Published on *The National Law Review* https://natlawreview.com

New Jersey Legislature Passes Consumer Privacy Bill

Article By:

Kyle R. Dull

Alan L. Friel

On January 8, New Jersey's General Assembly and Senate passed a consumer privacy bill, S332, which would grant New Jersey residents several rights, and obligate controllers and processors of New Jersey residents to take action. The law is similar to consumer privacy laws passed last year in other states, with some distinctions.

Note: In reviewing the text of S332, start your review on page 8, line 31. Text in bold brackets (**[ ]**) was removed by amendment from the bill. If signed by Governor Phil Murphy, most of S332 would take effect one year from the date of enactment, with the requirement to recognize universal opt-out mechanisms ("UOOM") taking effect eighteen (18) months from the date of enactment.

As with the other state consumer privacy laws, S332 covers consumers' personal data, which is broadly defined as "information that is linked or reasonably linkable to an identified or identifiable person," but not including data that meets the definitions of de-identified or publicly available information. This is a similar definition employed by several other states. Consumers are New Jersey residents acting in an individual or household context. Persons acting in a commercial or employment contexts are not consumers under S332. Of the now fourteen consumer privacy laws, only California applies in human resources and business-to-business contexts.

Obligations on Businesses

S332 applies to controllers and processors who 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 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." Section 2. Non-profits, government entities and certain regulated entities and data are exempt.

1. Privacy Notice

Controllers are required to provide a privacy notice that describes (1) the categories of personal data

processed, (2) the processing purpose, (3) the categories of third parties to which the controller discloses personal data, (4) the categories of personal data shared with third parties, (5) how consumers may exercise their rights and how consumers may appeal a rights request decision, (6) how the controller notifies consumers of material changes to the privacy notice, (7) and an email address or other online mechanism that the consumer may use to contact the controller (e.g., a webform or portal). Section 3.a. Third parties are persons, public entities, agencies or other entities that are not controller or processors under the law, or affiliates of such controllers or processors.

2. Data Processing Agreements and Data Protection Assessments

Controllers are required to complete data protection assessments where processing "presents a heightened risk of harm to consumer." Without limitation, data protection assessments are specifically required for (1) targeted advertising, (2) profiling, (3) selling personal data and (3) processing sensitive data. These assessments must be presented to the New Jesey Attorney General upon request. Section 9.b. The bill also places several familiar data processing obligations on controllers and processors which would necessitate the need for a written agreements between such parties outlining such obligations (e.g. collection and purpose limitations, reasonable security requirements, processor adhere to controller instructions and help controller meet its obligations, etc.). Sections 9 and 13.

3. Consumer Rights

Rights requests for deletion, correction, or access (confirm processing, access, copy and portability) request must be verified, and must be responded to within 45-days of receipt, with a possible 45-day extension. Sections 4.a. and 7.a. Consumers also have a right to opt-out of (1) targeted advertising, (2) the sale of personal data and (3) profiling that has a legal or similar effect. Similar to other states, a controller is not required to authenticate opt-out requests, but may deny fraudulent requests, and must accept requests made through authorized agents. Section 4.e and 8.a. For children at least 13 and younger than 17, opt-in rather than opt-out is required. Non-exempted processing of sensitive personal data, including personal data of children under 13, is subject to opt-in consent (with the federal Children's Online Privacy Protection Act applied to personal data of a known child under 13). Section 9.a.4. Sales involve any consideration and targeted advertising does not include data from affiliated websites.

4. Universal Opt-Out Mechanisms

As noted above, within eighteen months following S332 enactment date, controllers must recognize UOOM that enable consumers to opt-out of targeted advertising and the sale of personal data, but not profiling as an earlier bill version proposed. Section 8.b.1. However, consumers may still "designate an authorized agent using technology, including a link to an Internet website, an Internet browser setting or extension, or a global setting on an electronic device, that allows the consumer to indicate the consumer's intent to opt-out of the collection and processing . . . for profiling," "when such technology exists." Section 8.a.

Under S332, a UOOM shall "not make use of a default setting that *opts-in* a consumer to the processing [for purposes of targeted advertising] or sale of personal data, unless the controller has determined that the consumer has selected such default setting and the selection clearly represents the consumer's affirmative, freely given and unambiguous choice to opt into any processing of such consumer's personal data." Section 8.b.(2)(b) (emphasis added). S332's UOOM requirements in Section 8.b.(2) are unique, and at first glance might suggest that UOOM's default setting is opt-out,

but this would conflict with California and Colorado which require the consumer to make an affirmative decision to have the UOOM opt-out of sales, sharing and targeted advertising, and conflict with other provisions in S332. Instead, reading the bill as a whole, the consumer must make an affirmative choice to opt-out of the sale of personal data or the processing of personal data for targeted advertising. See Sections 8.a., 8.b.(2)(e) and 8.c. S332's UOOM opt-in language appears to mean that if a third party creates a UOOM that has the ability to signal an opt-in, that opt-in signal cannot be the default setting and the consumer must affirmatively select the opt-in signal. Reading it as requiring an opt-in to targeted advertising or sales would conflict with the requirements found elsewhere in the bill and would also conflict with the laws and regulations in several other states. So, no signal (opt-in or opt-out) can be set by default and UOOM signals require affirmative consumer action. The law authorizes the New Jersey Attorney General's Division of Consumer Affairs to adopt rules and regulations regarding UOOM technical specifications. Section 15. It also provides that such be as consistent as possible with the approach taken in other states. Section 8.b.(2)(d).

5. Exceptions and Enforcement

S332 also includes several familiar exemptions and exceptions found in other consumer privacy bills. Sections 10 and 12. There is no private right of action under this bill, and it is to be enforced only by the New Jersey Attorney General. Section 16. There will be a cure period for the first eighteen months following the effective date (effective date is one year after the bill is enacted). The Attorney General must also promulgate rules and regulations to effectuate the law. Section 15. Additional guidance on consumer rights requests, verification of requests, effectuating opt-outs, and data protection assessments would likely be in these regulations. Finally, a violation of S332, is a violation of New Jersey's UDAP act, and the Attorney General may seek penalties of up to $10,000 for the first violation and up to $20,000 for the second and subsequent violations. Section 14.a. and P.L.1960, c.39 (C.56:8-1 et. seq).

What happens next?

Because S332 has passed both the General Assembly and Senate, the next step is Governor Murphy's desk. Should Governor Murphy sign the bill, the law would take effect one year from the date it is signed. As S332 was passed on the last day of the two-year legislative session, with a new session starting on January 9, Governor Murphy has seven days to sign the bill. If the bill is vetoed and returned to the legislature, two-thirds of all members of the legislature may override the veto. Because the bill was passed during the final ten days of the session, Governor Murphy may "pocket veto" the bill by failing to sign it. N.J. Constitution, Article V, Section 1, Paragraphs 14(c)(3).

During the year between enactment and the effective date, the Attorney General will likely promulgate rules and regulations to implement the act. As a whole, New Jersey's S332 would grant consumers many of the same rights afforded to consumers in laws already effective in California, Colorado, Connecticut, Utah and Virginia, and in several other states with consumer privacy laws going into effect in 2024 and 2025. However, there are some material differences between these various laws. If signed by Governor Murphy, S332 would add another state to the patchwork of consumer privacy laws in the United States and require businesses to parse which laws apply to them and decide how they are going to implement the requirements of each law in a meaningful and realistic manner.

National Law Review, Volume XIV, Number 9

Source URL:https://natlawreview.com/article/new-jersey-legislature-passes-consumer-privacy-bill