
Oregon Set to Become the 11th State with a Comprehensive Privacy Law

JUNE 26, 2023

As of June 25, 2023, the Oregon House and Senate have signed [Senate Bill 619](#) (the “Act”), which previously passed in the House 54-0. The Act now moves to the Oregon Governor’s desk for signature (and is set to become law as long as it is not vetoed). Assuming it makes it through the process, the Act will take effect July 1, 2024.

2023 has been a watershed year for privacy legislation. With this law, Oregon is set to become the sixth state this year to pass “comprehensive” privacy legislation (joining [Iowa](#), [Indiana](#), [Montana](#), [Tennessee](#), and [Texas](#)). This list does not include the privacy laws that have passed in 2023 in [Florida](#), [Washington](#), [Nevada](#), and [Connecticut](#), all of which are narrower in scope but still add to the patchwork of privacy rules that companies must account for as part of their compliance programs.

Though the Oregon law includes many of the same provisions as the laws in effect in other states, it does not offer the same broad exemptions as many of the other comprehensive privacy laws. For example, unlike other comprehensive privacy laws passed this year, the Oregon law does not provide entity level exemptions for covered entities and business associates regulated under the Health Insurance Portability and Accountability Act (HIPAA). Further, like the Colorado Privacy Act, the Oregon law does not provide a broad exemption to non-profits. Instead, it provides a limited one-year exemption for non-profits which expires on July 1, 2025, and only provides a permanent exemption to specified non-profits.

In this post, we highlight key takeaways from the Act and summarize its major provisions. We are happy to answer any questions you have about the Act and its implications for your company’s privacy compliance program. For additional updates, such as this, subscribe to the [WilmerHale Privacy and Cybersecurity Law Blog](#).

KEY TAKEAWAYS

- **Sensitive Data Defined Broadly.** The Act defines sensitive data broadly and includes information 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,

as well as specified precise location data, children's data, and biometric data. This definition is mostly similar to what has been passed in other states but is also slightly broader (e.g., none of the other states specifically include transgender or non-binary status).

- **Data-Level Exemptions.** The Act does not provide broad exemption to nonprofits, instead opting to provide specified exemptions such as for those nonprofits established for the purpose of making insurance determinations. Further, the Act does not provide entity-level exemptions for covered entities or business associates regulated under HIPAA or financial institutions covered under the Gramm-Leach-Bliley Act ("GLBA"). Instead, the Act only creates information-level exemptions for information governed under HIPAA and GLBA (though the Act does exempt financial institutions governed under the Bank Holding Company Act).
- **Obligations Regarding Opt-Out Signals.** The Act requires controllers that sell personal data or use personal data for targeted advertising purposes to respond to universal opt-out signals, similar to what is required under the California, Colorado, Connecticut, and Montana laws.
- **Heightened Protections for Children's Data.** The Act requires prior consent for the processing of children's data (an individual under the age of 13) for the purposes of targeted advertising or profiling in furtherance of decisions that produce legal or similarly significant effects.

SUMMARY OF MAJOR PROVISIONS

- **Applicability Thresholds:** Applies to any person that conducts business in Oregon or provides products or services to Oregon residents, and during a calendar year controls or process: (a) 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 (b) the personal data of 25,000 or more consumers while deriving 25% or more of its annual gross revenue from selling personal data.
- **Broad Exemptions:** Exempts various entities, activities, and information types including the following exemptions.
 - **Entities:** public corporations; state government bodies, local government bodies and special government bodies; financial institutions as defined under the Bank Holding Company Act; and insurers which meet specified definitions under Oregon state law including non-profit organizations that are established in connection with insurance activities;
 - **Activities:** any activity governed by Fair Credit Reporting Act; non-commercial activities of a publisher, editor, or reporter or other person who is connected with or employed by a newspaper, magazine, periodical, newsletter, pamphlet, report, or other publication in general circulation; non-commercial activities radio or television station that holds a license issued by the Federal Communications Commission; and a nonprofit organization that provides programming to radio or non-commercial activities of television networks, or an entity that provides an information service, including a press

association or wire service;

- **Information:** health information protected under HIPAA; specified employee-related information; as well as information governed by the GLBA, Driver's Privacy Protection Act Family Educational Rights and Privacy Act, and the Airline Deregulation Act.
- **Consumer Data Rights:** Creates rights for individual consumers, including: the right to confirm whether the controller is processing the consumer's personal information; the right to a list of specific third parties to which the controller has disclosed the consumer's personal data; the right to obtain a portable and readily usable copy of the consumer's personal data; the right to correct inaccuracies in personal data; the right to delete personal data; the right to opt out of the controller's processing for the purposes of the sale of personal data, targeted advertising, or profiling in furtherance of decisions that produce legal or similarly significant effects.
- **Privacy Notices:** Controllers must provide consumers with a privacy notice that describes: the categories of personal data processed (including sensitive data); purposes for said processing; how consumers may exercise their consumer data rights; categories of personal data the controller shares with third parties; all categories of third parties with whom the controller shares personal data; controller's contact information including identity, and email address; any processing of personal data in which the controller engages for the purpose of targeted advertising or for the purpose of profiling; and the method for consumers to submit requests.
- **Privacy by Design:** Incorporates privacy by design principles, such as purpose limitation and reasonable security practices.
- **Sensitive Data:** Prohibits controller from processing consumer's sensitive data without consent. Further, children's data must be processed in accordance with the Children's Online Privacy Protection Act.
- **Opt-Out Signals:** Requires controller to allow for consumer use of opt-out preference signals that indicate consumer's preference to opt-out of the sale of personal data or targeted advertising. Where a conflict arises between opt-out preferences and the consumer's indicated preferences when consent is collected, the controller must either comply with the opt-out request or notify the customer of such conflict and ask for consumer affirmation. (Opt-out provision takes effect on January 1, 2026)
- **Processor Duties:** Imposes a range of requirements on processors, including, among other things, requiring that a contract govern a processor's handling of data processing activities on behalf of the controller.
- **Data Protection Assessments:** Requires controller to conduct data protection assessment for each processing activity that presents a heightened risk of harm to a consumer including processing sensitive data and processing personal data for the purposes of targeted advertising, selling, or profiling where certain foreseeable risks exist.
- **Enforcement:** The Oregon Attorney General ("AG") may bring action to seek civil penalty of up to \$7,500 for each violation or to obtain injunctive or other equitable relief. All funds collected from violations of this Act are to be deposited in the "Department of Justice Protection and Education Revolving Account."

- **Cure Period:** Before bringing action, the AG must provide controller with 30-day cure period.
(This provision will sunset on January 1, 2026.)
- **Effective Date:** Subject to the exceptions outlined above, this Act takes effect on July 1, 2024.

Authors



Kirk J. Nahra

PARTNER

Co-Chair, Artificial
Intelligence Practice

Co-Chair, Cybersecurity
and Privacy Practice

✉ kirk.nahra@wilmerhale.com

☎ +1 202 663 6128



Ali A. Jessani

COUNSEL

✉ ali.jessani@wilmerhale.com

☎ +1 202 663 6105



Genesis Ruano

ASSOCIATE

✉ genesis.ruano@wilmerhale.com

☎ +1 202 663 6154