Data Privacy: Insights from the Recent FAQs on New Jersey Data Privacy Law

Author: Jana Slavina Farmer

As organizations prepare for compliance with the New Jersey Data Privacy Law (NJDPL), set to take effect on January 15, 2025, the Division of Consumer Affairs (DCA) has released a set of 24 Frequently Asked Questions (FAQs) that provide important insights and guidance on complying with New Jersey's robust regulatory framework. The FAQs are *not* binding and should not be considered a legal document or a complete explanation of the law. Rather, they are useful as a reference for persons within the entities covered by NJDPL that have a role in privacy compliance.

The FAQs specifically focus on sensitive data, children's data, opt-out or revocation of consent from sale of personal data (including via universal opt-out signals), contracts with data processors, and data protection assessments, indicating the New Jersey DCA's focus areas for the enforcement of the incoming law. This article explores the key takeaways from the FAQs, particularly concerning the treatment of sensitive data.

Understanding the New FAQs
The recent FAQs were published for the convenience of businesses (although the FAQs use the term "businesses," NJDPL also applies to nonprofits). The FAQs distill and clarify several key definitions contained in the NJDPL, summarize consumer rights, define business obligations, and provide additional guidance regarding processing of sensitive data and data of minors.

Specifically, NJDPL governs the use of personal data, which the law defines as any information that is linked or reasonably linkable to an identified or identifiable person. The FAQs clarify this definition as "any information that is not publicly available and can be used to identify a specific individual." The key difference between these definitions is in the "reasonably linkable" criteria in the statute, whereas the FAQs seem to focus on specific identifiability. Practically speaking, there are categories of data that may be linkable to an individual through context (for example, email metadata, or de-identified data combined with external data that permits reidentification, such as a fitness tracker ID combined with gym membership data) that would be within NJDPL's scope. Differences such as these highlight that the covered entities must not rely solely on the FAQs' definitions when building their NJDPL compliance program.

The FAQs also clarify the definitions of the key actors in the data privacy lifecycle under NJDPL:

- **Consumer**: A New Jersey resident acting in a personal or household context
- **Controller**: Any individual or entity that decides how and why consumers' personal data is processed
- **Processor**: An individual or entity that processes personal data on behalf of the controller. A processor is different than a controller because it does not have decision-making authority over personal data. A processor can only process personal data at the request and under the direction of a controller.

The FAQ clarifies that NJDPL applies to any **controller** that:

(1) Does business in New Jersey or produces products or services targeted to New Jersey residents and

(2) During a calendar year either (a) controls or processes the personal data of at least 100,000 consumers or (b) controls or processes the personal data of at least 25,000 consumers and makes money from the sale of personal data.

The FAQs detail some of the obligations of the controllers, including to prepare a written privacy notice accurately disclosing data practices, to honor consumer rights, to enter into written contracts with vendors receiving personal data from controllers (vendors generally will be processors, see below), to conduct data protection assessments, and to process certain categories of data only with consumers' express consent.

With respect to **processors**, the FAQs highlight that among other requirements, a processor must:

- Follow the controller's instructions
- Help the controller meet its obligations under NJDPL
- Keep personal data confidential
- Enter into a contract with the controller that contains processing instructions; identifies the data that will be processed and for how long it will be processed; and requires the processor to return or delete the personal data once processing is complete.

For **consumers**, the FAQs summarize their rights as follows:

- Confirm whether a controller processes the consumer's data
- Correct inaccuracies in the consumer's personal data
- Delete the consumer's personal data
- Say "no" (opt out) to a controller selling the consumer's personal data or using the consumer's personal data for targeted advertising and some types of profiling (for example, profiling to determine whether a consumer should receive a loan or mortgage, a job offer, or an insurance policy).

Controllers must provide clear and accessible mechanisms for consumers to exercise these rights. Additionally, by July 15, 2025, businesses must comply with universal opt-out signals, such as those from Global Privacy Control (users enable privacy preferences within their web browsers). A universal opt-out signal is a mechanism that allows individuals to communicate their preference to opt out of certain data processing activities, such as targeted advertising or sale of data, across multiple websites or platforms in a standardized way. It eliminates the need for consumers to manually opt out on each site individually.

Again, the FAQs do not repeat NJDPL's definitions, criteria, and recitations of rights word by word, but rather aim to give organizations a general sense of what these key concepts mean. While at first blush the distinctions between the FAQ and NJDPL definitions may not seem significant in practice, as the saying goes, the devil lurks in the details. Note, for example, that personal data processed solely for the purpose of completing a payment transaction is exempted from the 100,000 consumers' data threshold, and that receiving a discount on a price of any goods or services counts toward the "making money from personal data" threshold.

Update on Anticipated Regulations and Enforcement Deadlines

New Jersey is one of three states to date that provide rulemaking authority under their data privacy law to the state agency; here, the DCA. The FAQs are not such regulations, but they expressly state that the DCA will be issuing regulations under NJDPL in 2025. This is a new development, as NJDPL does not provide a deadline for promulgation of rules.

