



Jul 11, 2023

Categories:

[Publications](#)

Authors:

[Jean Paul Yugo](#)

[Nagashima](#)

[Gene F. Price](#)

[Lauren E. Cole](#)

Oregon Likely Next State to Pass Comprehensive Data Privacy Legislation

On June 22, 2023, Oregon's state legislature passed the Oregon Consumer Privacy Act (OCPA). Currently, the bill for the OCPA is awaiting signature by the Governor. If it becomes law, most of the Act will go into effect on July 1, 2024, and the remaining sections (discussed below) will go into effect on January 1, 2026.

[Who Does the OCPA Apply To?](#)

The OCPA applies to companies that conduct business in Oregon or provide products and services to Oregon residents and companies that annually control or process:

- The personal data (except personal data controlled or processed solely for the completion of a payment transaction) of 100,000 or more consumers; or
- The personal data of 25,000 or more consumers while deriving 25% or more gross revenue from personal data sales.

Public corporations, i.e., an entity created by the state to carry out public missions and services are exempted from the OCPA. As with other state privacy laws, the OCPA does not apply to information otherwise covered by HIPAA, employment information, information collected by nonprofit organizations, and information that originates from certain noncommercial activities.

[Who Does the OCPA Protect?](#)

The OCPA protects "consumers" that are (1) natural person[s] who reside in Oregon and (2) act in any capacity other than in a commercial or employment context. This means business-to-business (B2B) and employment-related activities are not within the scope of the OCPA.

What Type of Data is Protected by the OCPA?

Under the OCPA, “personal data” is defined as “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.” Like other state privacy laws, personal data also includes a subcategory of sensitive data which receives additional protection, such as data protection assessments (discussed below).

“Sensitive data” is defined as personal data that:

- reveals a consumer’s racial or ethnic background, national origin, religious beliefs, mental or physical condition or diagnosis, sexual orientation, status as transgender or non-binary, status as a victim of crime or citizenship or immigration status;
- is a child’s personal data;
- identifies within the radius of 1,750 feet a consumer’s present or past location, or the present or past location of a device that links or is linkable to a consumer by means of technology that includes, but not limited to, a global positioning system that provides latitude and longitude coordinates; or
- reveals genetic or biometric data.

As opposed to personal data which businesses are allowed to process data until consumers opt-out of sale or sharing for targeted advertising, businesses must first obtain consumer’s consent to process sensitive data.

What are Some Responsibilities for Controllers?

“Controllers” under the OCPA include any person (whether acting alone or jointly with another person) who determines the purposes and means for processing personal data. Such a person is thereby limited by certain responsibilities.

- The controller can only process personal data to the extent that the processing is adequate and reasonably necessary for,

relevant to, proportionate in relation to and limited to the purposes set forth in the OCPA.

- The controller is required to obtain the consumer's consent to collect sensitive data (as discussed above).
- The controller shall provide consumers with a reasonably accessible, clear, and meaningful privacy notice that:
 - lists the categories of personal data, including the categories of sensitive data, that the controller processes;
 - describes the controller's purposes for processing the personal data;
 - describes how the consumer may exercise their consumer's rights under the OCPA, including how a consumer may appeal a controller's denial of a consumer's requests;
 - lists all categories of personal data, including the categories of sensitive data, that the controller shares with third parties;
 - describes all categories of third parties with which the controller shares personal data at a level of detail that enables the consumer to understand what types of entity each third party is and, to the extent possible, how each third party may process personal data;
 - specifies an electronic email address or other online methods by which a consumer can contact the controller that the controller actively monitors;
 - identifies the controller, including any business name under which the controller registered with the Secretary of State and any assumed business name that the controller uses in this state;
 - provides a clear and conspicuous description of any processing of personal data in which the controller engages for the purposes of targeted advertising or profiling the consumer in furtherance of decisions that produce legal effects or effects of similar significance, and a procedure by which the consumer may opt out of

this type of processing; and

- describes the method or methods the controller has established for a consumer to submit a request under the OCPA.

What Rights Do Consumers Have Under the OCPA?

Under the OCPA, consumers have certain rights that they can exercise. Those are:

- **Right to Access:**

- The right to receive confirmation of the processing of their personal data and the categories of personal data processed;
- The right to receive a list of third parties, other than natural persons, who received any of the consumer's personal data or any personal data; and
- The right to receive a copy of their personal data that has been processed or is processing;

- **Right to Correct:** Consumers can require a controller to correct inaccuracies in personal data about the consumer;

- **Right to Delete:** Consumers can require a controller to delete their personal data, including personal data the consumer provided to the controller or personal data derived or received from another source; and

- **Right to Opt-out:** Consumers can opt-out from a controller's processing of their personal data for targeted advertising, sale of personal data, or profiling the consumer for decisions that would have a legal effect.

What is A "Sale" Under the OCPA?

The OCPA defines "sale" as "the exchange of personal data for monetary or other valuable consideration by the controller with a third party," compared to some other states that also consider the exchange of non-monetary consideration as a "sale."

Are Data Protection Assessments Needed?

In certain circumstances, a controller is required to conduct and document a data protection assessment for each of the controller's processing activities that presents a heightened risk of harm to a consumer.

Those activities include: (1) processing personal data for targeted advertising; (2) processing sensitive data; and (3) selling personal data; using the personal data for consumer profiling if the profiling presents reasonably foreseeable risks that may impose substantial injury to consumers, such as unfair or deceptive treatment or financial, physical, or reputational injury.

The assessments are not retroactive and will only apply to processing activities that occur on or after July 1, 2024. While the data protection assessments are confidential and not subject to disclosure, the Oregon Attorney General may request and evaluate such assessments.

Who Has Enforcement Authority? Is There a Private Right of Action?

The Oregon Attorney General has exclusive authority to enforce the OCPA, and there is no private right of action. Specifically, the Oregon Attorney General may bring an action to seek a maximum civil penalty of \$7,500 for each violation. The statute of limitations is five years.

Is There a Right to Cure?

Before bringing an action against the controller, the Oregon Attorney General is required to notify the controller of the violation. However, such notice is required only if the Attorney General determines that the controller can cure the violation. The controller then has 30 days to cure the violation (the "Curing Grace Period").

Which Obligations Take Effect on January 1, 2026?

The OCPA delays the implementation of the opt-out preference signal for the sale of personal data or targeted advertising to January 1, 2026. In addition, the Oregon Attorney General will no longer be required to provide a notice for the Curing Grace Period after January 1, 2026.

For more information, please contact any other member of Frost Brown Todd's [Data Security & Privacy](#) practice group.

**Frost Brown Todd summer associate Wenxi Lu contributed to this article.*

© 2026 FBT Gibbons LLP. May be considered attorney advertising in some jurisdictions.