



Privacy & Cybersecurity Update

July 2023

Oregon Legislature Passes Privacy Law

On June 23, the Oregon legislature passed the Oregon Consumer Privacy Act (OCPA). The bill awaits Governor Tina Kotek's signature, and if signed into law, Oregon will join [several other states](#) that have enacted a comprehensive data privacy framework this year. Although most of the provisions within the OCPA will go into effect on July 1, 2024, certain clauses will not take effect until January 1, 2026.

The Oregon state attorney general has the exclusive authority to enforce the law and the power to impose penalties, which could amount to \$7,500 per violation. Accordingly, the OCPA does not create a private right of action.

Scope of Applicability. The OCPA applies to any organization that conducts business in Oregon or that provides products or services to Oregon residents *and* during a calendar year meets at least one of the following criteria:

- Controls or processes the personal data of 100,000 or more consumers (other than personal data used solely for the purpose of completing a payment transaction), or
- Controls or processes the personal data of 25,000 or more consumers while deriving at least 25% of the organization's annual gross revenue from selling personal data.

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." Personal data does not include deidentified data, data that the consumer made publicly available, or data that is lawfully available through federal, state or local government records or through widely distributed media.

The OCPA defines "sensitive data" 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, a child's personal data, genetic and biometric data. Under the OCPA, sensitive data also includes personal data that accurately identifies within a 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 (e.g., a global positioning system that provides latitude and longitude coordinates).

The OCPA includes several exemptions that are standard in data privacy frameworks, including exemptions for data processing activities governed by federal law (e.g., HIPAA, GLBA, FCRA) and data processing conducted in the HR/employee and business-to-business contexts.

Consumer Data Privacy Rights. The OCPA provides that a controller may 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 law. It further provides consumers residing in Oregon with the following data privacy rights:

- The right to obtain from a controller a confirmation as to whether the controller is processing or has processed the consumer's personal data and the categories of personal data the controller is processing or has processed.
- The right to a copy of all the consumer's personal data that the controller has processed or is processing in a portable and, if feasible, a readily usable format that allows the consumer to transmit the personal data to another controller.
- The right to correct inaccuracies in personal data.
- The right to delete personal data about the consumer, including personal data the consumer provided to the controller, personal data the controller obtained from another source and derived data.
- The right to opt out from a controller's processing of personal data of the consumer that the controller processes for the purposes of targeted advertising, sale, or profiling in furtherance of decisions that produce legal effects or effects of similar significance.

Importantly, the OCPA defines a "sale of personal data" as the exchange of personal data for monetary or other valuable consideration by the controller with a third party but does not include the disclosure of personal data to data processors and other common data disclosure practices (e.g., disclosure of personal data to an affiliate, at the request of a consumer, or as part of corporate restructuring). Further, the OCPA provides that a data controller is prohibited from processing personal data for the purposes of targeted advertising or for certain types of profiling or selling the consumer's personal data without the consumer's consent if the controller has actual knowledge that, or willfully disregards whether the consumer is at least 13 years of age and not older than 15 years of age.

Privacy Right Processes and Universal Signals. The OCPA creates a framework for how controllers must intake, authenticate, and respond to consumer privacy requests and mandates that organizations "establish a process" to allow a consumer to "appeal" a controller's refusal to take action on a data rights request within a reasonable period of time after the consumer receives the decision. A data controller must provide information the consumer requests once during any 12-month period without charge and may (with some exceptions) charge a reasonable fee to cover the administrative costs of complying with a second or subsequent request within the 12-month period.

Under the OCPA, a controller that maintains a website must provide a mechanism on the website for consumers to submit data privacy requests. In addition, a data controller must allow a consumer or authorized agent to send a signal to the controller that indicates their preference to opt out of the sale of personal data or targeted advertising by means of a platform, technology or mechanism that, among other areas, does not use a default setting but instead requires the consumer or authorized agent to make an affirmative, voluntary, and unambiguous choice to opt out; is "consumer-friendly" and "easy" to use; is as consistent as possible with similar platforms, technologies or mechanisms required under federal or state laws or regulations; and enables the controller to accurately determine whether the consumer is an Oregon resident.

In addition, controllers must comply with consumer opt-out requests that originate from the consumer's agent, including from technologies (e.g., website link, browser setting, global setting on electronic devices) that indicate the consumer's intent to opt out of processing, provided the controller can, with commercially reasonable effort, verify the identity of the consumer and the authorized agent's authority to act on the consumer's behalf.

