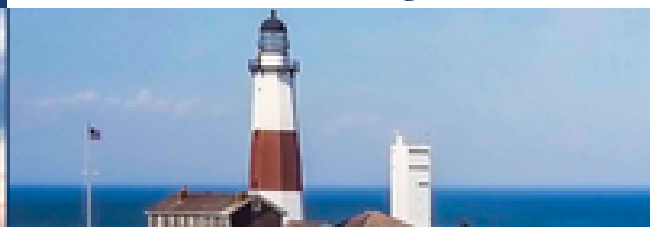
February 12, 2024

By: Nicole E. Osborne, Esq.
Liam Bradley, Esq.

RUSKIN MOSCOU FALTISCHEK P.C.
Smart Counsel. Straight Talk.



New Jersey Enacts Consumer Privacy Law

On January 16, 2025, the New Jersey Consumer Privacy Act (the "NJCPA") will take effect, affecting data collection and privacy rights in the State. Governor Murphy signed the legislation (S332/A1971) on January 16, 2024, which, according to the press release, will "protect consumer privacy by requiring the notification to consumers of collection and disclosure of personal data by certain entities, including internet website and online providers." Although the 13th state to enact a comprehensive privacy bill, New Jersey's bill stands out in its applicability, consumer rights, protection of children, enforcement, and penalties.

Applicability and Important Definitions. New Jersey's law is unique in its widespread applicability and lack of exemptions typically found in other states' consumer privacy laws.

The NJCPA applies to entities that do business in New Jersey and meet **either** of the following:

1. process the personal data of at least 100,000 New Jersey residents (excluding personal data processed solely for the purpose of completing a payment transaction); **or**
2. process the personal data of at least 25,000 New Jersey residents and derive revenue or receive a discount on goods or services from the sale of personal data.

Importantly, there is **no revenue threshold**.

Additionally, "sale" is broadly defined to capture "the exchange of personal identifiable information for monetary consideration by the operator to a third party for purposes of licensing or selling personally identifiable information at the third party's discretion to additional third parties." However, someone acting in a commercial or employment context is not regarded as a consumer for the purposes of this law. "Consumer" is defined to only mean "an identified person who is a resident of this State acting only in an individual or household context." Finally, what constitutes "sensitive data" is broader than in other states. Here, sensitive data is defined as "personal data revealing racial or ethnic origin; religious beliefs; mental or physical health condition, treatment, or diagnosis; financial information, which shall include 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; sex life or sexual orientation; citizenship or immigration status; status as transgender or non-binary; genetic or biometric data that may be processed for the purpose of uniquely identifying an individual; personal data collected from a know child; or precise geolocation data." More definitions are provided within the bill itself.

Exemptions, on the other hand, are far and few between. The law does not exempt nonprofits or institutions of high education. It also does not exempt personal data governed by the Family Educational Rights and Privacy Act (FERPA). There are, however, exemptions for data and entities subject to the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA), the Driver's Privacy Protection Act, and the Fair Credit Report Act (FCRA). There are also some exemptions for data processed by state entities and political subdivisions of the state.

Consumer Rights. The NJCPA expressly provides for both consumer rights and obligations for subject data controllers to follow to comply with the consumer privacy statute. The consumer has the right to know "whether a controller processes the consumer's personal data" and view such data. Additionally, the consumer may correct inaccuracies, delete data, or "obtain a copy of the consumer's personal data." Finally, the NJCPA gives consumers the right to "opt-out of processing of personal data for purposes of (a) targeted advertising; (b) the sale of personal data or (c) profiling in furtherance of decision that produce legal or similarly significant effects concerning the consumer." This opt-out preference must be available through a mechanism supplied by the controller before July 16, 2025 (six (6) months from when the law takes effect).

Correspondingly, businesses subject to the NJCPA have a duty to "provide to a consumer with a reasonably accessible, clear, and meaningful privacy notice." They must give notice as to the categories of the data collected, the categories of third parties for which the data is disclosed to, categories shared with third parties, and the purpose of data collection. Furthermore, controllers must detail how a consumer may exercise their rights described above and how they will be notified about any changes to the process for notification. Entities must also have "an active e-mail address or other online mechanism that consumers may use to contact the controller."

A request to exercise the consumer's rights from a verified consumer through this online point of contact must be responded to within forty-five (45) days. However, an additional 45-day extension is possible "when reasonably necessary considering the complexity and number of the consumer's requests, provided that the controller informs the consumer of any such extension within the initial 45-day response period and the reason for the extension." Finally, all sales of personal data and the opt-out mechanism must be clearly and conspicuously disclosed to the consumer.

Protection of Children. A distinguishing factor between the NJCPA and other data privacy laws is its focus on the protection of children's personal data. An entity subject to the law must not knowingly process the personal data of children between 13 and 17 without obtaining their consent. Consent is necessary when the controller is using a child's data for the purposes of selling it, creating targeted advertisements, or using it in some other manner that would normally require permission. Although the NJCPA creates additional protocols for controllers to implement, this enhanced child privacy requirement will help further safeguard children's personnel data from being sold or used without consent.

Enforcement. The NJCPA rests enforcement with the New Jersey Attorney General, who has sole and exclusive enforcement authority for a violation of the statute. Unlike some other states' privacy laws, there is no private right of action. Additionally, the statute designates the New Jersey Department of Law and Public Safety's Division of Consumer Affairs with rulemaking authority.

Penalties. Data controllers that fail to adhere to these new requirements will be subject to penalties under New Jersey Penal Law. Failure to notify a consumer of the sale of personally identifiable information is a violation of section 2 and 3 of the New Jersey Penal Law § 1960. Additionally, failure to allow a consumer to opt-out is a violation of section 4 of the same statute. These violations will only occur, however, if the controller "fails to cure any alleged violation within 30 days after receiving notice of alleged noncompliance from the Attorney General." A first offense violation constitutes a $2,000 penalty, while subsequent offenses can be up to $5,000 for each offense.

Overall, the NJCPA places prolific protections on consumer data. Entities that process such data should assess whether they are subject to the new law and how they can conduct the required Data Protection Assessments and comply with other obligations under the act. To learn more about whether your business may be subject to this new law and what your obligations are, please contact:

Nicole Osborne, Esq.
516.663.6687
nosborne@rmfpc.com