The following pages set out amendments that were requested from Legislative Counsel on February 15, 2023, along with explanations for the changes.

Note that this will not be the last round of amendments, as we are still discussing numerous requested changes with stakeholders.

We hope this will be helpful, however, to interested parties who want to see the current state of the bill.

Kimberly McCullough, Legislative Director, Oregon Department of Justice

SECTION 1. As used in sections 1 to 10 of this 2023 Act:

(1) "Affiliate" means a person that, directly or indirectly through one or more intermediaries, controls, is controlled by or is under common control with another person such that:

(a) The person owns or has the power to vote more than 50 percent of the outstanding shares of any voting class of the other person's securities;

(b) The person has the power to elect or influence the election of a majority of the directors, members or managers of the other person;

(c) The person has the power to direct the management of another person; or

(d) The person is subject to another person's exercise of the powers described in paragraph (a), (b) or (c) of this subsection.

(2) "Authenticate" means to determine, using ~~a~~ commercially reasonable methods, whether a consumer with the rights described in section 3 of this 2023 Act, or a person acting on behalf of the consumer, is the consumer who has asked, or has the authority ~~asked~~ to exercise any of the consumer's rights.

(3)

(a) "Biometric data" means 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.

Commented [MK1]: Note that we were asked to replace this language with "shares common branding with another person or that" to "maximize interoperability." Only CT has the "common branding" language. We are concerned that such language would be too broad, would capture more than what we consider to be an affiliate, and would create a loophole.

Commented [MK2]: This proposed language is a technical fix. The purpose is to ensure that the individual asking to exercise the rights is who they say they are.

Commented [MK3]: We were asked to limit this to data that is being used to identify a specific consumer. However, information of this type is extremely sensitive and something many consumers wish to keep private, regardless of whether it is used for identification purposes. Further, while this type of data may not be currently used to identify a specific consumer, it could easily be used for that purpose in the future and/or by a third party who obtains it.

To illustrate this point, my DNA data is sensitive because it can reveal all sorts of information about me: my health and genetic predispositions, my family connections, etc. It can also be used to identify me at some point in the future and/or by a third party who obtains this data (including the government, as government is not subject to this bill), even if the current controller is not using it for that purpose.

For these reasons, I should have heightened protections related to the collection, sale, and use of my DNA. These protections should not be triggered only if the current controller of that data is using the information to identify me. It should be enough that the information is linked or linkable to me and that it is highly sensitive.

Similarly, a fingerprint could be used for identity theft by a nefarious person who hacks a data set that contains fingerprint data. Even if the controller wasn't using the fingerprint data for identification purposes, the collection, sale, and use of this data raises serious privacy concerns for consumers that should trigger elevated protections.

Commented [MK4]: We were asked to expand this definition to add the words "physical" and "physiological." However, both of those things are encompassed by the definition of "biological," as the common definition of biology includes the physiology and other qualities of a particular organism. For that reason, we believe the addition is unnecessary.

Commented [MK5]: We were asked to add this additional example of a biological characteristic, because of the ways that a unique gait may be used (particularly as technology in this are is continuing to evolve) to identify a person and to identify other sensitive information about a person.

(b) "Biometric data" does not include:

(A) A photograph recorded digitally or otherwise;

(B) An audio or video recording; ~~or~~

(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 used to identify a specific consumer; or.

(D) Facial mapping or facial geometry, unless generated for the purpose of identifying a specific consumer or used to identify a specific consumer.

(4) "Business associate" has the meaning given that term in 45 C.F.R. 160.103, as in effect on the effective date of this 2023 Act.

(5) "Child" means an individual under the age of 13.

(6) "Consent" means 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.

(7) "Consumer" means a natural person who resides in this state and acts in any capacity other than a commercial or employment context ~~engaging in commercial activity or performing duties as an employer or employee~~.

Commented [MK6]: Because of the pervasiveness of photos, audio and video on the Internet, we are not classifying these things as "sensitive data", except for data from those things that is generated for or used to identify a person. As soon as these things are used to identify someone, they are much more sensitive (e.g., think of the way that facial recognition technology can be used to track people).

