New Jersey Data Privacy Law (S.332/A.1971) Summary

On January 17, 2024, Governor Phil Murphy (D) signed S. 332, which would require notification to consumers of collection and disclosure of personal data by certain entities, into law. The law will become effective on January 16, 2025. A non-comprehensive summary of significant elements of the Act follows:

Covered Entities	Applies to any entity that "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."
Covered Data	***"Personally Identifiable Information"***: any information that is linked or reasonably linkable to an identified or identifiable person. "Personally identifiable information" shall not include de-identified data. ***"Sensitive Data"***: 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 known child; or precise geolocation data "***Biometric data***": data generated by automatic or technological processing, measurements, or analysis of an individual's biological, physical, or behavioral characteristics, including, but not limited to, fingerprint, voiceprint, eye retinas, irises, facial mapping, facial geometry, facial templates, or other unique biological, physical, or behavioral patterns or characteristics that are used or intended to be used, singularly or in combination with other or with other personal data, to identify a specific individual. The term does ***not*** include a digital or physical photograph, an audio or video recording, or any data generated from a digital or physical photograph, or an audio or video recording, unless such data is generated to identify a specific individual.
Key Definitions	***"Consent"***: 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. "Consent" may include a written statement, including by electronic means, or any other unambiguous affirmative action. "Consent shall not include: acceptance of a general or broad terms of use or similar document that contains descriptions of personal data processing along with other, unrelated information; hovering over, muting, pausing, or closing a given piece of content; or agreement obtained through the use of dark patterns. ***"Dark Pattern":*** a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making, or choice, and includes, but is not limited to, any practice the United States Federal Trade Commission refers to as a "dark pattern." ***"De-Identified Data"***: data that cannot be reasonably used to infer information about, or otherwise be linked to, an identified or identifiable individual, or a device linked to such an individual, if the controller that possesses the data: (1) takes reasonable measures to ensure that the data cannot be associated with an individual, (2) publicly commits to maintain and use the data only in a de-identified fashion and not to attempt to re-identify the data, and (3) contractually obligates any recipients of the information to comply with the requirements of this paragraph

	"Publicly available information": information that is lawfully made available from federal, State, or local government records, or widely-distributed media. ***"Targeted advertising"***: displaying advertisements to a consumer where the advertisement is selected based on personal data obtained or inferred from that consumer's activities over time and across nonaffiliated Internet web sites or online applications to predict such consumer's preferences or interests. "Targeted advertising" shall not include: advertisements based on activities within a controller's own internet websites or online applications; advertisements based on the context of a consumer's current search query, visit to an internet website or online application; advertisements directed to a consumer in response to the consumer's request for information or feedback; or processing personal data solely to measure or report advertising frequency, performance, or reach. ***"Sale":*** the sharing, disclosing, or transferring of personal data for monetary or other valuable consideration by the controller to a third party. "Sale" shall not include: • The disclosure of personal data to a processor that processes the personal data on the controller's behalf; • The disclosure of personal data to a third party for the purposes of providing a product or service requested by the consumer; • The disclosure or transfer of personal data to an affiliate of the controller; • The disclosure of personal data that the consumer intentionally made available to the general public through a mass media channel and did not restrict to a specific audience; or • The disclosure or transfer of personal data to a third party as an asset that is part of a proposed or actual merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the controller's assets.
Consumer Rights	**Access:** A consumer has 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. **Affirmative Consent:** A controller may not process sensitive data concerning consumer without first obtaining the consumer's consent, or, in the case of processing of personal data concerning a known child, without processing such data in accordance with COPPA. **Correction:** A consumer has 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. **Deletion**: A consumer has the right to require an entity to delete their personal data. **Portability:** A consumer has 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. **Revocation:** A controller must provide an effective mechanism for a consumer to revoke the consumer's consent that is at least as easy as the mechanism by which the consumer provided the consumer's consent and, upon revocation of such consent, cease to process the data as soon as practicable, but not later than 15 days after the receipt of such request. **Opt Out Rights**: A consumer has 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.

