MINTZ

New Jersey Adopts a Comprehensive Data Privacy Law

April 15, 2024 | Blog | By **Cynthia J. Larose**, **Jon Taylor**

VIEWPOINT TOPICS

- Privacy & Cybersecurity

RELATED PRACTICES

- Privacy & Cybersecurity

RELATED INDUSTRIES

New Jersey's New Law is on the Books

2023 was a record-breaking year, with legislators in Delaware, Indiana, Iowa, Montana, Oregon, Tennessee and Texas passing comprehensive data privacy laws, joining California, Colorado, Connecticut, Utah and Virginia. Already 2024 is on pace to beat 2023's record year, as New Hampshire (New Hampshire Privacy Act, **SB 255-FN**), New Jersey (**New Jersey Privacy Act, SB 332**) and Kentucky (**HB 15**) lawmakers have already passed comprehensive privacy laws.

This post provides the details and information you and your business need to know about the New Jersey Privacy Act (NJPA), signed into law by Governor Phil Murphy. You can find our discussion regarding the New Hampshire Privacy Act **here**. For a full list of all state privacy laws we've covered, visit the **U.S. State Consumer Privacy Law** page.

Applicability Criteria

The NJPA applicability criteria mirrors the Virginia and New Hampshire data privacy laws and applies to any business or person that produces products or services that are targeted to residents of New Jersey, and either: (i) control or process the personal data of at least 100,000 New Jersey consumers, excluding personal data processed solely for the purpose of completing a payment transaction; **or** (ii) control or process the personal data of at least 25,000 New Jersey consumers and the controller derives revenue, or receives a discount on the price of any goods or services, from the sale of personal data.

The notion of "consumer" as used in the NJPA means an individual who is a resident of New Jersey and does not include individuals acting in a commercial or employment context. This distinction continues to be the predominant approach we are seeing adopted by the states, **with the notable exception being California**.

Notably, like Colorado's law, the NJPA does not provide a revenue threshold for the percentage of revenue a business must derive from the sale of data. Most other current state privacy laws generally apply only if the business derives a material portion of its annual revenue from the sale of personal data. **In addition, applicability under the NJPA does not involve any form of a revenue threshold, meaning small to medium-sized businesses processing personal data of high numbers of New Jersey consumers, or a company deriving any revenue at all from the selling of personal data of New Jersey consumers, may be subject to the law.**

Exemptions

The NJPA does not apply to:

- New Jersey government entities (or of any political subdivision of New Jersey)
- Financial institutions and affiliates, or data subject to the federal GLBA
- Covered entities or business associates governed by certain rules under HIPAA
- Certain secondary market institutions
- Certain research data or employment-related information; and
- Information governed by federal laws, such as HIPAA, Driver's Privacy Protection Act or the Fair Credit Reporting Act

Notably, the NJPA does not contain an entity exemption for HIPAA-regulated entities or exempt data that is processed by nonprofits or institutions of higher education (or educational data subject to FERPA).

The NJPA requires also requires businesses to obtain consent before knowingly processing the personal data of minors between the ages of 13-17 for targeted advertising, sale, or profiling.

Consumer Rights

Consumers who are New Jersey residents will be able to exercise the following rights under the NJPA:

- Right to confirm whether or not their personal data is processed (unless such confirmation or access would require the controller to reveal a trade secret)
- Right to access their personal data
- Right to correct inaccuracies in their personal data
- Right to deletion of their personal data
- Right to portability of their personal data
- Right to opt-out of the processing of their personal data for purposes of (i) targeted advertising, (ii) the sale of personal data, or (iii) profiling in furtherance of decisions that produce legal or similarly significant effects of the consumer's personal data

Business Obligations to Consumers

The NJPA looks a lot like the new New Hampshire law enacted this year and the **business-friendly regulation enacted in Virginia two years ago**, Here are some of the compliance obligations on the horizon for covered businesses:

- Respond to consumer requests under the NJPA without undue delay, but not later than 45 days of receipt of such request (may be extended an additional 45 days when reasonably necessary so long as the controller notifies the consumer of their intent to extend and provide the information for all disclosures of personal data that occurred in the prior 12 months)
- Provide required information to consumers free of charge, once per twelve-month period
- Use commercially reasonable efforts to authenticate requests
- Establish a process for consumers to appeal any refusal to take action on a consumer request

Notices to Consumers

- Businesses must provide consumers with a "reasonably accessible, clear and meaningful" privacy notice that includes, but is not limited to the following:
  - Categories of personal data processed by the business;
  - The purpose of processing personal data;
  - 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);
  - Categories of personal data that the business may share with third parties;
  - Categories of third parties with which the business shares personal data;
  - The process by which the business notifies consumers of material changes to the notification required to be made available pursuant to this subsection, along with the effective date of the notice; and
  - An active email address or online mechanism that the consumer may use to contract the business.