Our original draft only excluded data that is generated for identification purposes, but we realized that this won't carry forward to subsequent controllers of data who didn't generate the data themselves but obtained it from another source. If they are using the data for identification purposes, it should also be subject to heightened protections. That is why we have made the addition here.

Commented [MK7]: This was added to address the concern that "photograph" and "video" don't include websites that use real-time facial mapping to apply filters, try on glasses, etc. We are adding this language to exclude those specific uses of technology, as long as the data isn't generated for the purpose of identifying someone or being used to identify a person (for the same reason explained above).

Commented [MK8]: This is being added to align our definition more closely with CT and CO, and to ensure that our definition of consent is strong.

Commented [MK9]: These changes revert to the language that we submitted to LC for this definition, as advocates on both the industry and privacy side of things had concerns with the reworking of this language.

On the privacy side, the concern is that "engaging in commercial activity" could include a consumer purchasing things, when the goal here was to exclude business activity.

On the industry side, the concern is this doesn't capture things like collecting information about job candidates, as that wouldn't fit within the "employee/employer" language, when we agreed as a task force that specific protections related to employment are an issue we are not tackling with this bill.

Further, the "commercial or employment context" language has been used in CO, CT, VA and UT. We are not trying to do anything different here, so we'd like to keep consistent language.

(8) "Controller" means a person that, ~~acts~~ alone or jointly ~~in concert~~ with another person, ~~to~~ determines the purposes and means for processing personal data.

(9) "Covered entity" has the meaning given that term in 45 C.F.R. 160.103, as in effect on the effective date of this 2023 Act.

(10) "Decisions that produce legal effects or effects of similar significance" means a decision that results in the provision or denial of financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunities, health-care services, or access to essential goods or services.

(10) "Deidentified data" means data that:

(a) 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 linked to or is reasonably linkable to a consumer; or

(b) Is:

(A) 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 of 1996, P.L. 104-191, as in effect on the effective date of this 2023 Act, or the Federal Policy for the Protection of Human Subjects, codified as 45 C.F.R. part 46 and in various other deferral regulations, as codified in various sections of the Code of Federal Regulations and as in effect on the effective date of this 2023 Act; and

(B) Deidentified as provided in 45 C.F.R. 164.514, as in effect on the effective date of this 2023 Act.

(11) "Device" means electronic equipment designed for a consumer's use that can transmit or receive personal data.

(12)

(a) "Personal data" means 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.

(b) "Personal data" does not include deidentified data or data that:

(A) Is lawfully available through federal, state or local government records or through widely distributed media; or

(B) A controller reasonably has understood to have been lawfully made available to the public by a consumer.

(13) "Process" or "processing" means an action, operation or set of actions or operations that is performed, automatically or otherwise, on personal data or on sets of personal data, such as collecting, using, storing, disclosing, analyzing, deleting or modifying the personal data.

Commented [MK10]: These changes revert to the language we originally proposed, which is the same as CO, CT, and VA, and mirrors how this language is adopted in California's definition of businesses. This edit is to clarify that the standard for a "controller" in Oregon is the same as those other states' laws and not a different standard. This is operationally important.

Commented [MK11]: Advocates from all corners of our task force asked for a definition of this term to be added. We pulled this one from the CO law. Note that the term has slightly different phrasing, based on LC's edits.

Commented [MK12]: Note that we have received requests to broaden and narrow this definition.

On the privacy side, it has been suggested that we add the words "identified or identifiable" before the word consumer (in both places it appears). We believe that the words "reasonably linkable" are equivalent to "identifiable" in this context and are therefore unnecessary.

On the industry side, it has been suggested that we should remove devices. Not covering data that is linked/linkable to a device that is itself linked/linkable to a consumer could create a significant loophole, considering how much data our personal devices are collecting these days (and this will only increase as technology advances).

On the industry side, we also received requests to remove derived data and unique identifiers. Derived data can reveal many things about a consumer that they may wish to keep private. If we exclude data, when a consumer exercises their deletion rights, a controller could still retain significant amounts of derived data they hold about that consumer based on inferences they made from the consumer's data. This would frustrate the ability of consumers to truly exercise their rights under the bill.

