Oregon Consumer Privacy Act (OCPA) Summary

On July 18, 2023, Governor Tina Kotek (D) signed SB 619, the "Oregon Consumer Privacy Act" into law. The Act's provisions take effect on July 1, 2024 for all covered entities except non-profits (July 1, 2025). A non-comprehensive summary of significant elements of the Act follows:

Covered Entities	The **Oregon Consumer Privacy Act (OCPA)** applies to any person that conducts business in Oregon or that produces products or services to Oregon residents and that during a calendar year, controls or processes: (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 a person's annual gross revenue from selling personal data.
Covered Data	***"Personal data"***: data, derived data or any unique identifier that is linked 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 or data that is lawfully available through federal, state or local government records or through widely distributed media, or data lawfully made available to the public by a consumer. ***"Sensitive data"***: personal data that: (a) 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; (b) is a child's personal data; (c) 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 that includes, but is not limited to, a global positioning system that provide latitude or longitude coordinates; or (d) is genetic or biometric data. ***"Biometric data"***: means 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. "Biometric data" does not include (a) a photograph recorded digitally or otherwise, (b) an audio or video recording, (c) data from a photograph or from an audio or video recording, unless the data were generated for the purpose of identifying a specific consumer or were used to identify a particular consumer; or (d) facial mapping or facial geometry, unless the facial mapping or facial geometry was generated for the purpose of identifying a specific consumer or was used to identify a specific consumer.
Key Definitions	***"Consent"***: an affirmative act by means of which a consumer clearly and conspicuously communicates the consumer's freely given, specific, informed and unambiguous assent to another person's act or practice under the following conditions: (a) the user interface by means of which the consumer performs the act does not have any mechanism that has the purpose or substantial effect of obtaining consent by obscuring, subverting or impairing the consumer's autonomy, decision-making or choice; and (b) the consumer's inaction does not constitute consent. The user interface by means of which the consumer performs the act does not have any mechanism that has the purpose or substantial effect of obtaining consent by obscuring, subverting or impairing the consumer's autonomy, decision-making or choice. ***"De-Identified Data"***: data that cannot reasonably be used to infer information about, or otherwise be linked to, an identified or identifiable consumer, or to a device that identifies, is liked to or is reasonably linkable to a consumer or is derived from patient information that was originally created, collected, transmitted or maintained by an entity subject to regulation under the Health Insurance Portability and Accountability Act or the Federal Policy for the Protection of Human Subjects.

	"Targeted Advertising": advertising that is selected for display to a consumer on the basis of personal data obtained from the consumer's activities over time and across one or more unaffiliated websites or online applications and is used to predict the consumer's preferences or interests. "Targeted advertising" does not include: (a) advertisements based on activities within a controller's own websites or online applications; (b) advertisements based on the context of a consumer's current search query, visit to a specific website or use of an online application; (c) advertisements that are directed to a consumer in response to the consumer's request for information or feedback; or (d) processing of personal data solely for the purpose of measuring or reporting an advertisement's frequency, performance or reach. ***"Sale" or Sell"***: the exchange of personal data for monetary or other valuable consideration by the controller with a third party. "Sale" or "sell" does not include: (a) disclosure of personal data to a processor; (b) disclosure of personal data to an affiliate of a controller or to a third party for the purpose of enabling the controller to provide a product or service to a consumer that requested the product or service; (c) disclosure or transfer of personal data from a controller to a third party as part of a proposed or completed merger, acquisition, bankruptcy or other transaction in which the third party assumes control of all or part of the controller's assets, including the personal data; or (d) disclosure of personal data that occurs because a consumer directs a controller to disclose the personal data, intentionally discloses the personal data in the course of directing a controller to interact with a third party; or intentionally discloses the personal data to the public by means of mass media, if the disclosure is not restricted to a specific audience.
Consumer Rights	• **Access:** A consumer may obtain from a controller the 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. At the controller's option, a consumer may also obtain a list of specific third parties, other than natural persons, to which the controller has disclosed the consumer's personal data or any personal data. • **Affirmative Consent:** A controller may not process sensitive data about a consumer without first obtaining the consumer's consent or, if the controller knows the consumer is a child, without processing the sensitive data in accordance with the Children's Online Privacy Protection Act of 1998. A controller may not process a consumer's personal data for the purposes of targeted advertising, of profiling the consumer in furtherance of decisions that produce legal effects or effects of similar significance or of 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. • **Correction:** A consumer may require a controller to correct inaccuracies in personal data about the consumer, taking into account the nature of the personal data and the controller's purpose for processing the personal data. • **Deletion**: A consumer may require a controller to delete personal data about the consumer, including personal data the consumer provided to the control, personal data the controller obtained from another source and derived data. • **Portability:** A consumer may obtain from the controller a copy of all of the consumer's personal data that the controller has processed or is processing. A controller that provides a copy of personal data to a consumer shall provide the personal data in a portable and, to the extent technically feasible, readily usable format that allows the consumer to transmit the personal data to another person without hindrance. • **Opt Out Rights**: A consumer may opt out from a controller's processing of personal data of the consumer that the controller processes for any of the following purposes: (a) targeted advertising; (b) selling personal data; or (c) profiling the consumer in furtherance of decisions that produce legal effects or effects of similar significance.

