasonably linkable by a third party that has access to other data points that, when cross-referenced with the data collected by the covered business, would identify the person.

Sensitive Data

As for sensitive data, the proposed regulations similarly provide a broad definition, especially when compared to other states. The NJDPA uniquely includes financial information such as account numbers, login credentials, and credit or debit card numbers when combined with security codes. The inclusion of these financial data elements in the definition of sensitive data introduces heightened risk and may trigger additional consent, security, and processing requirements. Compared to other states, the NJDPA takes a broader approach by expressly including this type of

financial information, which expands the scope of compliance for covered businesses.

What Should You Do?

Businesses that are currently subject to other state privacy laws, such as the California Consumer Privacy Act (CCPA) or the Colorado Privacy Act (CPA), will need to reassess their data inventories and classification practices to ensure they capture additional categories that would be considered personal or sensitive under the proposed NJDPA regulations should they take effect as proposed. These include mother's maiden name, place and date of birth, unique device identifiers, and identifying information related to social media accounts.

Consent and Dark Patterns

The proposed regulations set forth detailed requirements for designing user interfaces used to obtain consumer consent and to facilitate the submission of data rights requests. When seeking consent, the proposed regulations make clear that a consumer's silence or failure to take affirmative action cannot be interpreted as acceptance or consent.

Businesses would be prohibited from implementing the following methods in their efforts to obtain consent:

- Use language, visuals, or interactive elements to **coerce or steer consumer choice or consent**, including presenting choices in a way that shames or pressures the user into selecting a specific choice. For example, presenting the choice: "I accept, I want to help defeat cancer" versus "No, I don't care about cancer patients" may violate this provision.
- Require the consumer to **search or scroll** through the text of a privacy policy or similar document or webpage to locate the mechanism for submitting an opt-out request.
- **Bundling choices** so that the consumer is forced to consent to the use of personal data for any purposes that are incompatible with the context in which the personal data was collected. For example, a controller that provides a location-based service, such as a mobile application that finds gas prices near the consumer's location, shall not require the consumer to consent to incompatible uses (for example, the sale of the consumer's geolocation to data brokers) together with a reasonably necessary and proportionate use of geolocation data for providing the location-based service.

The regulations also prohibit the use of dark patterns, which include but are not limited to:

- Choice options presented with a preselected or default option; or
- Redirecting consumers away from the content or service they are attempting to interact with because they declined the consent choice offered, unless consent to process the requested data is strictly necessary to provide the website or application content or experience.

What Should You Do?

Given these proposed requirements, businesses subject to the NJDPA should review and, if needed, redesign their websites to ensure that cookie consent mechanisms such as cookie banners are accessible and present choices with symmetry. You'll want to avoid designs that nudge or pressure consumers into consenting to data uses beyond what is reasonably necessary.

Data Minimization and Data Privacy Impact Assessments

The proposed regulations impose a heightened data minimization standard that goes beyond traditional requirements in most states.

- Businesses must not only limit the collection of personal data to what is reasonably necessary for the disclosed purposes, but also document the necessity of each category of personal data collected.
- Additional requirements include maintaining detailed data inventories and regularly reassessing retention practices, particularly for high-risk data such as biometrics.
- Data must be deleted when it is no longer needed, including immediately after consent is withdrawn, and processors (vendors) must be instructed to do the same.
- If a business relies on an exception or introduces a new processing purpose, it must document its justification and assess compatibility based on consumer expectations, the sensitivity of the data, and the potential risks involved.

In relation to data privacy impact assessments, the proposed regulations require data privacy impact before processing any data that presents a "heightened risk of harm," regular review and update of the assessment and retain relevant documentation for at least three years after processing concludes.

Duty of Care

The proposed regulations impose what is labeled as a "duty of care" to protect the confidentiality, integrity, and accessibility of personal data, which is a relatively new concept in the state consumer privacy landscape. This duty would require businesses subject to the NJDPA to implement and maintain comprehensive security practices to safeguard personal data from unauthorized access and misuse during both storage and use. When evaluating appropriate security measures, organizations would have to consider several factors, including industry standards, the size and complexity of the business, the sensitivity and volume of data, the source of the data, and the potential risk to consumers.

This heightened obligation is particularly relevant given the growing wave of privacy litigation targeting companies' data practices. The proliferation of privacy litigation involving website cookies and third-party pixels and trackers have included negligence claims, alleging a company violated

and third-party pixels and trackers have included negligence claims, alleging a company violated such a duty. The explicit inclusion of a duty of care standard could lead plaintiffs' firms to target New Jersey businesses.

What Should You Do?