Commented [MK13]: We propose limiting this to households to avoid unintended consequences relating to the exercise of consumer rights. But we also are mindful of the fact that devices may be shared in a home - such as smart TV or VR headset - that may be linkable to more than one person, and which collect significant amounts of information about a household's members. It is important that consumers have rights with respect to data collected about us in this way.

(14) "Processor" means a person that processes personal data on behalf of a controller.

(15) "Profiling" means an automated processing of personal data for the purpose of evaluating, analyzing or predicting an identified or identifiable consumer's economic circumstances, health, personal preferences, interests, reliability, behavior, location or movements.

(16)

(a) "Sale" or "sell" means the exchange of personal data for monetary or other valuable consideration by the controller to a third party. ~~a controller's act of exchanging personal data with a third party for money or other valuable consideration or, as appropriate, the completion of such an exchange~~.

(b) "Sale" or "sell" does not include:

(A) A disclosure of personal data to a processor;

(B) A 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) A 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) A disclosure of personal data that occurs because a consumer:

(i) Directs a controller to disclose the personal data;

(ii) Intentionally discloses the personal data in the course of directing a controller to interact with a third party; or

(iii) Intentionally discloses the personal data to the public by means of mass media, when such disclosure is not restricted to a specific audience.

(17) "Sensitive data" means 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 nonbinary ~~gender identity~~, 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 provides latitude and longitude coordinates; or

Commented [MK14]: We received a suggestion to delete the words "identified or identifiable" from this definition. We are concerned that taking these words out would allow a controller to avoid a consumer's exercise of their opt-out rights by setting up automated processes that profiles a consumer but does not identify the consumer at the time profiling is happening. Consumers will be equally impacted by profiling, regardless of whether the consumer is identified by the controller at the time the profiling is happening.

Commented [MK15]: This was the language that we originally proposed to LC and is the definition in CO and CT. Advocates who supported those bills, believe that the language in SB 619 narrows the scope of what is a sale, but our intent was for this to be co-extensive with CO and CT. We have also heard from industry that a consistent definition will be easier to implement.

Commented [MK16]: We received a request to break this up so that disclosures to affiliates are exempted from sales, even when they are not used for the purpose of enabling the provision of a product or service requested by the consumer. This would essentially allow "laundering" of data to occur. When we are dealing with companies that have extremely large numbers of affiliates, and conglomerates continue to grow, this would create a significant loophole that would frustrate consumers' rights.

Commented [MK17]: This language was requested to ensure that, e.g., social media posts only to friends, or otherwise restricted audiences, do not count as publicly available data. This qualifier is in CT and VA and in the proposed regulations in CO.

Commented [MK18]: Oregon's definition of "gender identity" is broad enough to include sex and gender, even though the goal here is to protect data that identifies a person as transgender and nonbinary. That is why we are tightening up this language.

Commented [MK19]: We received a request to change this to "known child's personal data." However, if you look at the way this term is used (go to the operative provisions), whether the child is known to be a child is addressed there, so there is no need to amend this language here.

Commented [MK20]: We have been asked to replace this with the phrase "precise geolocation information" and then define that term. Doing so would go against Oregon drafting conventions, so LC would prefer that we just spell out what this is here.

(d) Is genetic or biometric data.

(18)

(a) "Targeted advertising" means 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.

(b) "Targeted advertising" does not include:

(A) Advertisements that are 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) A processing of personal data solely for the purpose of measuring or reporting an advertisement's frequency, performance or reach.

(19) "Third party" means a person or a public body, as defined in ORS 174.109, other than a consumer, a controller, a processor or an affiliate of a controller or processor.

SECTION 2.

(1) Sections 1 to 10 of this 2023 Act apply to any person that conducts business in this state, or that provides products or services to residents of this state, and that during a calendar year, controls or processes:

(a) The personal data of 100,000 or more consumers, personal data from 100,000 or more devices that identify or that link to or are reasonably linkable to one or more consumers, or personal data from a combination of 100,000 or more consumers and devices that identify or that link to or are reasonably linkable to one or more consumers; or

(b) The personal data of 25,000 or more consumers, while deriving 25 percent or more of the person's annual gross revenue from selling personal data.

