The Washington Privacy Act Gets its Third Bite at the Apple

Related Attorneys

John L. Landolfi

Christopher L. Ingram

Christopher A. LaRocco

Gretchen Rutz Leist

Related Services

Data Strategy, Privacy and Security

CLIENT ALERT | 1.20.2021

After failing to pass in 2019 and 2020, the Washington state legislature has introduced a comprehensive consumer privacy law for a third year in a row. This year's version, the 2021 Washington Privacy Act (the "WPA") contains many of the same concepts, business obligations, and consumer rights as the recently-passed California Privacy Rights Act (CPRA), and also borrows concepts from Europe's General Data Protection Regulation (GDPR). A copy of the bill can be found here.

The WPA applies to legal entities that conduct business in Washington and either: (1) control or process personal data of 100,000 consumers or more during a calendar year; or (2) derive over 25% of their gross revenue from the sale of personal data. Like the CPRA, "personal data" is broadly defined to include any information that is "reasonably linkable to an identified or identifiable natural person."

Below are seven key things to know about the WPA.

1. Creates New Consumer Rights

Like the CCPA/CPRA and GDPR, the WPA grants consumers certain rights, including: (1) the right to confirm whether or not a business is processing personal data concerning the consumer and the categories of personal data the business is processing; (2) the right to correct inaccurate personal data; (3) the right to delete; (4) the right to data portability; and (5) the right to opt out of targeted advertising, the sale of personal data, and automated decision-making.

2. Mandates Appeal Process for Rejected Consumer Requests

The WPA is the first U.S. privacy law to require that businesses create an internal process for consumers to appeal rejected consumer requests. Businesses must respond to an appeal within 30 days with a written explanation of the reasons affirming or reversing the initial decision. This report must be sent to the consumer and can ultimately be passed on to the Washington attorney general.

3. Requires Data Protection Assessments

The WPA requires businesses to conduct a "data protection assessment" when engaging in certain activities such as processing data for targeted advertising or processing sensitive data. These assessments identify the potential risk to consumers posed by the particular processing at issue and weigh that risk against the benefits of the processing activity. These assessments must be produced to the Washington attorney general upon request.

4. Obligates Businesses to Create a Privacy Notice

Like the CCPA and CPRA, the WPA requires a consumer privacy notice, and specifies what must be included in that privacy notice.

5. Provides New Restrictions Related to Public Health Emergencies

In response to the COVID-19 pandemic, the WPA creates specific restrictions surrounding the handling of personal data collected during public health emergencies. Most notably, the bill requires that businesses give notice and receive consent when processing certain "covered data" (geolocation, proximity data, or personal health data) for a "covered purpose" (contact tracing, symptom detection, and similar activities).

6. Places New Restrictions on "Sensitive Data"

Like the CPRA, the WPA creates separate restrictions for "sensitive data," which include things like race, religion, sexual orientation, citizenship, biometric data, and personal data known to be from a child (under 13). Under the WPA, a business must obtain consent before processing sensitive data.

7. Restricts Processing of Personal Data

The WPA creates the new restriction that businesses, regardless of what their privacy notice provides, may not process personal data for purposes that are not "reasonably necessary to, or compatible with the purposes for which the personal data is processed" unless the business obtains the consumer's consent.

The Washington legislature failed to pass similar versions of the WPA in 2019 and 2020, as legislators could not reach an agreement on the inclusion of a private right of action. The 2021 version of the WPA takes a somewhat hybrid approach: it is enforced exclusively against businesses by the state attorney general, but provides a narrow private right of action against government entities in public health emergencies. Under the WPA, the attorney general could impose fines of up to $7,500 per violation, plus the state would be able recover its investigation and attorney's fees. If passed, the primary components of the WPA would become effective on July 31, 2022.

For assistance with creating or reviewing your organization's privacy compliance program or privacy laws in general, please contact John Landolfi, Christopher Ingram, Christopher LaRocco, Sarah Boudouris, Gretchen Rutz, or your Vorys attorney.