Oregon Becomes Twelfth State to Enact a Comprehensive Consumer Privacy Law

Oregon Governor Tina Kotek signed into law the Oregon Consumer Privacy Act (OCPA) (Senate Bill 619) on July 18, making Oregon the twelfth state to enact comprehensive data privacy legislation. The OCPA is primarily based on other existing state privacy laws, particularly those in Connecticut and Colorado, but it differs in a few ways. The OCPA lacks several common exemptions found in other state privacy laws and has various unique definitions. These provisions, in addition to the OCPA's applicability threshold and various consumer rights and business obligations, are discussed in further detail below. The OCPA will go into effect on July 1, 2024.

Applicability Threshold

The OCPA applies to any person that conducts business in Oregon and controls or processes the personal data of either: (1) at least 100,000 Oregon residents (other than personal data controlled or processed solely to complete a payment transaction) or (2) at least 25,000 Oregon residents while deriving at least 25% of its revenue from the sale of personal data. This follows the standard threshold common in various other state privacy laws.

Exemptions

The Oregon legislature did not include in the OCPA some of the exemptions found in other state privacy laws. Some exemptions *not* included are:

- No entity-level exemption exists for Gramm-Leach-Bliley Act (GLBA)-regulated financial institutions.
- There is no HIPAA-covered entity exemption (similar to Colorado).
- There is no nonprofit exemption (similar to Colorado) after July 1, 2025. However, there are certain limited nonprofit exemptions for specific types of organizations (those intended to prevent fraudulent acts in connection with insurance and radio and television programming organizations).

There are, however, several entity-level and data-level exemptions in the OCPA, including the below.

- The OCPA does not apply to employment (including employment-related) or business-to-business (B2B) data.
- The OCPA contains a broad exemption for personal health information (PHI), which exemption includes the following:
    - Information processed by HIPAA-covered entities or business associates.
    - Data that is intermingled with and indistinguishable from HIPAA-covered PHI.
    - Various other data uses related to health and medical research.
- The OCPA also does not apply to data collected or processed in accordance with the following laws:
    - Fair Credit Reporting Act
    - GLBA
    - Driver's Privacy Protection Act

    - Family Educational Rights and Privacy Act
- The OCPA does not apply to several entities defined and regulated at the state level under Oregon law, including insurers (and some affiliates) and non-commercial activities of publishers, radios, and television stations.
- The OCPA does not apply to de-identified and publicly available data (per its definition of "personal data").

Definitions

Several definitions in the OCPA are somewhat unusual, including the definition of "personal data." The OCPA defines "personal data" as "data, derived data or any unique identifier that is linked to or is reasonably linkable to a consumer or device that identifies, is linked to or is reasonably linkable to one or more consumers in a household." This is broader than most states' definitions, which are often limited to identifiable individuals and do not include devices or households.

"Biometric data" is defined in the OCPA as "personal data generated by automatic measurements of a consumer's biological characteristics, such as a consumer's fingerprint, voiceprint, retinal pattern, iris pattern, gait or other unique biological characteristics that allow or confirm the unique identification of the consumer." This definition varies from the standard definition in other states (like California, Connecticut, and Colorado) in that it does not require Controllers to *use* biometric data to identify an individual for it to fall within the definition. The definition has a carve-out, however, for photographs, audio or video recordings, data from a photograph or audio or video recording, and facial mapping or facial geometry, unless the data "was generated for the purpose of identifying a specific consumer or was used to identify a particular consumer." The requirement that photographs and audio and video recordings be used for purposes of identifying a particular consumer was included in the definition of biometric data due to the pervasiveness of photos, audio, and video on the internet.

The OCPA's definition of "sensitive data" largely tracks the definitions in other state laws, though it additionally covers "status as transgender or nonbinary" and "status as a victim of a crime." Connecticut's law was amended this year to include the "status as a victim of a crime" in its definition of sensitive data. It is also important to note that Oregon's definition of "sensitive data" does *not* require such data to be generated or used to identify a particular individual, like its definition of "personal data."

Controller Obligations

The OCPA imposes several requirements on persons that determine the purposes and means for processing personal data (Controllers) that meet its applicability threshold, including the provision of specific consumer rights, privacy notices, and data protection assessments.

- **Consumer Rights:** Oregon residents will receive many of the same consumer rights provided in other previously enacted state laws, with a few notable exceptions. First, Oregon will require Controllers to recognize universal opt-out mechanisms (UOOMs) by January 1, 2026. Additionally, Oregon does not exclude pseudonymous data from certain rights like other states. Even if businesses can prove that the information necessary to identify the consumer is kept separately and subject to effective technical and organizational controls that prevent the Controller from accessing that information, an Oregon resident's rights still allow a consumer to request deletion of *all* their data, including this pseudonymous data. Lastly, and perhaps most significantly, the OCPA allows Oregon residents to obtain, at the Controller's option, a list of specific third parties that have received their personal data or any

personal data from the Controller. No other previously enacted comprehensive state data privacy law requires Controllers to identify specific third parties (only categories of third parties). (Note that California's Shine the Light law requires the identification of specific third parties with which data is shared for direct marketing purposes. CA Civil Code § 1798.83).

- **Privacy Notices:** The OCPA's privacy notice requirement is more detailed than those found in other states' privacy laws but largely tracks those requirements with one main exception. The OCPA requires the privacy notice to identify the Controller, any business name under which the Controller is registered with the Secretary of State, and any assumed business name that the Controller uses within the state.
- **Data Protection Assessments:** The data protection assessment requirements in the OCPA are less stringent than those found in some other states' laws (like Colorado, for example), except its data retention requirement. Colorado only requires Controllers to maintain data protection assessments for three years, while the OCPA requires at least five years of retention.
- **Processing of Sensitive Personal Information:** Controllers must obtain consent from consumers prior to processing sensitive personal information. If the Controller knows that the consumer is a child (an individual under the age of 13), they must process sensitive data in accordance with the Children's Online Privacy Protection Act of 1998 (COPPA).
- **Sale of Personal Data and Targeted Advertising:** Beginning July 1, 2026, Controllers must honor consumer requests to opt out of the sale of personal data or targeted advertising using Global Privacy Control (GPC) signals, which must be honored within 15 days of the request. GPC signals are used in a web browser to convey a request to opt out of certain processing automatically. If the Controller has actual knowledge that a consumer is between 13 and 15 years of age, it may not process the consumer's personal data for targeted advertising, profiling, or the sale of personal data without the consumer's prior consent.

Rulemaking and Enforcement

The Oregon Attorney General's Office will enforce the OCPA. The OCPA does not contain a private right of action, though it did when it was first introduced, and it does not authorize rulemaking. Lastly, it contains a 30-day right to cure, which sunsets on January 1, 2026. Remedies include an injunction and a fine of up to $7,500 per violation.

Important Dates

- **July 1, 2024**: The OCPA goes into effect.
- **July 1, 2025**: The OCPA applies to nonprofits.
- **January 1, 2026**: The right to cure sunsets and UOOM recognition deadline.
- **July 1, 2026**: Consumers can opt out of the sale of personal data or targeted advertising using GPC signals.

Our team will continue to monitor the OCPA. If you have any questions about the OCPA or other state privacy laws and how they could affect your business, please contact the authors.