(2) Sections 1 to 10 of this 2023 Act do not apply to:

(a) A public body, as defined in ORS 174.109;

Commented [MK21]: Similar to above, industry has requested that this be limited to data that is used to identify a consumer. But DNA, iris scans, fingerprints, etc. are sensitive whether or not they are being used to identify a consumer or have been collected for that purpose. The point is that this information is unique to a person and could be used for purposes like identity theft, it could later on be used to identify someone (by a third party, for example), and it can also reveal other information about a person that they do not wish to share.

Commented [MK22]: We received a request from a privacy advocate to apply the opt-out right to this data." However, the opt-out right already applies, as "targeted advertising" as one of the things consumers can opt out of. *See* Section 3 (1)(d)(A). For this reason, no change is necessary.

We also received a request to expand "targeted advertising" to include 1st party targeted advertising (tracking and profiling consumers on a "first party" basis, rather than tracking them across third-party or unaffiliated websites). Note that proposed legislation in NY would address this, but that legislation has not yet passed. This is an area worthy of future discussion, but because we have not had time to do a deep dive with the task force in this area, we do not wish to include this in this current bill.

Commented [MK23]: We received a request to remove public bodies from the definition of "third party." The term "third party" is used in the definition of sale. Because consumers have a right to opt out of sales of data, if we excluded public bodies from the definition of "third party", a consumer would not have a right to opt out of their data being sold to the government. Because many consumers are indeed concerned about their data being sold to the government, we do not want to make the suggested edit.

Commented [MK24]: We have receive industry requests to remove personal data from devices from the thresholds here. But data collected through our devices is data that consumers wish to protect.

Commented [MK25]: This is a technical fix. We did not intend to include devices that are not linkable to one or more consumers. Doing so would erode the incentive to create devices that aren't linked to consumers.

(b) Protected health information that a covered entity or business associate processes in accordance with the Health Insurance Portability and Accountability Act of 1996, P.L. 104-191, and regulations promulgated under the Act, as in effect on the effective date of this 2023 Act;

(c) Information used only for public health activities and purposes described in 45 C.F.R. 164.512, as in effect on the effective date of this 2023 Act;

(d) Information that identifies a consumer in connection with:

(A) Activities that are subject to the Federal Policy for the Protection of Human Subjects, codified as 45 C.F.R. part 46 and in various other federal regulations, as in effect on the effective date of this 2023 Act;

(B) Research on human subjects undertaken in accordance with good clinical practice guidelines issued by the International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use;

(C) Activities that are subject to the protections provided in 21 C.F.R. parts 50 and 56, as in effect on the effective date of this 2023 Act; or

(D) Research conducted in accordance with the requirements set forth in subparagraphs (A) to (C) of this paragraph or otherwise in accordance with applicable law;

(e) Information ~~collected~~ processed or maintained solely in connection with, and for the purpose of, enabling:

(A) An individual's employment or application for employment;

(B) An individual's ownership of, or function as a director or officer of, a business entity;

(C) An individual's contractual relationship with a business entity;

(D) An individual's receipt of benefits from an employer, including benefits for the individual's dependents or beneficiaries; or

(E) Notice of an emergency to persons that an individual specifies;

(f) Any activity that involves collecting, maintaining, disclosing, selling, communicating or using information for the purpose of evaluating a consumer's creditworthiness, credit standing, credit capacity, character, general reputation, personal characteristics or mode of living if done strictly in accordance with the provisions of the Fair Credit Reporting Act, 15 U.S.C. 1681 et seq., as in effect on the effective date of this 2023 Act, by:

(A) A consumer reporting agency, as defined in 15 U.S.C. 1681a(f), as in effect on the effective date of this 2023 Act;

(B) A person who furnishes information to a consumer reporting agency under 15 U.S.C. 1681s-2, as in effect on the effective date of this 2023 Act; or

Commented [MK26]: We have received some requests to make the HIPAA exemption entity-level rather than data level. The problem with this is that there are many HIPAA-covered entities that are covered only for a small portion of the data they process. Including an entity-level exemption would create a huge loophole for any entity that engages in any amount of HIPAA covered activities, no matter how much data they process that is not covered by HIPAA.

Along those lines, we have heard that Connecticut's law is not having the impact that was expected because of the fact that it includes an entity-level exemption here.

