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

Washington State's GDPR-like Bill Passes Senate

Article By:

Joseph J. Lazzarotti

Jason C. Gavejian

Maya Atrakchi

The California Consumer Privacy Act (CCPA), passed in 2018 and taking effect January 1, 2020, is considered the most expansive state privacy law in the United States, and sparked a flurry of state privacy law legislative proposals, in particular in Washington state. This January, a group of state senators in Washington introduced the Washington Privacy Act, SB 5376 (WPA), slightly updated in late February. On March 6th, the bill passed the Senate with a nearly unanimous vote, and now heads to the House for review. If approved, the WPA will take effect July 31, 2021.

Unlike other states that are modeling their bills largely on the CCPA (*e.g.* Hawaii, Maryland, New Mexico), the WPA would establish more GDPR-like requirements on businesses that collect personal information related to Washington residents. In fact, the WPA's legislative findings explicitly state that Washington residents "deserve to enjoy the same level of privacy safeguards", as those afforded to EU residents under the GDPR. In addition to requirements for notice, and consumer rights such as access, deletion, and rectification, the WPA would impose restrictions on use of automatic profiling and facial recognition.

Below are key aspects of the WPA:

- *Jurisdictional Scope*. The WPA would apply to legal entities that conduct business in Washington or produce products or services intentionally targeted to residents of Washington, and that satisfy one or more following thresholds: Controls or processes data of 100,000 consumers or more; or Derives over 50% of gross revenue from the sale of personal information and processes or controls personal information of 25,000 consumers or more. The bill includes exemptions for personal data regulated by HIPAA, HITECH, or the GLBA, and *data sets maintained for employment record purposes.* Personal data is defined vaguely to include any information relating to an identified or identifiable natural person.
- *Consumer Rights.* Washington residents are afforded the power to request that controllers of their personal data:
    - provide them with confirmation whether their personal information is being processed by the controller or sold to a third-party;
    - provide them with a copy of the personal data undergoing process;

    - correct inaccurate personal data;
    - delete their personal data under specified circumstances (*g.* personal data is no longer necessary in relation to the purpose for which it was collected, the processing is for direct marketing purposes, personal data has been unlawfully processed).
- In general, businesses in the U.S. are used to needing only implied or negative consent from customers with respect to the collection and use of their data. The WPA would require consent to be a "clear affirmative act establishing a freely given, specific, informed, and unambiguous indication of a consumer's agreement to the processing of personal data relating to the consumer, such as by a written statement or other clear affirmative action."
- *Controllers and Processors.* In general, controllers determine the purposes and means of processing personal data, while processors process personal data on behalf of the controllers. Thus, under the WPA, controllers would be responsible for meeting the requirements of the WPA, while processors are responsible for following the instructions of their controllers and assisting them with meeting the requirements of the law. Contracting between the parties will be critical.
- Controllers must be transparent and accountable for processing of personal data by making a "meaningful," "clear," and "reasonably accessible" privacy notice available (although the language in the bill is less than clear). Notice must include: the categories of personal data collected, the purpose for which personal data is disclosed to third parties, the rights the consumer may exercise, the categories of personal data shared with third-parties, the categories of third-parties with whom the controller shares data.
- *Risk Assessments.* Controllers must conduct and document risk assessments covering the processing of personal data prior to the processing of such personal data whenever there is a change in processing that materially impacts the risk to individuals, and on at least an annual basis regardless of changes in processing.
- A controller in violation of the law is subject to an injunction and liable for a civil penalty of not more than $2,500 for each violation or $7500 for each intentional violation.

It is worth noting that unlike California's CCPA which leaves open the possibility of application to employee data, the WPA explicitly states that a protected "consumer" *does not include an employee or contractor of a business acting in their role as an employee or contractor*. Moreover, as already mentioned above, data sets maintained for employment record purposes are exempt from the jurisdictional scope. That said, the WPA is not yet final, and could be revised during the legislative process to include employee data.

States across the country are contemplating ways to enhance their consumer privacy and security protections. For example, we recently spotlighted New Jersey in two posts (available here and here), detailing several NJ Assembly bills relating to privacy and security, currently under consideration. Organizations, regardless of their location, should be assessing and reviewing their data collection activities, building robust data protection programs, and investing in written information security programs (WISPs).

National Law Review, Volume IX, Number 88