With respect to consumer data and privacy rights appeals, the OCPA specifies that the appeal process must be conspicuously available and similar to the process for intaking privacy rights requests. The controller must inform consumers in writing about the actions taken in response to appeals, including reasons for the decisions reached, and how consumers may contact the attorney general to submit a complaint.

Privacy policies and other notices. Controllers are required to provide consumers with a "reasonably accessible, clear and meaningful" privacy notice that describes their data processing activities (e.g., categories of personal data processed, purposes of processing, categories of personal data, including the categories of sensitive data, that the controller shares with third parties). With respect to categories of third parties, OCPA requires controllers to provide sufficient detail that enables the consumer to understand the type of entity each third party is and, to the extent possible, how each third party may process personal data. The notice must also describe how consumers can exercise their data privacy rights (e.g., clear and conspicuous link to a webpage), including how to appeal a controller's decision. A controller that sells personal data or uses it for targeted advertising and profiling purposes has

the additional obligation to provide a clear and conspicuous description of such processing. Controllers are also obligated to specify the method by which a consumer can contact the controller as well as the registered and assumed names of the business.

Processor obligations and contracts. The OCPA places affirmative obligations on processors, such as those related to compliance with a controller's instructions, assistance in responding to consumer rights requests, and the implementation of security controls to safeguard personal data from unauthorized use.

Like many other data protection laws, the OCPA also requires controllers and processors to execute written agreements that contain certain data protection clauses, which must address, among other things, the nature and purpose of data processing, duration of the processing, the type of data subject to processing, rights and obligations of parties, confidentiality, and compliance assessments. The OCPA requires these controller-to-processor contracts to include clauses requiring the processor to delete or return the personal data in its custody at the end of the data processing services unless retention is required by law. In addition, the OCPA mandates written contracts between processors and subcontractors that require the subcontractor to meet the processor's obligations with respect to personal data.

Contractual obligations extend to relationships related to deidentified data. In particular, a controller must execute a contract with recipients of deidentified data that is in the controller's possession. The agreement must provide that a recipient of deidentified data comply with the same obligations as the controller.

Data protection assessments. When engaging in data processing that "presents a heightened risk of harm to a consumer," the OCPA requires a controller to conduct and document a data processing assessment. The OCPA defines this category of processing broadly to address a variety of common business activities, such as targeted advertising, selling of personal data, processing of sensitive data, and certain types of profiling. The assessment must be made available to the Oregon attorney general upon request.

Rewards programs and anti-discrimination. The OCPA permits controllers to offer a different price, rate, level of quality or selection of goods or services to a consumer, including an offer for no fee or charge in connection with a

consumer's voluntary participation in a bona fide loyalty, rewards, premium features, discount or club card program. Like other state data protection laws, a controller may not discriminate against a consumer for exercising a data privacy right (e.g., by denying the consumer a good or service, charging a different price, or providing a different level of quality of a good or service).

Consent. The OCPA limits how a controller can use personal data without a consumer's consent. For example, an organization cannot "process personal data for purposes that are not reasonably necessary for and compatible with the purposes the controller specified in [its privacy notice], unless the controller obtains the consumer's consent." A controller is also prohibited from processing sensitive data without first obtaining appropriate consent and must comply with the Children's Online Privacy Act if the controller intends to process the sensitive data of a known child.

Data security requirements. The OCPA places affirmative data security obligations on controllers to implement administrative, technical, and physical security measures to protect the confidentiality, integrity, and accessibility of "personal data" in the same manner they must protect "personal information" pursuant to the state's [data safeguarding law](#), to the extent appropriate for the volume and nature of the personal data.

FOR MORE INFORMATION

For more information, please contact:

Steven G. Stransky

216.566.5646

202.263.4126

Steve.Stransky@ThompsonHine.com

Certified Information Privacy Professional/Government (CIPP/G)

Certified Information Privacy Professional/United States (CIPP/US)

Thomas F. Zych

216.566.5605

Tom.Zych@ThompsonHine.com

Marla M. Izbicky

312.998.4253

Marla.Izbicky@ThompsonHine.com

Certified Information Privacy Professional/United States (CIPP/US)

Thora Knight

212.908.3971

Thora.Knight@ThompsonHine.com

This advisory bulletin may be reproduced, in whole or in part, with the prior permission of Thompson Hine LLP and acknowledgment of its source and copyright. This publication is intended to inform clients about legal matters of current interest. It is not intended as legal advice. Readers should not act upon the information contained in it without professional counsel.

This document may be considered attorney advertising in some jurisdictions.

© 2023 THOMPSON HINE LLP. ALL RIGHTS RESERVED.