



OREGON CONSUMER PRIVACY ACT (OCPA)

CHECKLIST



USERCENTRICS

Oregon Consumer Privacy Act (OCPA), gives Oregon residents rights over how their personal data is collected and used.

This checklist walks through steps that support your compliance efforts under the Act, along with recommended best practices for privacy-related user experience.



Important to know:

Action	Date
Effective date	July 1, 2024 (nonprofits: July 1, 2025)
Retroactive	No
Mandatory cure period	Expired January 1, 2026
2026 amendments	Universal opt-out mechanism now mandatory; outright ban on sale of personal data of consumers under 16; outright ban on sale of precise geolocation data for all Oregon consumers

1 Determine If Your Company Is Required to Comply

If your organization, including nonprofits since July 1, 2025:

- Controls or processes personal data of at least 100,000 consumers, or
- Controls or processes personal data of at least 25,000 consumers, and derives 25 percent or more of annual gross revenue from selling personal data

Note: The OCPA differs from most peer laws as it largely exempts specific data or activities rather than entire organizations. Nonprofits are not broadly exempt, with only a narrow insurance-fraud carve-out.

Exempted organizations and activities:

- Governmental agencies, public corporations, and public bodies
- Financial institutions and their affiliates/subsidiaries, focused exclusively on financial activities
- Insurers, insurance producers, insurance consultants, and licensed third-party administrators
- Nonprofit organizations established to detect and prevent insurance fraud
- Non-commercial activities of publishers, editors, and reporters connected with newspapers, magazines, or similar publications
- Non-commercial activities of FCC-licensed radio and television stations
- Press, wire, or other information services

Personal data exempt under the following federal laws:

- [HIPAA](#)
- [GLBA](#)
- Health Care Quality Improvement Act
- [FCRA](#)
- Driver's Privacy Protection Act
- FERPA
- Airline Deregulation Act
- Patient-identifying substance-use research data (42 U.S.C. § 290dd-2)

2 Create a Comprehensive Privacy Policy

Businesses are required to inform consumers at or before the point of data collection about:

- Categories of personal data processed, including sensitive data
- Purposes for which data is processed
- Categories of personal data the controller shares with third parties, if any
- Categories of third parties the controller shares personal data with, if any
- Identity of the controller, including any business name(s) under which it is registered or operates in the state

Rights: Inform website visitors of their privacy rights and how to exercise them, including how to appeal a controller's decision.

Language: Keep the [privacy policy](#) clear and easy to understand.

Implementation: As a best practice, pair the privacy notice with an opt-out mechanism. For example, use a banner or popup when visitors visit your site, [powered by a CMP](#).

3 Disclose Targeted Advertising and Profiling Practices

Clearly disclose in your privacy notice any processing of personal data for targeted advertising or profiling, and how a consumer may opt out. For example, use a [Privacy Policy Generator](#).

4 Honor Universal Opt-Out Signals

Recognize a consumer's opt-out preference signal, such as [Global Privacy Control \(GPC\)](#), as a valid method of opting out of the sale of personal data and targeted advertising. This became mandatory January 1, 2026.

5 Do Not Sell Personal Data of Consumers Under 16, or Precise Geolocation Data

Since January 1, 2026, the sale of personal data of a consumer the controller knows to be under 16 is prohibited outright, regardless of consent. The sale of precise geolocation data is also prohibited outright for all Oregon consumers.

6 Inform Consumers About Their Rights

Consumers' rights under the OCPA:

- **Right to access:** Request and receive a copy of their personal data and information about third parties it's shared with
- **Right to correction:** Updates or corrections to inaccuracies in personal data collected
- **Right to deletion:** Personal data that has been collected about them (with exceptions)
- **Right to data portability:** Copy of personal data must be provided in a portable and readily useable format
- **Right to opt out:** Of processing of personal data for the purposes of sale, targeted advertising, or profiling
- **Right to nondiscrimination:** For exercising privacy rights
- **Right of minors:** Consent must be obtained from a parent or guardian before children's (under age 13) personal data is collected, or directly from individuals between the ages of 13 and 15
- **Right to restrict sensitive personal information:** Limit or refuse the collection or use of personal data the law classifies as sensitive

7 As a Best Practice, Review and Update Your Privacy Policy Every 12 Months

Review your operations and any changes in the law every 12 months. Update the privacy policy and its effective date, even if no other changes are made.

Transparency: Keep the information visitors must be notified about clear, comprehensive, and up to date, with the last-update date clearly visible.

Data sold: List all categories of personal information your business has sold in the past 12 months.

8 Enable Clear Options When Consent Is Required

When: If the personal data collected is sensitive, or that of a child.

Availability: Easily accessible on your website.

Method: Via a CMP.

9 Authenticate Consent for Collection of Sensitive Personal Data or Data From Minors

Sensitive personal data: Consent is required for processing [sensitive personal data](#).

Consent for children: Obtain consent from a parent or legal guardian for collection of personal data if the data subject is 13 or younger, or directly from the individual if they are between 13 and 15, including for targeted advertising or profiling.

10 Enable Consumers to Make Data Subject Access Requests (DSARs)

Provide one or more contact options (e.g., toll-free phone number, web form, email). Set up a system to enable submission of [DSARs](#).

11 Set Up a System to Verify Data Subject Access Requests (DSARs)

As a best practice, enable consumers to attach documentation to help verify their identity and residency. If your business cannot reasonably verify a consumer's identity, inform them and explain why, and enable them to rectify.

12 Keep Track of Data Subject Access Requests (DSARs)

Set up a system to track all requests. Keep records of requests and responses for two years after the last consumer interaction.

13 Fulfill Data Subject Access Requests (DSARs)

Respond within 45 days from the date the request is received, extendable by an additional 45 days if the business notifies the consumer of the extension and its reason within that first 45-day window.

Falling thresholds, rising enforcement and litigation, eroding ad revenue. Do you know your risk?

GET IN TOUCH