	Disclosure/Third Parties: if a controller sells personal data to third parties or processes personal data for the purposes of targeted advertising, the sale of personal data, or profiling in furtherance of decisions that produce legal or similarly significant effects concerning a consumer, the controller must clearly and conspicuously disclose such sale or processing, as well as the manner in which a consumer may exercise the right to opt out of such sale or processing.
Business Obligations	**Transparency**: A controller must provide a consumer with a reasonably accessible, clear, and meaningful privacy notice that includes, but is not limited to: (i) the categories of the personal data that the controller processes; (ii) the purpose for processing personal data; (iii) the categories of all third parties to which the consumer may disclose a consumer's personal data; (iv) the categories of personal data that the controller shares with third parties, if any; (v) how consumers may exercise their consumer rights, including the controller's contact information and how a consumer may appeal a controller's decision with regard to the consumer's request; (vi) the process by which the controller notifies consumers of material changes to the notification required to be made available, along with the effective date of the notice, and; (vii) an active electronic mail address or other online mechanism that the consumer may use to contact the controller. **Responding to Consumer Requests**: Controllers must respond to a consumer personal data request within 45 days of receipt of the request, with a 45-day extension available. **For Users between 13 to 16 Years Old.** The law prohibits controllers from processing personal data for targeted advertising, sale of personal data, or certain types of profiling without the consumer's consent where the controller has actual knowledge, or willfully disregards, that the consumer is at least 13 but younger than 17 years old. **Data Security**: The law establishes 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. **Avoid Secondary Use**: Except as otherwise provided, a controller may not process personal data for purposes that are neither reasonably necessary to, not compatible with, the purposes for which such personal data is processed, as disclosed to the consumer, unless the controller obtains the consumer's consent. **Universal Opt-Out Mechanisms:** Beginning no later than six months after January 16, 2025, a controller that processes personal data for purposes of targeted advertising or the sale of personal data must allow consumers to exercise the right to opt-out through a user-selected universal opt-out mechanism. The platform, technology, or mechanism must: (i) not permit its manufacturer to unfairly disadvantage another controller; (ii) not use a default setting that opts-in a consumer to the processing or sale of personal data, unless the controller has determined the consumer has selected such default setting as an affirmative, freely given, and unambiguous choice; (iii) be consumer-friendly, clearly described, and easy to use by the average consumer; (iv) be as consistent as possible with any other similar platform, technology, or mechanism required by any federal or state law or regulation, and; (v) enable the controller to accurately determine whether the consumer is a resident of New Jersey and whether the consumer has made a legitimate request to opt out of the processing of personal data for the purposes of any sale of such consumer's personal data or targeted advertising. **No Unlawful Discrimination:** The law 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 Protection Assessments	The law 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" **before conducting such processing.** Data protection assessments shall identify and weigh the benefits that may flow, directly and indirectly, from the processing to the controller, the consumer, other stakeholders, and the public against the potential risks to the rights of the consumer associated with the processing, as mitigated by safeguards that the controller can employ to reduce the risks. The controller shall factor into this assessment the use of de-identified data and the reasonable expectations of consumers, as well as the context of the processing and the relationship between the controller and the consumer whose personal data will be processed. A controller shall make the data protection assessment available to the Division of Consumer Affairs in the Department of Law and Public Safety upon request.
Controller / Processor Distinction	Processing by a processor must be governed by a contract between the controller and processor that is binding on both parties. The contract must include: (i) the processing instructions to which the processor is bound, including the nature and purpose of the processing; (ii) the type of personal data subject to the processing, and the duration of the processing. A processor would be required to: (a) at the discretion of the controller, delete or return all personal data to the controller as requested at the end of the provision of services, unless retention is required by law; (b) make available to the controller all information necessary to demonstrate compliance with the state privacy law; (c) allow for, and contribute to, reasonable assessments and inspections by the controller or the controller's designated assessor, or, with the controller's consent, arrange for a qualified and independent assessor to conduct, at least annually and at the processor's expense, an assessment of the processor's policies and technical and organizational measures in support of the obligations under the state's privacy law, using an appropriate and accepted control standard or framework for the assessment, in addition to providing a report of the assessment to the controller upon request.
Exceptions and Exemptions	The law includes exemptions for certain types of entities and data categories, such as health information under HIPAA; financial institutions and data subject to the GLBA; certain insurance institutions; certain personal data covered by the Driver's Privacy Protection Act; personal data governed by FCRA; as well as state entities and political subdivisions of the state. The bill notably does not provide exemptions to nonprofit organizations or institutes of higher education.
Enforcement	The Attorney General has sole enforcement authority of violations in the law. The law also includes a 30 day cure period, which will sunset on the first day of the 18th month following January 16, 2025, which would be July 1, 2026."The Office of the Attorney General shall have sole and exclusive authority to enforce a violation of [this law])Nothing in [this law] shall be construed as providing the basis for, or subject to, a private right of action for violations of [this law]."
Rulemaking Authority	The law requires the Director of the Division of Consumer Affairs in the Department of Law and Public Safety to promulgate rules and regulations necessary to effectuate the purposes of the law. Notably, only California and Colorado have passed comprehensive privacy laws with provisions that provide for similar rulemaking authority.