THOMPSON HINE

Privacy & Cybersecurity Update

January 2024

New Jersey Enacts Consumer Data Privacy Law

New Jersey is the latest to join the list of states with comprehensive privacy laws, adding to the patchwork of laws governing personal information. On January 16, Governor Phil Murphy signed into law Bill 332 (NJ Act), which affords New Jersey residents data protection rights and requires covered businesses to comply with new data privacy and information security requirements. While the law imposes new compliance obligations on covered businesses, it notably does not create a private right of action and has a limited "cure period" allowing covered entities to remedy their noncompliance. The law assigns enforcement and rulemaking authority to the New Jersey Director of the Division of Consumer Affairs. The NJ Act will enter into force in January 2025.

Scope of Applicability

The NJ Act applies to a broad range of businesses, specifically entities that conduct business in New Jersey or produce products or services targeted to residents of the state, *and* that during a single calendar year:

- Controlled or processed the personal data of at least 100,000 consumers, excluding personal data controlled or processed solely for the purpose of completing a payment transaction; or
- Controlled or processed the personal data of at least 25,000 consumers and derived revenue or granted discounts on the price of any goods or services from the sale of personal data.

Unlike other privacy laws, the NJ Act does not impose specific revenue thresholds.

The NJ Act includes several exemptions that are standard in data privacy frameworks, including those for data processing activities governed by federal law (e.g., HIPAA, GLBA) or state agencies. The NJ Act's HIPAA exemption is only a data-level exemption, not entity-level, while the GLBA exemption is at the entity level. Notably, unlike similar state laws, there is no exemption for nonprofits or FERPA/institutions of higher education. Additionally, New Jersey joins Oregon as the only states not exempting pseudonymous data.

Key Terms

The NJ Act primarily regulates how a data controller can use and process a consumer's personal data. The term "consumer" means a New Jersey resident acting only in an individual or household context and excludes from its definitions individuals "acting in a commercial or employment context." The NJ Act's definition of "personal data" is akin to other state privacy laws and includes "any information that is linked or reasonably linkable to an identified or identifiable person." It does not, however, include within its scope either de-identified data or publicly available information. De-identified data is defined as data that cannot reasonably be used to infer information about or otherwise be linked to an identified individual or a device linked to such individual.

The NJ Act creates additional burdens when an entity processes "sensitive data," which is defined as a subset of personal data revealing racial or ethnic origin; religious beliefs; a mental or physical health condition, treatment, or diagnosis; financial information; sex life or sexual

orientation; citizenship or immigration status; transgender or non-binary status; certain types of genetic or biometric data; personal data collected from a known child under 13 years old; or precise geolocation data (i.e., information derived from technology that directly identifies the specific location of an individual with precision and accuracy within a radius of 1,750 feet). The NJ Act's definition of "biometric data" is broader than similar laws, including biological, physical, or behavioral characteristics as well as data generated by technological processing.

Consumer Data Privacy Rights

As with existing state privacy law, the NJ Act grants consumers substantial data privacy rights, namely:

- The right to confirm whether a controller is processing their personal data and to access such personal data, unless such confirmation or access would require the controller to reveal a trade secret.
- The right to correct inaccurate personal data, taking into account the nature of the personal data and the purposes of the processing of the consumer's personal data.
- The right to require an entity to delete their personal data.
- The right to obtain a copy of their personal data, in a portable and, to the extent technically feasible, readily usable format that allows them to transmit the personal data to another controller.
- The right to opt out from a controller's processing of personal data for the purposes of targeted advertising and profiling, the sale of personal data, or profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer.

The NJ Act defines a "sale of personal data" as the sharing, disclosing, or transferring of personal data for monetary or other valuable consideration by the controller to a third party. However, the sale of personal data does not include the mere disclosure of personal data to data processors and other common data disclosure practices (e.g., disclosure of personal data to an affiliate at the request of a consumer or as part of a corporate restructuring).