Ensuring your business is in solid legal compliance will help avoid costly and extensive litigation, which we predict will continue. Further, we expect plaintiffs' firms to find new avenues for alleging privacy claims with potential changes to the California Invasion of Privacy on the horizon by 2027 (click here for status of that legislative effort), which if enacted may limit claims against businesses employing online tracking technologies.

Privacy Policy and Required Disclosures

The NJDPA requires controllers to provide consumers with a detailed privacy notice that includes the categories of personal data processed, the purposes for processing, data sharing practices, consumer rights, retention periods, and contact information.

The proposed regulations would expand on these requirements by clarifying that each category of personal data must be described with enough specificity to allow consumers to understand what is being collected, such as specifying examples like "email address" or "government-issued identification number." They also require businesses to disclose how long each category of data will be retained, whether any profiling practices have a legal or similarly significant effect on the consumer, and whether the personal data of minors is knowingly sold or shared.

The proposed regulations also introduce specific accessibility standards. Disclosures must be clear, written in plain language, accessible to individuals with disabilities, provided in the languages the business typically uses to communicate with consumers, and formatted so they are easily printable. Importantly, a separate section specific to New Jersey is not required as long as the privacy notice, taken as a whole, satisfies all requirements under the NJDPA.

Artificial Intelligence and Internal Research Exemption

The NJDPA allows controllers and processors (vendors) to use personal data for internal research purposes, such as improving or developing products, services, or technologies. However, the proposed regulations significantly narrow this exemption, particularly in the context of AI, and adopt a stricter approach than other state privacy laws.

Specifically, the regulations clarify that the exemption does not apply where:

- The data or resulting research is used to train AI, unless the consumer has affirmatively consented to such use; or
- The data or resulting research is shared with a third party, unless it is either de-identified or shared pursuant to a lawful exemption under the regulations (e.g., compliance with applicable

shared pursuant to a lawful exemption under the regulations (e.g., compliance with applicable law).

The proposed regulations do not define "artificial intelligence," which may create uncertainty for businesses leveraging consumer data to develop or enhance AI and machine learning models. Without a clear definition and given the requirement for affirmative consent, companies without established consent mechanisms may face increased compliance challenges. This marks a more restrictive approach than other state privacy laws and may require organizations to reassess whether their existing data practices remain permissible under the NJDPA's internal research exemption.

Loyalty and Discount Program Disclosures

The proposed regulations introduce detailed compliance obligations for businesses offering loyalty programs, discounts, or other incentives in exchange for the collection, processing, or sale of personal data. Controllers that offer such programs must provide a "loyalty program notice" at or before the point of enrollment, similar in concept to California's "Notice of Financial Incentive" under the CCPA.

Consumers must be able to withdraw from a loyalty or incentive program at any time without incurring any penalty, and any benefits offered must be reasonably related to the value of the consumer's personal data. Importantly, if a business cannot in good faith calculate the value of that data or demonstrate that the benefit is proportionate, it may not offer the program at all. This introduces a heightened obligation to maintain documented assessments, valuation methodologies, or calculations, particularly where personal data is sold or exchanged for consideration.

Engage With State Regulators

We recommend you submit comments before August 1 to provide regulators your perspective on how these changes could impact your business. For assistance, consider reaching out to the authors of this Insight or the FP Advocacy team to help develop best strategies for having your voice heard.

Conclusion

While not exhaustive, the changes outlined here spotlight critical developments that could significantly impact businesses operating in New Jersey. The proposed regulations introduce several new requirements not found in other state privacy laws, raising the compliance bar in key areas. Organizations will need to conduct proactive, thorough due diligence to assess whether their current data practices align with these emerging legal expectations.

Fisher Phillips will closely monitor the evolution of the New Jersey Data Privacy Act and stands ready to help businesses navigate compliance challenges, identify potential compliance risks, and

bridge the gap between today's policies and tomorrow's regulatory demands. Make sure you are subscribed to Fisher Phillips' Insight system to receive critical updates.

For assistance in evaluating whether the Act applies to your business, determining which other data privacy and security laws may apply, and identifying the actions needed to ensure legal compliance, contact your FP attorney, the authors of this Insight, any attorney on our Privacy and Cyber Team or Consumer Privacy Team, or any attorney in our New Jersey office.

Related People

Catherine M. Contino
Associate
610.230.6103
Email

Vivian Isaboke, CIPP/US, CIPM
Associate
908.516.1028
Email

Usama Kahf, CIPP/US
Partner
949.798.2118
Email

Jillian Seifrit, CIPP/US
Associate
610.230.6129
Email

Service Focus

Privacy and Cyber

Consumer Privacy Team

AI, Data, and Analytics

Trending

U.S. Privacy Hub

Related Offices

New Jersey

New Jersey