Commented [MK27]: We received feedback that this section needs edits, but we did not receive any specific feedback to help us craft amendments. We are therefore leaving this as-is for now, unless we receive further input that allows us to craft amendments.

Commented [MK28]: This is a technical edit. We intended to use CT's language which reads "processed or maintained" and erroneously wrote "collected" in the draft we submitted to LC.

(C) A person who uses a consumer report as provided in 15 U.S.C. 5 1681b(a)(3);

(g) Information collected, processed, sold or disclosed under and in accordance with the following federal laws, all as in effect on the effective date of this 2023 Act:

(A) The Gramm-Leach-Bliley Act, P.L. 106-102, and regulations adopted to implement that Act;

(B) The Driver's Privacy Protection Act of 1994, 18 U.S.C. 2721 et seq.;

(C) The Family Educational Rights and Privacy Act, 20 U.S.C. 1232g and regulations adopted to implement that Act; and

(D) The Airline Deregulation Act, P.L. 95-504, only to the extent that an air carrier collects information related to prices, routes or services and only to the extent that the provisions of the Airline Deregulation Act preempt sections 1 to 10 of this 2023 Act; or

Commented [MK29]: We received a request to add language here stating that these exemptions only apply to the extent that the entity processing the data is subject to regulation under the laws listed here.

This addition is unnecessary as the language already requires that the data be processed under and in accordance with these federal laws. The word "under" means that the federal law applies to the data and therefore the entity holding that data that is subject to the regulation.

We also received requests not to limit these exemptions to the current form of these federal laws. Unfortunately we cannot change this, as it would create an impermissible delegation issue (where the feds could essentially change state law by changing federal law, with no action by state government). This means we will need to come back and update these if there are substantive changes at the federal level.

Commented [MK30]: We received several requests to remove this exemption, although it is in the CA, CO, CT, and VA laws. Note that this federal law regulates the processing of data from DMV's, and data obtained from the DMV already exempted as it is "lawfully available through federal, state or local government records."

Commented [MK31]: We have received several requests to remove the FERPA exemption. It has been suggested that one way to mitigate this would be to limit the exemption to covered organizations with first-party relationships with the students, but we haven't received specific language for how to accomplish this. It has also been noted that FERPA may have preemptive effect here, though we have not done a deep-dive on that analysis.

(h) A financial institution as defined in ORS 706.008(9). ~~or an affiliate of a financial institution, as defined in the Gramm-Leach-Bliley Act, P.L. 106-102, and in regulations adopted to implement that Act, as in effect on the effective date of this 2023 Act~~.

(i) An insurance producer as defined in ORS 731.104.

Commented [MK32]: This language is DOJ's proposed compromise to address concerns raised at the last task force meeting about the breadth of an entity-level GLBA exemption. For example, exempting "financial institutions" and their affiliates as defined in the GLBA would lead to the exemption of businesses like payday lenders and car dealerships.

Note that there is already a data-level exemption above, so this would supplement that exemption by fully exempting (a) banks, credit unions and other entities defined as a financial institution under state law, and (b) insurance producers as defined under state law.

Under ORS 706.008(9), "Financial institution" "means an insured institution, an extranational institution, a credit union as defined in ORS 723.006, an out-of-state credit union under ORS 723.042 or a federal credit union."

Under ORS 706.008(11), "Insured institution" means a company, the deposits of which are insured under the provisions of the Federal Deposit Insurance Act, as amended, 12 U.S.C. 1811, et seq. (i.e., any institution that is FDIC insured)

Under ORS 706.008(6), "Extranational institution" means a corporation, unincorporated company, partnership or association of two or more persons organized under the laws of a nation other than the United States, or other than a territory of the United States, Puerto Rico, Guam, American Samoa or the Virgin Islands, that engages directly in banking business.

Under ORS 723.006, "A credit union is a cooperative, nonprofit association, incorporated under the laws of this state, for the purposes of encouraging thrift among its members, creating a source of credit at a fair and reasonable rate of interest and providing an opportunity for its members to use and control their own money in order to improve their economic and social condition."

Under ORS 731.104, "Insurance producer" means a person required to be licensed under the laws of this state to sell, solicit or negotiate insurance.