Business Obligations	• **Responding to Consumer Requests**: A controller shall respond to a request from a consumer without undue delay and not later than 45 days after receiving the request. The controller may extend the period within which the controller responds by an additional 45 days if the extension is reasonably necessary to comply with the consumer's request, taking into consideration the complexity of the request and the number of requests the consumer makes. A controller that intends to extend the period of responding shall notify the consumer within the initial 45-day response period and explain the reason for the extension. A controller shall notify a consumer without undue delay and not later than 45 days after receiving the consumer's request if the controller declines to take action on the request. The controller in the notice shall explain the justification for not taking action and include instructions for appealing the controller's decision. A consumer has the right to a free response once during any 12-month period. A controller may charge a reasonable fee to cover the administrative costs of complying with a second or subsequent request within the 12-month period, unless the purpose of the second or subsequent request is to verify that the controller corrected inaccuracies in, or deleted, the consumer's personal data in compliance with the consumer's request. A controller shall establish a process by means of which a consumer may appeal the controller's refusal to take action on a request. The appeal process must: (a) allow a reasonable period of time after the consumer receives the controller's refusal within which to appeal; (b) be conspicuously available to the consumer; (c) be similar to the manner in which a consumer must submit a request; and (d) require the controller to approve or deny the appeal within 45 days after receiving the appeal and notify the consumer in writing of the consumer's decisions and reasons for the decision. If the controller denies the appeal, the notice must provide or specify information that enables the consumer to contact the Attorney General to submit a complaint. • **Recognizing Opt-Out Signals**: A consumer may designate another person to act on the consumer's behalf as the consumer's authorized agent for the purpose of opting out of a controller's processing of the consumer's personal data. The consumer may designate an authorized agent by means of an internet link, browser setting, browser extension, global device setting or other technology that enables the consumer to opt out of the controller's processing of the consumer's personal data. A controller shall comply with an opt-out request the controller receives from an authorized agent if the controller can verify, with commercially reasonable effort, the identity of the consumer and the authorized agent's authority to act on the consumer's behalf. • **Data Minimization:** A controller may process personal data only 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. • **Avoid Secondary Use:** A controller may not process personal data for purposes that are not reasonably necessary for and compatible with the purposes the controller specified unless the controller obtains the consumer's consent. • **Data Security:** Collection, use and retention of personal data must, where applicable, take into account the nature and purpose of the collection, use or retention. The personal data must be subject to reasonable administrative, technical and physical measures to protect the confidentiality, integrity and security of the personal data and reduce reasonably foreseeable risks of harm to consumers from the collection, use or retention. • **Transparency:** A controller shall provide to consumers a reasonably accessible, clear and meaningful privacy that: (a) lists the categories of personal data, including the categories of sensitive data that the controller process; (b) describes the controller's purposes for processing the personal data; (c) describes how a consumer may exercise the consumer's rights, including how a consumer may appeal a controller's denial of a consumer's request; (d) lists all categories of personal data, including the categories of sensitive data, that the controller shares with third parties; (e) 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 type of entity each third party is and, to the extent possible, how each third party may process personal data; (f) specifies an electronic mail address or other online method by which a consumer can contact the controller that the controller actively