While the formal regulations under NJDPL are not yet available, the FAQs expressly state that the entities obligated under NJDPL are required to comply starting on January 15, 2025. A limited

opportunity to cure violations may be available until July 1, 2026: If the DCA identifies a potential violation that the controller can remedy, the DCA will send a notice to the controller to give them the chance to fix the problem within 30 days of the notice. If the violation is not remedied, the DCA can proceed with an enforcement action. While this provision is certainly beneficial for covered entities, it should not be interpreted as a license to avoid carefully thinking through and implementing the entity's compliance obligations before the January 15, 2025, deadline. At most, this grace period should be used to remedy inadvertent mistakes in compliance.

Treatment of Sensitive Data

The FAQs explain that **sensitive data** is a subset of personal data that reveals a consumer's racial or ethnic origin, religious beliefs, health condition, financial information, sexual activity or sexual orientation, immigration or citizenship status, status as transgender or non-binary, genetic or biometric data, or precise geolocation data. It also includes personal data collected from a known child. This restatement loosely tracks NJDPL's definition. Most of the data considered sensitive in New Jersey also is recognized as sensitive under most U.S. state privacy laws. However, New Jersey includes additional types of data as sensitive, including status as transgender or non-binary and financial information, which only a handful of other states recognize as sensitive.

The sensitive financial information in New Jersey includes "a consumer's account number, account log-in, financial account, or credit or debit card number, in combination with any required security code, access code, or password that would permit access to a consumer's financial account." Thus, not every piece of financial data will be deemed sensitive; however, NJDPL's definition is open-ended and types of financial data not presently listed in the statute may be included in the future.

For entities operating in more than one state that are required to comply with several state data privacy laws, it is important to correctly classify data as sensitive or not sensitive to ensure compliance with each such applicable law. Each U.S. state privacy law recognizes sensitive information and imposes heightened compliance requirements for its processing. Some states require a valid consent to be obtained before collection and processing of personal data, as well as a data protection assessment. Others follow an opt-out model, giving consumers the right to limit the use of their sensitive data.

The FAQs highlight that New Jersey requires consent before sensitive data is processed and that a data protection impact assessment must be conducted. NJDPL specifies that a valid consent must be "a clear affirmative act signifying a consumer's freely given, specific, informed and unambiguous agreement to allow the processing of personal data relating to the consumer." Such consent may include a written statement, including by electronic means, or any other unambiguous affirmative action. Notably, acceptance of a general or broad terms of use or similar document that contains descriptions of personal data processing along with other, unrelated information will not constitute a valid consent. As such, organizations should not rely on statements such as "if you visit our website, you consent to our privacy policy" as evidence of consent to processing of sensitive information. Furthermore, hovering over, muting, pausing, or closing a given piece of content will not be considered sufficient evidence of consent.

Treatment of Children's Data

NJDPL requires businesses to obtain explicit consent for processing personal data of children under the age of 13, treating such data as sensitive. Consent also is required for processing of data of minors that are at least 13 and are younger than 17, if such processing is done for the purposes of targeted advertising, sale of personal data, or profiling in furtherance of decisions that produce legal or similarly significant effect on the consumer. With this latter provision, New Jersey's law extends protections beyond federal standards under the Children's Online Privacy Protection Act (COPPA), which only safeguards the data obtained online from children under 13.

The FAQs state that when a controller knows or should know that a consumer is between the ages

of 13 and 16 (note, NJDPL uses the term “younger than 17” but the FAQ is using the 13–16 range), the controller must get the consumer's consent before processing the consumer's personal data. This is interesting as this statement is broader than NJDPL. First, the FAQs use the term “should know” whereas the statute requires actual knowledge or willful disregard. Second, the FAQs claim that consent is necessary for any processing of the data of minors ages 13–16, and not only when sale of data, targeted advertising, or profiling is occurring.

Businesses processing children’s data should take note and consider building a more stringent compliance regime: even where FAQs are non-binding, this is an enforcement focus area for the New Jersey regulator (and for the regulators in other states and on the federal level).

Considerations for Compliance
With the enforcement deadline looming, organizations within the scope of NJDPL should consider the following workflow to align their compliance with the incoming law:

1. **Review/Update Privacy Policies**: Update privacy notices to clearly outline data processing activities, purposes of processing, consumer rights, and opt-out procedures, among other mandatory disclosures, to track NJDPL’s requirements.

2. **Implement Consent Management Systems**: Adopt technologies that facilitate obtaining, managing, and documenting consumer consent for sensitive data processing.

3. **Conduct Data Protection Assessments**: Regularly evaluate data handling practices to identify risks and benefits of processing activity that presents heightened risk of harm to the consumers to ensure alignment with New Jersey’s law.

4. **Enhance Training Programs**: Educate employees with data privacy responsibility in different departments (including IT, Marketing, and Customer Service, not just Legal) about NJDPL’s provisions and the importance of safeguarding consumer data and respecting consumer choices regarding their data.

5. **Stay Informed of the Regulatory Changes**: Be aware of evolving privacy regulations to anticipate and address new compliance obligations. Aside from New Jersey’s anticipated regulations, other states are poised to adopt new privacy laws or amend existing ones, promising that 2025 will be a busy year for data privacy. While the FAQs serve as an important resource for understanding the law’s practical application, highlighting the importance of explicit consent and enhanced protections for sensitive data, organizations should consider following the more precise requirements of NJDPL and the incoming regulations in aligning their practices with New Jersey’s requirements. As compliance with the NJDPL becomes mandatory, legal experts can provide tailored advice to navigate the intricacies of the law and ensure that data practices align with both state and federal regulations.