(3) Sections 1 to 10 of this 2023 Act do not prohibit a controller or processor from:

(a) Complying with federal, state or local statutes, ordinances, rules or regulations;

(b) Complying with a federal, state or local governmental inquiry, investigation, subpoena or summons related to a civil, criminal or administrative proceeding;

(c) Cooperating with a law enforcement agency concerning conduct or activity that the controller or processor reasonably and in good faith believes may violate federal, state or local statutes, ordinances, rules or regulations;

(d) Investigating, establishing, initiating or defending legal claims;

(e) Preventing, detecting, protecting against or responding to, and investigating, reporting or prosecuting persons responsible for, security incidents, identity theft, fraud, harassment or malicious, deceptive or illegal activity or preserving the integrity or security of systems;

(f) Identifying and repairing technical errors in a controller's or processor's information systems that impair existing or intended functionality;

(g) Providing a product or service that a consumer specifically requests from the controller or processor or requests as the parent or guardian of a child on the child's behalf or as the guardian or conservator of a person subject to a guardianship, conservatorship or other protective arrangement on the person's behalf;

(h) Negotiating, entering into or performing a contract with a consumer, including fulfilling the terms of a written warranty; ~~or~~

(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 the expectations of the consumer or reasonably anticipated based on the consumer's existing relationship with the controller or are otherwise compatible with processing data in furtherance of the provision of a product or service specifically requested by a consumer or the performance of a contract to which the consumer is a party; or

(m) Assisting another controller or processor with any of the activities set forth in this subsection.~~.~~

(4) Sections 1 to 10 of this 2023 Act do not apply to the extent that a controller's or processor's compliance with sections 1 to 10 of this 2023 Act would violate an evidentiary privilege under the laws of this state. Notwithstanding the provisions of sections 1 to 10 of this 2023 Act, a controller or processor may provide personal data about a consumer in a

Commented [MK33]: In addition to the language in redline below, one task force member asked us to add the following paragraphs to this subsection, but we believe that a consumer should have the right to opt out of these uses of personal data, and so we are not including them here.

Process personal data for reasons of public interest in the area of public health, community health or population health, but solely to the extent that such processing is (A) subject to suitable and specific measures to safeguard the rights of the consumer whose personal data is being processed, and (B) under the responsibility of a professional subject to confidentiality obligations under federal, state or local law.

Engaging in public or peer-reviewed scientific or statistical research in the public interest that adheres to all other applicable ethics and privacy laws and is approved, monitored and governed by an institutional review board that determines, or similar independent oversight entities that determine, (A) whether the deletion of the information is likely to provide substantial benefits that do not exclusively accrue to the controller, (B) the expected benefits of the research outweigh the privacy risks, and (C) whether the controller has implemented reasonable safeguards to mitigate privacy risks associated with research, including any risks associated with re-identification

Commented [MK34]: We received a request to add the words "responding to" here, but we believe that language would be duplicative and is unnecessary.

Commented [MK35]: We received a request to edit this to read "investigation or proceeding." However, the word "proceeding" is used throughout Oregon law to include both filed actions and investigations, so we do not believe that change is needed here.

Commented [MK36]: This is a technical edit. We intended this to match the language in CT's statute and erroneously omitted "establish"

Commented [MK37]: This is a technical edit that aligns our bill with language in Colorado.

Commented [MK38]: This language is being added as clarification. A warranty is a type of contract, so it is already included here, but adding this language will provide an illustration that could be useful for entities complying with the law.

Commented [MK39]: These additions are also in CO, CT, and VA and are being added to address implementation concerns by industry. Note that the additions of (5)-(7) below act as a counterweight to these changes.

privileged communication to a person that is covered by an evidentiary privilege under the laws of this state.

(5) Personal data processed by a controller pursuant to this section may be processed to the extent that such processing is: (a) Reasonably necessary and proportionate to the purposes listed in this section; and (b) adequate, relevant and limited to what is necessary in relation to the specific purposes listed in this section.

(6) Personal data collected, used or retained pursuant to subsection (3)(e) and (3)(f) of this section shall, where applicable, take into account the nature and purpose or purposes of such collection, use or retention. Such data shall be subject to reasonable administrative, technical and physical measures to protect the confidentiality, integrity and accessibility of the personal data and to reduce reasonably foreseeable risks of harm to consumers relating to such collection, use or retention of personal data.