The NJ Act creates a framework for how controllers must receive, authenticate, and respond to consumer data privacy requests, including that controllers must respond to a consumer personal data request within 45 days of receipt of the request, with a 45-day extension available. It also mandates that organizations "establish a process" to allow a consumer to "appeal" a controller's denial of a consumer request, which must be delivered within 45 days, detailing the reasons for the decision, and if an appeal is denied, the manner in which the consumer may contact the New Jersey Division of Consumer Affairs to submit a complaint.

Consent

The NJ Act limits how a controller can use personal data without a consumer's consent. For example, an organization must obtain consumer consent to process or collect sensitive data, personal data concerning a child under 13 years old, or personal data for the purposes of sale, targeted advertising, or certain profiling. An entity must also obtain consent to process personal data for purposes that are not reasonably necessary for, nor compatible with, the purposes for which the data originally was processed, as disclosed to the consumer. The NJ Act also prohibits the collection and processing of personal data of minors between 13 and 17 years old for the purpose of selling the data, targeted advertising, or profiling (where the profiling would result in legal or similarly significant effects).

Data Protection Assessments

Like other privacy laws, the NJ Act requires a controller to conduct and document a data processing assessment for each of its processing activities that "presents a heightened risk of harm to a consumer." The NJ Act defines this term as including targeted advertising, selling of personal data, processing of sensitive data, and certain types of profiling. The assessment must be made available to the New Jersey Division of Consumer Affairs upon request.

Privacy and Other Notices

Controllers are required to provide consumers with a reasonably accessible, clear, and meaningful privacy notice that describes their data processing activities (e.g., categories of personal data collected and processed, purposes of processing, categories of personal data shared with third parties, categories of third-party recipients). The notice also must include the controller's contact

information and how consumers can exercise their data privacy rights, including how they can appeal a controller's decision. The notice must provide an active email address or other online mechanism that the consumer may use to contact the controller.

A controller that sells personal data to third parties or processes personal data for targeted advertising, engages in the sale of personal data, or conducts profiling that produces legal effects has the additional obligation to "clearly and conspicuously disclose" such processing and how consumers can exercise their opt-out rights.

Processor Obligations and Contracts

The NJ Act places affirmative obligations on processors, such as those related to compliance with a controller's instructions, to assist in responding to consumer rights requests and the implementation of security controls to safeguard personal data from unauthorized use. Moreover, the law requires processors to help meet a controller's obligations related to the security of processing personal data and providing notification of a security breach. It also requires controllers and processors to execute written agreements that contain certain data protection clauses, which must address, among other things, the nature and purpose of data processing, the duration of the processing, the type of data subject to processing, parties' rights and obligations, confidentiality duties, compliance assessments, and subprocessing.

Rewards Programs and Anti-Discrimination

The NJ Act permits controllers to offer consumers different services or similar services at different prices that are related to loyalty or rewards programs. However, a controller may not discriminate against a consumer for exercising a data privacy right or making decisions related to the consumer's personal data that produce legal or similarly significant effects (e.g., by denying the consumer a good or service, charging a different price, or providing a different level of quality of a good or service).

Data Security Requirements

The NJ Act places affirmative data security obligations on controllers to protect the confidentiality, integrity, and accessibility of personal data and secure personal data from unauthorized acquisition during storage and use. It requires them to establish, implement, and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data appropriate to the volume and nature of the personal data at issue.

FOR MORE INFORMATION

For more information, please contact:

Steven G. Stransky
216.566.5646
202.263.4126
Steve.Stransky@ThompsonHine.com
Certified Information Privacy Professional/Government (CIPP/G)
Certified Information Privacy Professional/United States (CIPP/US)

Thomas F. Zych
216.566.5605
Tom.Zych@ThompsonHine.com

Marla M. Izbicky
312.998.4253
Marla.Izbicky@ThompsonHine.com
Certified Information Privacy Professional/United States (CIPP/US)

Thora Knight
212.908.3971
Thora.Knight@ThompsonHine.com