Lowenstein Sandler

Privacy & Cybersecurity

January 12, 2024

New Jersey Adopts a Comprehensive Data Protection Law: What You Need to Know and Do Now

By Mary J. Hildebrand CIPP/US/E, Manali Joglekar CIPP/US, CIPP/E, CIPT, and Judith G. Rubin CIPP/US/E, CIPT

On January 8, 2024, after multiple amendments, the New Jersey Legislature passed a comprehensive data protection bill (SB 332). Gov. Philip Murphy has 45 days to execute SB 332, making New Jersey the 13th state to adopt legislation to protect and secure consumer personal information. The New Jersey Data Protection Act (the Act) will become effective one year from the date of signature.

Who is regulated by the Act?

The Act regulates individuals or entities (referred to as "controllers" or "processors") that conduct business in the state of New Jersey **or** produce products or services that are targeted to residents of the state of New Jersey, **and** during a calendar year eitherr:

- Control or process the personal data of at least 100,000 consumers, excluding personal data processed solely for the purpose of completing a payment transaction; or
- Control or process the personal data of at least 25,000 consumers **and** derive revenue or receive a discount on the price of any goods or services from the sale of personal data.

What type of data is protected by the Act?

The Act applies to the personal data of New Jersey residents ("consumers") acting in an individual or household context. Consumer personal data means "information that is linked or reasonably linkable to an identified or identifiable person" and does not include data that meets the definitions of de-identified or publicly available information. In contrast to the California Consumer Protection Act and the European Union's General Data Protection Regulation, the Act does not apply to business contact data or personal data associated with employees who reside in New Jersey.

As do most state data protection laws, the Act defines a category of "sensitive personal data," but does so with a decidedly broader scope. The Act adds a range of consumer financial information and consumers' status as transgender or nonbinary to data elements frequently identified as sensitive personal data, in other state data protection laws such as data revealing racial or ethnic origin; religious beliefs; biometric data; genetic data; mental or physical health condition, treatment, or diagnosis; sex life or sexual orientation; citizenship or immigration status; personal data of children; and precise geolocation data. Controllers are prohibited from collecting or processing sensitive personal data without first obtaining affirmative consent from the consumer and conducting a data protection assessment. With respect to collection of personal information relating to children under 13, controllers are required to comply with the Children's Online Privacy Protection Act.

Aligned with data protection laws in other states, the Act excludes certain categories of data and entities. For example, the Act adopts Virginia's approach by exempting financial institutions regulated by the Gramm-Leach-Bliley Act and, consistent with the California Consumer Privacy Act, the Act exempts protected health information regulated by the Health Insurance

Portability and Accountability Act of 1996 (HIPAA), but not HIPAA-regulated entities. New Jersey state agencies and related institutions are also exempt from the Act, but the status of nonprofits is not entirely clear. Nonprofits were specifically excluded from the Act through penultimate version of SB 332, but the exemption was struck from the final version.

Consumer rights

The Act grants consumers certain rights regarding their own personal data, including the right to (i) confirm processing; (ii) access personal data; (iii) correct inaccuracies (taking into account the nature of the information and the purposes of processing); (iv) delete personal data; and (v) obtain a copy of their personal data held by the controller in a portable and, to the extent technically feasible, readily usable format that allows the consumer to transmit the data to another entity without hindrance (referred to as the right of "data portability"). Controllers must respond to verified consumer rights requests within 45 days of receipt, with the potential for a 45-day extension.

Consumers also have the right to opt out of the processing of their personal data for the purpose of any sale of data, targeted advertising, or profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer. In accordance with laws in other states, controllers are not required to authenticate opt-out requests and must accept requests through authorized agents; however, controllers may deny fraudulent requests.

Controller obligations under the Act

The Act imposes numerous obligations on controllers including the following, among others:

- Provide consumers with a privacy notice that describes (i) the categories of personal data processed, and the purpose of processing; (ii) the categories of personal data shared with third parties, and the categories of third parties to which the controller discloses personal data; (iii) the process for exercising consumer rights and appealing a rights request decision, (iv) the process for notifying consumers of changes to the privacy notice; and (v) an email address or other online mechanism for consumers to contact the controller.
- Limit the collection of personal data to what is adequate, relevant, and reasonably necessary for the purpose of processing, as disclosed to the consumer, and not process personal data for purposes that are not reasonably necessary for or compatible with the disclosed purpose, without first obtaining consent.
- Implement reasonable administrative, technical, and physical data security practices that are appropriate to the volume and nature of the personal data at issue and that protect the confidentiality, integrity, and accessibility of such personal data.
- Conduct and document data protection assessments when processing personal data acquired on or after the effective date of the Act "presents a heightened risk of harm to consumer(s)." The Act specifically requires assessments for targeted advertising, profiling, selling personal data, and processing sensitive data. These documented assessments may be requested by the New Jersey Attorney General.
- Ensure that agreements with processors such as service providers, vendors and contractors, include appropriate data protection and compliance obligations.
- Provide an effective mechanism for consumers to revoke consent and, upon revocation of such consent, cease to process the relevant personal data as soon as practicable, but no later than 15 days after the receipt of such request.

Universal opt-out mechanism

Within six months following the Act's effective date, a controller that processes personal data for purposes of targeted advertising or the sale of personal data or (assuming the technology is available) profiling that has a legal or similarly significant effect on a consumer is required to allow consumers to exercise their right to opt out of such processing through a user-selected universal opt-out mechanism. An affirmative act by the consumer is required to indicate an opt-out. The New Jersey Attorney General's Division of Consumer Affairs is authorized to adopt regulations on technical specifications applicable to universal opt-out mechanisms, and the Act provides that such specifications be as consistent as possible with the approach taken in other states.

Who enforces the Act?

The Office of the Attorney General has sole and exclusive authority to enforce the Act and the

Division of Consumer Affairs in the Department of Law and Public Safety is authorized to develop associated rules and regulations. There is no provision for a private civil cause of action. The Act provides for a 30-day cure period, but the right to cure expires 18 months after its effective date. Violation of the Act is punishable by penalties of up to $10,000 for the first violation and up to $20,000 for the second and subsequent violations.

What comes next?

Gov. Murphy is expected to sign SB 332 within the allotted 45 days, which would mean the Act becomes effective in the first quarter of 2025. While that may seem a long runway, by then data protection laws in Texas, Florida, Oregon, Montana, and potentially other states, will also be effective, so regulated entities would be well advised to:

- Revisit current data protection programs (and related data inventories) to ensure that all personal data processed by and on behalf of the regulated entity is properly collected, processed, and secured under applicable data protection laws.
- Privacy officers and Legal should closely coordinate with Chief information Security Officers or equivalent, as the Act and its state, federal, and foreign counterparts include substantive cybersecurity requirements.
- Ensure that the regulated entity has an appropriate cyber insurance policy is in place with a reputable carrier.
- Revisit and update the vendor selection process to include compliance with the Act and other applicable data protection laws, confirm that vendors have procured cyber insurance under an acceptable policy, and memorialize the vendors' commitments in appropriate agreements.

Contacts

Please contact the listed attorneys for further information on the matters discussed herein.

MARY J. HILDEBRAND CIPP/US/E
Partner
Chair, Privacy & Cybersecurity
T: 973.597.6308
mhildebrand@lowenstein.com

MANALI JOGLEKAR CIPP/US, CIPP/E, CIPT
Counsel
T: 973.597.2540
mjoglekar@lowenstein.com

JUDITH G. RUBIN CIPP/US/E, CIPT
Counsel
T: 212.419.5908
jrubin@lowenstein.com