- Businesses must "clearly and conspicuously" disclose any sale of personal data or processing of personal data for targeted advertising (and how to opt-out of such sale or processing)
- Businesses must establish (and describe in a privacy notice), one or more secure and reliable means for consumers to submit a request to exercise their consumer rights, including:
  - A clear and conspicuous link on the business' website (or other prominently accessible location) enabling opt-out of targeted advertising or sale of the consumers personal data; and
  - Not later than July 15, 2025, allow a consumer to opt-out of any processing of the consumer's personal data for the purposes of targeted advertising, or any sale of such personal data.

Other Business Obligations

The Do's:

- **Do** conduct and document data protection impact assessments for data processing that presents a "heightened risk of harm" to the consumer, including targeted advertising, processing of sensitive data, selling personal data, or processing or profiling if the profiling presents an unreasonably foreseeable risk of unfair or deceptive treatment or disparate impact on consumers, financial or physical injury to consumers, or an intrusion offensive to a reasonable consumer upon their "solitude or seclusion, or the private affairs, or concerns." Businesses must provide these assessments to the New Jersey Attorney General Division of Consumer Affairs in the Department of Law and Public Safety upon request
- **Do** limit collection of personal data to what is adequate, relevant, and reasonably necessary in relation to the disclosed purposes for which such data is processed
- **Do** process personal data solely for disclosed purposes or purposes compatible with disclosures, unless the consumer consents (noting that aggregate data is excluded from the definition of personal data)
- **Do** establish, implement, and maintain data security practices

And the Do Not's:

- **Do not** process personal data in violation of state and federal laws that prohibit unlawful discrimination against consumers
- **Do not** discriminate against a consumer for exercising any consumer rights, including denying goods or services, charging different prices or rates for goods or services, or providing a different level of quality of goods and services to consumers
- **Do not** process sensitive data concerning a consumer without obtaining the consumer's consent, or, in the case of the processing of sensitive data concerning a known child, without processing such data in accordance with the federal Children's Online Privacy Protection Act

“Sensitive data” means 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.

Impacts on Vendors/Data Processors

Vendors that are data processors have direct obligations under the NJPA, such as adhering to instructions from data controllers, assisting data controllers with their own compliance obligations, assisting data controllers with data protection impact assessments, and required subcontractor flow-down obligations.

The NJPA also contains specific requirements that must be included in data processing agreements between data controllers and data processors.

Private Right of Action

Like comprehensive data privacy laws in most other states where they have been enacted (except California’s limited private right related to data breaches), the NJPA does not provide for a private right of action. The NJPA is exclusively enforced by the Office of the Attorney General and provides for a 30-day cure period where, prior to brining an enforcement action, the AG will notify controllers and grant an opportunity to cure (if a cure is deemed possible). However, this cure period is not permanent and will sunset 18 months after the law takes effect.

The Director of the Division of Consumer Affairs has rulemaking power to issue additional rules in the future.

Fines and Penalties

Civil penalties are not specified, but the AG may bring violations as constituting a violation of the New Jersey Consumer Fraud Act, which can come with fines of up to $10,000 for the initial violation and up to $20,000 for subsequent violations.

Effective Date for NJPA

January 15, 2025.

Authors

Cynthia J. Larose, Member / Co-chair, Privacy & Cybersecurity Practice

Cynthia J. Larose is Chair of the firm's Privacy & Cybersecurity Practice, a Certified Information Privacy Professional-US (CIPP-US), and a Certified Information Privacy Professional-Europe (CIPP-E). She works with clients in various industries to develop comprehensive information security programs on the front end, and provides timely counsel when it becomes necessary to respond to a data breach.

Jon Taylor, Associate

Jon S. Taylor is an Associate at Mintz who focuses on M&A, private equity deals, debt and equity financings, and general corporate matters. He advises private equity firms, financial services companies, and clients in the technology, health care, manufacturing, and retail industries.