Oregon Expected to Pass Consumer Privacy Law: 8 Things Businesses Need to Know

Insights
7.03.23

Businesses should prepare now for a potential new law in Oregon designed to provide consumer privacy rights regarding access to and control over personal data collected by covered entities. The state legislature recently passed the Oregon Consumer Privacy Act (OCPA), which now moves to Governor Tina Kotek for consideration. If approved, Oregon will become the eleventh state — and the sixth in just 2023 alone — to pass comprehensive consumer privacy legislation. The OCPA follows in the footsteps of similar laws passed in California, Virginia, Colorado, Utah, Connecticut, Iowa, Indiana, Tennessee, Montana, and Texas. Assuming that the legislation is approved by the Governor in its current form, here are the answers to your top eight questions about the OCPA.

1. When Will the OCPA Take Effect?

For-Profit Organizations - The OCPA will take effect on July 1, 2024. In comparison to similar legislation passed in other states, this is a very short period for covered entities to prepare. For example, the Tennessee and Indiana laws, which were both passed earlier in 2023, will not become effective until July 1, 2025, and January 1, 2026, respectively.

Nonprofit Organizations - The OCPA exempts only certain nonprofit organizations. For covered nonprofit organizations, the OCPA becomes effective on July 1, 2025.

2. Will the Law Apply to Your Business?

The OCPA will apply to any person that conducts business in Oregon or that provides products or services to Oregon residents, and controls or possesses the following data during a calendar year:

- The personal data of 100,000 or more consumers (other than personal data controlled or processed solely for the purpose of completing a payment transaction); or
- The personal data of 25,000 or more consumers, while deriving at least 25% of the person's annual gross revenue from selling personal data.

"Consumer" is defined to mean a natural person who resides in Oregon and acts in any capacity other than in a commercial or employment context.

"Personal data" means data, derived data, or any unique identifier that is linked to or is reasonably linkable to a consumer or to a device that identifies, is linked to, or is reasonably linkable to one or more consumers in a household. However, "personal data" excludes deidentified data or data that: (1) is lawfully available through government records or through widely distributed media; or (2) a controller reasonably has understood to have been lawfully made available to the public by a consumer.

Similar to the Colorado Privacy Act, the OCPA does not provide a full exemption for nonprofit organizations. The OCPA only exempts (1) a non-profit organization that is established to detect and prevent fraudulent acts in connection with insurance, and (2) the non-commercial activity of a nonprofit organization that provides programming to radio or television networks.

The OCPA does not provide entity-level exemptions for organizations subject to the Health Insurance Portability and Accountability Act (HIPAA) or the Gramm-Leach-Bliley Act (GLBA). However, it does contain data-level exemptions for these organizations.

3. Are Employees Treated As Consumers?

No. The definition of "consumer" excludes those acting in an employment context. Moreover, the OCPA does not apply to information processed or maintained solely in connection with, and for the purpose of, enabling:

- An individual's employment or application for employment;
- An individual's ownership or function as a director or officer of a business entity;
- An individual's contractual relationship with a business entity; or
- An individual's receipt of benefits from an employer, including benefits for the individual's dependents or beneficiaries.

4. What Rights Will Consumers Have?

The OCPA provides consumers with access, correction, deletion, opt-out, and data portability rights:

- **Access** - A consumer's access rights include the right to confirm whether the controller is processing or has processed the consumer's personal data and the categories of personal data that the controller is processing or has processed. Consumers will also be able to obtain a copy of their personal data that the controller has processed or is processing. A consumer will also have the right, at the controller's option, to obtain a list of specific third parties (other than natural persons) to which the controller has disclosed the consumer's personal data or any personal data.
- **Correction** - Consumers will have the right to require a controller to correct inaccuracies in

their personal data.

- **Deletion** - Consumers will have the right to require a controller to delete their personal data, including personal data that the consumer provided to the controller and personal data the controller obtained from another source.
- **Opt-out** - Consumers will have the right to opt-out from a controller's processing of their personal data that the controller processes for purposes of targeted advertising, selling the personal data, or profiling the consumer.
- **Data portability** - Controllers are required to provide personal data to a consumer in a portable and, to the extent technically feasible, readily usable format that permits the consumer to transmit the personal data to another person without hindrance.

5. What About Biometric Data?

The OCPA defines biometric data to mean "personal data generated by automatic measurements of a consumer's biological characteristics, such as the consumer's fingerprint, voiceprint, retinal pattern, iris pattern, gait or other unique biological characteristics that allow or confirm the unique identification of the consumer."

Connecticut's Data Privacy Act also defines biometric data, which is "data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, a voiceprint, eye retains, irises or other unique biological patterns or characteristics that are used to identify a specific individual." *Notably, Connecticut requires usage, while the OCPA does not.*

6. What About Sensitive Data?

The OCPA prohibits controllers from processing a consumer's sensitive data without first obtaining consent from the consumer. If the controller knows that the consumer is a child, the controller must process data in accordance with the Children's Online Privacy Protection Act of 1998.

Oregon's definition of sensitive data is broader than the definitions used in other states' consumer privacy laws. While it includes traditional categories such as data pertaining to racial/ethnic origin and religious beliefs, the OCPA also includes status as transgender or non-binary and status as a victim of a crime in its definition of sensitive data.

7. Can Individuals Bring an Action for Violation of the OCPA?

No. There is no private right of action that would permit an individual to sue for violations.

The Oregon Attorney General has the sole authority to enforce the OCPA and may file an action seeking a maximum of $7,500 per violation or to enjoin a violation. These actions are subject to a five-year statute of limitations.

A court may award reasonable attorneys' fees, expert witness fees, and costs of investigation to the Attorney General if it prevails in an action under the OCPA. A court may also award reasonable attorneys' fees to a defendant that prevails in an action under the OCPA if the court finds that the Attorney General had no objectively reasonable basis for asserting the claim or for appealing a trial court's adverse decision.

The OCPA also requires the Attorney General to notify a controller of a violation if the Attorney General determines that the controller can cure the violation. The Attorney General may then bring an action if the controller fails to cure the violation within 30 days. However, this requirement has a sunset date of January 1, 2026.

8. What Should Businesses Be Doing?

If your business will be subject to the OCPA, you should be taking immediate action to prepare for compliance — particularly given the short window of time before the anticipated effective date. This may include:

- assessing your current data collection and privacy practices;
- conducting an inventory of data; and
- working with data privacy counsel.

Your compliance plan can be fast-tracked with the help of Fisher Phillips' Consumer Privacy Team. We are prepared to work with your organization on steps such as a privacy gap assessment, data inventory, and drafting compliant privacy notices and policies.

Conclusion

For further information, contact your Fisher Phillips attorney, the author of this Insight, or any attorney on the firm's Consumer Privacy Team. Fisher Phillips will continue to monitor consumer privacy law developments and will provide updates as warranted, so make sure that you are subscribed to Fisher Phillips' Insight System to get the most up-to-date information direct to your inbox.

Related People

Jeffrey M. Csercsevits
Partner
610.230.2159
Email

Service Focus

Privacy and Cyber

Related Offices

Portland