

Publications

Client Alert: New Push for Another U.S. Privacy Law as Washington State Senate Approves the Washington Privacy Act (SB 6281)

Related Attorneys

John L. Landolfi

Christopher L. Ingram

Gretchen Rutz Leist

Related Services

Data Strategy, Privacy and Security

CLIENT ALERT | 2.18.2020

Washington legislators recently reintroduced the Washington Privacy Act (WPA). The bill sailed through the Senate in less than a month and is now before the House, where a prior version of the legislation failed last year. This year's version was revised to address some of the privacy concerns that blocked the prior bill. In many respects the WPA resembles the EU's General Data Protection Regulation (GDPR) and would impose more privacy restrictions than the California Consumer Privacy Act (CCPA).

As **currently drafted**, the WPA would apply to companies that conduct business in Washington or produce products or services that are targeted to Washington residents and either (a) control or process the personal data of 100,000 or more consumers, or (b) derive over 50% of their gross revenue from the sale of personal data and process or control personal data of 25,000 or more consumers.

If enacted, the WPA would grant consumers new rights over their personal data. Some of these rights overlap with the rights granted under California's law, but there would be distinctions. The WPA grants the following rights:

- **Right of access:** a consumer has the right to confirm whether a controller is processing their personal data and to access that data.
- **Right to data portability:** a consumer has the right to access their data in a portable, "readily usable" format.
- **Right to correction:** a consumer has the right to correct inaccurate personal data about them.
- **Right to deletion:** a consumer has the right to delete their personal data.
- **Right to opt out:** a consumer has the right to opt out of the processing of their personal data for targeted advertising, the sale of personal data, or profiling.
- **Right to exercise privacy right without discrimination:** a consumer can exercise their privacy rights under the law without

discrimination.

A special subset of data, “sensitive data,” requires **opt in consent** from consumers before it can be processed. **Sensitive data** includes personal data revealing racial or ethnic origin, religious beliefs, mental or physical health conditions or diagnosis, sexual orientation, citizenship or immigration status, unique biometric data, data from a known child (under 13), and specific geolocation data. The WPA also places affirmative duties on processing facial recognition data.

The WPA would also require many companies to revisit their privacy policies to reflect among other things, their practices for the collection, use, and dissemination of personal data, along with a description of how consumers can exercise their rights under the WPA.

Another key requirement tucked in the WPA is a requirement for certain companies to conduct and document a **data protection assessment** to evaluate how they:

- Process personal data for targeted advertising;
- Sell personal data;
- Process personal data for the purpose of profiling;
- Process sensitive data; and
- Process personal data in any way that presents a heightened risk of harm to consumers.

The WPA would allow the Washington attorney general to request copies of data protection assessments to evaluate the company’s compliance with the WPA. Additionally, the law would require some companies to limit their collection of personal data to a specified purpose and adhere to practices of data minimization, reasonable security, and use limitations. None of the privacy rights granted by the WPA are waivable by contract or agreement of any kind.

The WPA gives Washington’s attorney general exclusive authority to enforce the WPA, and does not provide a private right of action. Violations of the WPA could result in a civil penalty of up to \$7,500 per violation.

Should the WPA be enacted, it would take effect **July 31, 2021**.

Current Status of the WPA

One of the reasons the last year’s version did not pass was because legislators were concerned about its limited protections for commercial use of facial recognition technology. The 2020 bill strengthens protections for consumers against the use of facial recognition technology. For example, it requires testing of the technology to ensure that it is used accurately and fairly, posting conspicuous notice explaining that facial recognition is in use and the purpose for its use, and requiring opt-in consent for enrolling images in facial recognition services in certain circumstances. The WPA is scheduled to be taken up by the House Innovation, Technology & Economic Development committee this Friday.

For any questions regarding the WPA, the CCPA, or privacy laws in general, please contact John Landolfi, Christopher Ingram, Gretchen Rutz, or your Vorys attorney.