Insights, News & Events

# CONSUMER PRIVACY COMPLAINTS POURING IN FROM OREGONIANS: HOW YOUR BUSINESS CAN AVOID TOP COMPLIANCE ISSUES NOTED BY STATE'S A.G.

Insights
Apr 1, 2025

Oregon consumers submitted more than 100 privacy complaints to the state's justice department within six months of the Oregon Consumer Privacy Act (OCPA) taking effect, and businesses subject to the new law need to take note. A new report, released by Attorney General Dan Rayfield on March 7, identifies the top issues driving the complaints and enforcement actions. The good news? The AG's office will continue to give companies a 30-day window to cure violations – but the OCPA mulligans will end January 1, 2026. We break down the most common mistakes in this Insight, along with how your business can stay on the right side of the law.

**Brief Summary of the OCPA**

The OCPA, which took effect July 1 last year, provides consumer privacy rights regarding access to and control over personal data collected by covered entities. While employees are not considered consumers under the OCPA and data collected in the employment context is exempt, the law applies to businesses (referred to as "controllers") operating in Oregon or offering products or services to Oregon residents. Specifically, it applies to those businesses handling the personal data of either:

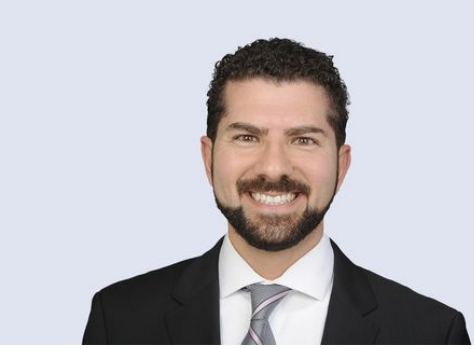
- 100,000 or more Oregon consumers in a calendar year; or
- 25,000 Oregon consumers in a calendar year if at least 25% of their revenue comes from selling personal data.

## Related People

**Darcey M. Groden, CIPP/US**

Partner

858.597.9627



**Usama Kahf, CIPP/US**

Partner

949.798.2118

The state's 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. However, for violations identified during the law's "cure period" – which will expire on January 1, 2026 – the state must send the controller a "cure notice" if the AG believes the issues are fixable and give the controller 30 days to address the issues identified.

You can read more about the OCPA, and how it differs from other states' privacy laws, here.

**New Report Summarizes State's Initial OCPA Enforcement Efforts**

According to Enforcement Report released March 7, the Oregon Department of Justice's (DOJ) Privacy Unit:

- received **110 consumer complaints** by 2025; and
- in the past six months, issued **21 cure letter matters** (which each included an inquiry letter, plus a letter with both inquiry and cure components) and **additional "light" cure letters** (to businesses who made only minor mistakes in their privacy notices).

The report notes that the volume of consumer complaints shows that "Oregonians care about their privacy rights, and that they are engaged with the process." It also highlights some common deficiencies in companies' privacy notices, including **failures to provide**:

- **adequate disclosures** (for example, failing to include any notice of consumer rights under the OCPA, or failing to sufficiently explain how to exercise those rights, such as the right to request a list of third parties a consumer's data has been sold to);
- notices that are **clear and accessible** to the average consumer (for example, misleading consumers by naming one or two states in the "your state rights" section without identifying Oregon); or
- **proper rights mechanisms** (such as requiring inappropriately difficult authentication requirements).

**5 Next Steps for Oregon Controllers**

**Rachel Song**

Associate

415.926.7651

## Service Focus

Consumer Privacy Team

Privacy and Cyber

## Resource Hubs

U.S. Privacy Hub

## Related Offices

Portland, OR

The report emphasizes the DOJ's focus on transparency when enforcing the OCPA. Given this agenda, here are five action items Oregon controllers can implement to stay compliant:

**1. Explain how Oregon consumers can exercise their privacy rights**. It can be difficult to write a privacy notice and operationalize privacy rights which comply with the myriad of state consumer privacy laws. Nevertheless, your businesses must identify which state consumer privacy laws apply and include all necessary disclosures and consumer rights for those states (including Oregon). This can be done without having to call out specific states and what each state requires – instead, you can describe all of the consumer rights provided by all applicable state laws and state that those rights may or may not apply depending on the consumer's state of residence. Be careful not to mislead consumers into thinking that privacy rights do not apply to them.

**2. Revise privacy policies to clarify unclear provisions**. Businesses should step into their consumers' shoes and evaluate whether their privacy policies make sense to a layperson who is not familiar with consumer privacy laws. Write your privacy policies in plain and straightforward language, and avoid legalese or highly technical language. Ensure that the privacy notices are not inadvertently misleading.

**3. Establish simple method for consumers to exercise their rights**. Businesses should also implement mechanisms for consumers to exercise each of their O.C.K.E.D. rights, and these mechanisms should be clearly and plainly laid out in your privacy policy. Make sure to provide a clear and conspicuous link that consumers can use to opt-out of targeted advertising, selling of personal data, and certain types of profiling. Also, authentication procedures should not be so difficult that it prevents consumers from exercising their rights. When opting out, the OCPA does not permit authentication – businesses should not ask for more information than that needed to identify the consumer who made the request to opt-out. Moreover, for requests that do permit authentication, the requests should not be "inappropriately difficult" (to quote the DOJ). Authentication should not be difficult for the actual consumer – it should only be a challenge for people who are not the consumer making the request.

**4. Assess whether you are a nonprofit that must comply**. Nonprofit organizations that otherwise qualify as a "controller" will have to comply with the OCPA starting on July 1 this year, subject to two very narrow exemptions for nonprofits established to detect or prevent fraudulent, insurance-related acts or and nonprofits that provide programming to radio or television networks.

**5. Keep an eye on enforcement trends in other states**. Enforcement trends in other states may inform or provide a preview for enforcement trends that the DOJ could pursue next. Indeed, the DOJ's focus on noncompliant notices, issues with exercising rights, and the opt-out mechanism reflect concerns raised by regulators in other states, including California. Looking at other state's enforcement priorities may give you a sneak peak of what is on the horizon – and allow your business to fix issues before a regulator looks at your business.

**Conclusion**

We will continue to monitor developments and provide updates as warranted, so make sure you subscribe to Fisher Phillips' Insight System to gather the most up-to-date information. Should you have any questions on the implications of these developments and how they may impact your operations, contact your Fisher Phillips attorney, the authors of this Insight, or any attorney in our Privacy and Cyber Practice Group.