(7) If a controller processes personal data pursuant to an exemption in this section, the controller bears the burden of demonstrating that such processing qualifies for the exemption and complies with the requirements in subsections (5) and (6) of this section.

SECTION 3. (1) Subject to section 4 of this 2023 Act, a consumer ~~or an authorized agent of the consumer~~ may:

(a) 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;

(B) A list of specific third parties, other than natural persons, to which the controller has disclosed the consumer's personal data; and

(C) A copy of all of the consumer's personal data that the controller has processed or is processing;

Commented [MK40]: We were asked to add a clarification here that this bill does not infringe on First Amendment rights or apply to processing of data by an individual in the course of a purely personal or household activity. Neither of these additions are necessary.

First, we do not need to state that the First Amendment is supreme to any state law that infringes on free speech. That is the case regardless of whether it is stated in our bill. Same goes for all other constitutional rights.

Second, our bill applies to persons "that conducts business" in Oregon, not to individuals acting in a household/personal context.

Commented [MK41]: These data minimization and purpose limitations were inadvertently omitted from our prior draft. This language is adapted from Connecticut's privacy law but the same concept is in the California, Colorado, and Virginia privacy laws.

Commented [MK42]: This is a technical edit. We did not intend all rights to be exercised by an authorized agent. The draft submitted to LC only gave an authorized agent the right to opt-out.

Commented [MK43]: Industry has requested that we limit this right to the categories of third parties data has been shared with, while privacy advocates have requested that we allow consumers to obtain a list of specific third parties data has been disclosed to.

We think it is very important for consumers have the right to know specific third parties so that they can track their data downstream and effectively exercise their rights under the bill.

However, we do want to protect vulnerable individuals from having their acquisition of data disclosed, such as victims of domestic violence who may have requested information about an abuser from entities such as PeopleSearch.

Therefore, we are proposing a compromise position that this only apply to third parties that are not natural persons.

(b) 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;

(c) Require a controller to delete personal data about the consumer including~~whether data~~ the consumer provided ~~the personal data or~~to the controller, data obtained from another source ~~the personal data from another source~~and derived data; or

(d) 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 the personal data; or

(C) Profiling the consumer ~~to support~~in furtherance of decisions that produce legal effects or effects of similar significance.

(2) A controller that provides a copy of personal data to a consumer under subsection (1)(a)(C) of this section 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.

(3) This section does not require a controller to provide personal data to a consumer in a manner that would disclose the controller's trade secrets, as defined in ORS 646.461.

SECTION 4.

(1) A consumer may exercise the rights described in section 3 of this 2023 Act by submitting a request to a controller using the method that the controller specifies in the privacy notice described in section 5 of this 2023 Act.

(2) A controller may not require a consumer to create an account for the purpose described in subsection (1) of this section, but the controller may require the consumer to use an account the consumer created previously.

Commented [MK44]: For this right, we want the deletion right to apply not just to info that a controller "collects" from a consumer, but also to personal data it obtains from third-party sources (e.g., data it buys from a data broker), and to data that it derives or infers about a consumer (because, for instance, targeted advertising profiles contain inferences about a consumer's preferences which are derived from the consumer's web browsing activities). We are concerned that the way the bill is drafted, it might exclude derived data, so we have re-worked this language.

Commented [MK45]: We received a request to add processors to this right, as someone was reading this language to not require a processor to comply with an opt-out when the opt-out was directed at the controller. However, the operative provisions below that explain a processor's obligations make it clear that processors must assist controllers in meeting their obligations under the bill. Therefore, a processor must also comply with these opt-out requests to the degree the processor is processing data on behalf of a controller.

Commented [MK46]: This is a technical fix requested by several task force members. The language we proposed, and which is in CO and CT is *in furtherance of* rather than *to support*. We don't read this as functionally different, but we understand how it could cause an operational headache for companies that need to evaluate the alternative language here.

This will also align with language used later on in the bill.

