



New Jersey Legislature Passes Comprehensive Consumer Privacy Bill

Client Advisories

01.10.2024

By: Kate A. Sherlock

On January 8, 2024, the New Jersey legislature passed the state's first comprehensive consumer privacy bill, Senate Bill S332. S332 follows in the footsteps of other comprehensive state consumer privacy laws and aims to protect consumer personal data, which is broadly defined under the bill as "information that is linked or reasonably linkable to an identified or identifiable person," but excluding de-identified data and publicly available information. As a general matter, the bill grants New Jersey consumers many of the same rights afforded to consumers in states with comprehensive privacy laws, including California, Washington, Colorado, Connecticut, Utah and Virginia. However, there are notable distinctions between S332 and the patchwork of state privacy laws currently in effect, making nationwide compliance difficult to implement. The following alert provides a summary of S332 and some of its key provisions.

Does S332 Apply to My Business?

If you do business in New Jersey and collect personal data from New Jersey residents, you may be subject to S332. S332 applies to businesses that conduct business in New Jersey or produce products or services that are targeted to residents of New Jersey, and (1) "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 (2) "control or process the personal data of at least 25,000 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 bill defines "consumers" as New Jersey residents acting in an individual or household context. Unlike California's law, S332 exempts from the definition of consumers persons acting in a commercial or employment context. The bill also exempts certain types of data and entities, including but not limited to, PHI as defined under HIPAA and HITECH, financial institutions, data, and affiliates of a financial institution that are subject to the Gramm-Leach Bliley Act, and state agencies.

What Does S332 Require?

Privacy Policy and Consumer Rights

S332 requires that a data controller subject to the law provide a privacy notice describing (i) its data collection, processing, and sharing activities, including the categories of personal data it collects and processes, (ii) the purpose for processing the data, (iii) the categories of third parties to which the controller shares the data and the categories of data shared, (iv) consumers' rights with respect to their data and how they may exercise such rights, (v) how material changes to the privacy notice will be communicated, and (vi) an email address or other online mechanism that consumers may use to contact the controller. Consumer rights under the bill include the right to request that the controller delete, correct, or provide access to their personal information. If a controller receives a consumer request to exercise such rights, the controller must verify the request and respond within 45-days of receipt, with a possible 45-day extension.

In addition to the consumer rights outlined above, S332 also provides consumers with the right to opt-out of targeted advertising, the sale of their personal data, and profiling. However, for children ages 13 to 17, affirmative opt-in is required. Additionally, affirmative opt-in is required for processing sensitive personal data, including the personal data of children under 13 (which must be processed in accordance with the Federal Children's Online Privacy Protection Act "COPPA").

Data Processing Agreements

Like most other comprehensive state privacy laws, S332 requires data controllers and their data processors (third-party vendors and service providers) to enter into written data processing agreements outlining the parties' obligations with respect to personal data, including collection and purpose limitations, reasonable security requirements, and requirements that the processor follow the controller's processing instructions and assist the controller in meeting its obligations under law.

Data Protection Assessments

Under S332, controllers must complete a data protection assessment where processing "presents a heightened risk of harm to consumer," such as where the controller will be processing data for targeted advertising, profiling, selling personal data, or processing sensitive data. If requested by the Attorney General, a controller must provide a copy of such assessment.

Universal Opt-Out Mechanisms

S332 also requires controllers to recognize universal opt-out mechanisms (UOOMs) that allow consumers to opt-out of targeted advertising and the sale of their personal data no later than six months after the bill's effective date.

What are the Penalties for Failing to Comply?

Unlike California's law, the New Jersey bill does not include a private right of action, and the bill will be enforced solely by the New Jersey Attorney General who may seek penalties of up to \$10,000 for the first violation and up



to \$20,000 for the second and subsequent violations. The bill also provides a 30-day cure period during the eighteen month period following the bill's enactment date.

The bill directs the Attorney General to promulgate rules and regulations to effectuate the law. We anticipate such rules and regulations to issue sometime between the law's enactment and effective date and to provide additional guidance on consumer rights requests, opt-outs, and data protection assessments.

Next Steps

The bill now moves to Governor Murphy for approval. If he signs the bill, S332 will take effect one year from its enactment date, making New Jersey the 13th state to pass a comprehensive state privacy law. We will continue to monitor its progress and will update you once Governor Murphy signs or vetoes the bill.

If you need assistance in evaluating your business's privacy compliance or if you have any questions or would like more information on the issues discussed in this Advisory, please contact **Kate Sherlock** at 856-673-3919 or ksherlock@archerlaw.com.

DISCLAIMER: This client advisory is for general information purposes only. It does not constitute legal or tax advice, and may not be used and relied upon as a substitute for legal or tax advice regarding a specific issue or problem. Advice should be obtained from a qualified attorney or tax practitioner licensed to practice in the jurisdiction where that advice is sought.

Related People



Kate A. Sherlock

Partner

✉ ksherlock@archerlaw.com

☎ 856.673.3919

Related Services

- Data Privacy & Cybersecurity

© 2025 Archer & Greiner, P.C. All rights reserved.