	monirtors; (g) identifies the controller, including any business name under which the controller registered with the Secretary fo State and any assumed business name that the controller uses in this state; (h) provides a clear and conspicuous description of any processing of personal data in which the controller engages for the purpose of targeted advertising or for the purpose of 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 (i) describes the method or methods the controller has established for a consumer to submit a request.
Data Protection Impact Assessments	A controller shall 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, including: (a) processing personal data for the purpose of targeted advertising; (b) processing sensitive data; (c) selling personal data; and (d) using the personal data for purposes of profiling, if the profiling presents a reasonably foreseeable risk of: (i) unfair or deceptive treatment of, or unlawful disparate impact on, consumers; (ii) financial, physical, or reputational injury to consumers; (iii) physical or other types of intrusion upon a consumer's solitude, seclusion or private affairs or concerns, if the intrusion would be offensive to a reasonable person; or (iv) other substantial injury to consumers. A controller shall retain all of its assessment for at least five years. A data protection assessment shall identify and weigh how processing personal data may directly or indirectly benefit the controller, the consumer, other stakeholders, and the public against potential risks to the consumer, taking into account how safeguards the controller employs can mitigate the risks. A controller shall consider how deidentified data might reduce risks, the reasonable expectations of consumers, the context in which the data is processed and the relationship between the controller and the consumers whose personal data the controller will process. The Attorney General may require a controller to provide to the Attorney General any data protection assessments the controller has conducted if the data protection assessment is relevant to an investigation the Attorney General conducts. A data protection assessment is confidential and not subject to disclosure. A data protection assessment that a controller conducts to comply with another applicable law or regulation satisfies the requirements of this section if the data protection assessment is reasonably similar in scope and effect.
Controller / Processor Distinction	• **A processor shall adhere to a controller's instructions and shall assist the controller** in meeting the controller's obligations. In assisting the controller, the processor must: (a) enable the controller to respond to request from consumers by means that take into account how the processor processes personal data and the information available to the processors and that use appropriate technical and organizational measures to the extent reasonably practicable; (b) adopt administrative, technical and physical safeguards that are reasonably designed to protect the security and confidentiality of the personal data the processes processes, taking into account how the processor processes the personal data and the information available to the processor; and (c) provide information reasonably necessary for the controller to conduct and document data protection assessments. • **The processor shall enter into a contract with the controller that governs how the processor processes personal data on the controller's behalf**. The contract must: (a) be valid and binding on both parties; (b) set forth clear instructions for processing data, the nature and purpose of the processing, the type of data that is subject to processing and the duration of the processing; (c) specify the rights and obligations of both parties with respect to the subject matter of the contract; (d) ensure that each person that processes personal data is subject to a duty of confidentiality with respect to the personal data; (e) require the processor to delete the personal data or return the personal data to the controller at the controller's direction or at the end of the provision of services, unless a law requires the processor to retain the personal data; (f) require the processor to make available to the controller, at the controller's request, all information the controller needs to verify

	that the processor has complied with all obligations the processor has; (g) require the processors to enter into a subcontract with a person the processor engages to assist with processing personal data on the controller's behalf and in the subcontract require the subcontractor to meet the processor's obligation under the processor's contract with the controller; and (h) allow the controller, the controller's designee or a qualified and independent person the processor engages, in accordance with an appropriate and accepted control standard, framework or procedure, to assess the processor's policies and technical and organizational measures for complying with the processor's obligations and, at the controller's request, report the results of the assessment to the controller.
Exceptions and Exemptions	• A controller that discloses deidentified data shall exercise reasonable oversight to monitor compliance with any contractual commitments to which the deidentified data is subject and shall take appropriate steps to address any breaches of the contractual commitments. • The OCPA does not prohibit a controller or processor from: (a) complying with laws or regulations; (b) complying with inquiries by government authorities; (c) cooperating with law-enforcement agencies; (d) preparing for and defending legal claims; (e) preventing, detecting, protecting against or respond to, and investigating, reporting or prosecuting persons responsible for, security incidents, identity theft, fraud, harrassment or malicious, deceptive, or illegal activity or preserving the integrity of security of systems; (f) identifying and repairing technical errors in a controller's or processor's information systems that impair existing of intended functionality; (g) providing a product or service specifically requested by a consumer or the parent or guardian of a child (h) negotiating, entering into of performing a contract with a consumer, including fulfilling the terms of a written warranty; (i) protecting any person's health and safety; (j) effectuating a product recall; (k) conducting internal research to develop, improve or repair products, services or technology; (l) performing internal operations that are reasonably aligned with a consumer's expectations, that the consumer may reasonably anticipate based on the consumer's existing relationship with the controller or that are otherwise compatible with processing data for the purpose of providing a product or service the consumer specifically requested or for the purpose of performing a contract to which the consumer is party; or (m) assisting another controller or processor. • Data exempt from the OCPA includes: a public corporation, or a public body, institutions of higher education, protected information under HIPAA, the Health Care Quality Improvement Act of 1986, the Patient Safety and Quality Improvement Act, the Fair Credit Reporting Act, the Driver's Privacy Protection Act of 1994, FERPA, the Farm Credit Act, and COPPA.
Enforcement	• The Attorney General has exclusive authority to enforce the provisions of the OCPA. The OCPA does not create a private right of action. • **Right to Cure**: The Attorney General may bring an action to seek a civil penalty of not more than $7,500 for each violation or to enjoin a violation or obtain other equitable relief. Before bringing an action, the Attorney General shall notify a controller of a violation if the Attorney General determines that the controller can cure the violation. If the controller fails to cure the violation within 30 days after receiving the notice of the violation, the Attorney General may bring the action without further notice.