Published on *The National Law Review* https://natlawreview.com

The Oregon Consumer Data Privacy Act Takes Effect July 1, 2024

Article By:

Gabrielle N. Ganze

With its passage of Oregon Consumer Data Privacy Act ("OCDPA"), Oregon became one of 16 states to pass comprehensive data privacy laws.

Regulated Entities and Data

The OCDPA generally applies to any person who meets two requirements:

1. conducts business in the state, or "provides" products or services to Oregon's residents; *and*
2. within a calendar year, controls or processes personal data of
    - 100,000 or more consumers, *or*
    - 25,000 or more consumers and also derives at least 25 percent of its gross revenue from selling personal data.

"Personal data" regulated by the Act broadly includes any "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."

The OCDPA imposes additional requirements for personal data that is considered *"sensitive data."* Such data includes children's data; genetic or biometric data; precise geolocation data; or data that "reveals a consumer's" national origin, citizen or immigration status, racial or ethnic background, religious beliefs, mental or physical condition/diagnosis, sexual orientation, transgender or non-binary status, or status as a victim of crime. This definition of sensitive data is more expansive that other privacy statutes with its inclusion of categories such as transgender or non-binary status.

The OCDPA also has various exclusions for certain entities and types of data. Some exclusions include data processed solely for the purpose of completing a payment transaction, employment data, and certain data protected by other regulations. Unlike many other privacy laws, non-profit organizations are subject to the OCDPA (effective July 1, 2025).

Biometric Data

Like its definition for sensitive data, OCDPA's definition of *"biometric data"* is expansive. It includes

"personal data generated by automatic measurements of a consumer's biological characteristics, such as the 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 is broad in that it includes biological characteristics that "allow or confirm" a consumer's identity, which likely means it includes the collection of biological characteristics that are capable of identifying a consumer due to the phrase "biological characteristics that *allow*…the unique identification of the consumer." Such a definition expands the type of data and collections regulated under the Act.

The OCDPA also has distinct exclusions. It excludes from the definition of biometric data photographs and audio or video recordings, as well as data from them unless it was (1) generated "for the purpose of identifying a specific consumer" or (2) used "to identify a specific consumer." Additionally, "facial mapping or facial geometry" is also not biometric data unless it was generated or used to identify a consumer. This exclusion is notable because it means mere facial scanning should not qualify as "biometric data" under the OCDPA, unless it is used or generated for the purpose of identifying a consumer.

The exclusions in the OCDPA's biometric data definition demonstrate the importance of understanding the nuances in privacy acts that vary across states that regulate the collection and use of biometric data. For example, Illinois' Biometric Information Privacy Act ("BIPA") has facial geometry in its definition of "biometric data" whereas the OCDPA includes it in a carveout. Some courts have broadly interpreted BIPA to apply to the collection of facial geometry that has the mere capability of identifying a person regardless of the purpose or use for the purported collection. The same information may not qualify as biometrics under the OCDPA.

Requirements, Rights, and Enforcement

Among other requirements, controllers (who determine the purpose and means of processing data) must maintain a privacy notice, implement safeguards for the protection of personal data, and enter into particular contracts with processors handling personal data on the controller's behalf. The privacy notice has a number of disclosures it must include in a reasonably accessible and clear manner. It must inform a consumer of the following:

1. The business name under which the controller is registered with the Secretary of State and any assumed names the controller uses;
2. An actively monitored e-mail address of the controller or online method that the consumer can use to contact the controller;
3. The personal data and sensitive personal data being processed;
4. The purpose for processing the data;
5. The method for a consumer to exercise their rights;
6. Details by which the controller processes data for advertising or profiling purposes and how a consumer can opt out of this processing; and
7. The categories of third parties with whom personal data and sensitive data is shared, including the type of entity the party is and, if possible, how the party will process the data.

Consumers are provided various rights to control their data, including the right to access, correct, and delete their personal data; the right to opt out of the selling or sharing of their data for targeted advertising; and the right to appeal the denial of their request to exercise their rights. For sensitive personal data, a consumer's consent is required prior to processing such data.

The Oregon Attorney General has exclusive authority to enforce the OCDPA and can recover civil penalties up to $7,500 per violation and reasonable attorney's fees. There is no private right of action.

National Law Review, Volume XIV, Number 134