Commented [MK47]: We received a request to add the words "solely automated" before the word "decisions." The rationale being that profiling happens in three buckets (solely automated, solely human review, and hybrid automated/human) and that not differentiating would opt consumers out of all three types. Colorado is wrestling with this now, but proposed regulations include guardrails on all three buckets. We would like to keep this as consumers being able to opt out of all three at this point.

(3) A parent or legal guardian may exercise the rights described in section 3 of this 2023 Act on behalf of the parent's child or on behalf of a child for whom the guardian has legal responsibility. ~~A guardian or conservator may exercise the rights described in subsection (1) of~~ this section on behalf of a consumer that is subject to a guardianship, conservatorship or other protective arrangement.

(4) 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, as provided in section 3 (1)(d) of this 2023 Act. 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 a request to opt out that the controller receives from a consumer's authorized agent~~. A controller shall comply with an opt-out request received from an authorized agent if the controller is able to verify, with commercially reasonable effort, the identity of the consumer and the authorized agent's authority to act on such consumer's behalf.

(5) Except as otherwise provided in sections 1 to 10 of this 2023 Act, in responding to a request under subsection (1) of this section, a controller shall:

(a) Respond to a request from a consumer ~~or an authorized agent~~ 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 ~~or authorized agent'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 for responding shall notify the consumer ~~or authorized agent~~ within the initial 45-day response period and explain the reason for the extension.

(b) Notify the consumer ~~or authorized agent~~ without undue delay and not later than 45 days after receiving the consumer's ~~or authorized agent'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.

(c) Provide information the consumer ~~or authorized agent~~ requests once during any 12-month period without charge to the consumer or authorized agent. 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 additional requests is to verify that the controller actually corrected inaccuracies in personal data about the consumer as requested by the consumer or to verify that the controller complies with the consumer's request to delete personal data.

Commented [MK48]: We received a request to specify a mechanism for how a company goes about getting verifiable consent. CT's law includes this provision:

Controllers and processors that comply with the verifiable parental consent requirements of COPPA shall be deemed compliant with any obligation to obtain parental consent pursuant to sections 1 to 11, inclusive, of this act.

However, upon review, COPPA doesn't specify how to obtain consent. The FTC has given some guidance, but that's not the same thing, so we are unsure that we could do this in Oregon law.

See: https://www.ftc.gov/business-guidance/privacy-security/verifiable-parental-consent-childrens-online-privacy-rule

Commented [MK49]: We received a request to remove the global opt-out, but we think this is an important way for consumers to exercise their rights and wish to keep it in the bill.

Commented [MK50]: This language is in both CO and CT. Because we want the technology to be effective across state lines (i.e., we want consumers in Oregon to be able to utilize the global opt-out technology that will be in place in CO and CT) it makes sense to align the requirements for using that technology with the requirements already enacted in those states.

Commented [MK51]: These references to an authorized agent need to be taken out throughout, to conform with our removal of authorized agents from Section 3. The only thing we want an authorized agent to be able to do under this bill the opt-out right under section 3(1)(d), and we do not want authorized agents involved in the exercise of rights (or the provisions of this section related to the exercise of those rights) in any way. These additions of "authorized agent" were not included in our draft request.

Commented [MK52]: We received a request to allow controllers to refuse to respond to requests if they are manifestly unfounded, excessive, repetitive or technically unfeasible. This language is very squishy and we are concerned about how it would apply in practice. We believe the ability to charge a reasonable fee for second requests (with the new exception below for verification of inaccuracy correction requests) should allow controllers to comply without such an exception.

Commented [MK53]: CA law requires consumers to respond to data requests free of charge 2 times per year. CO & CT only permit once in a 12 month period. We are proposing a middle ground that will allow consumers to make a second free requests to verify that inaccuracies in their data have been corrected.

(d) Notify the consumer ~~or authorized agent~~ if the controller cannot, using commercially reasonable methods, authenticate the consumer's ~~or authorized agent's~~ request without additional information from the consumer ~~or authorized agent~~. A controller that sends a notification under this paragraph does not have to comply with the request until the consumer ~~or authorized agent~~ provides the information necessary to authenticate the request.

(e) Comply with a request under section 3 (1)(d) of this 2023 Act to opt out of the controller's processing of the consumer's personal data without requiring authentication, except that:

(A) A controller may ask for additional information necessary to comply with the request, such as information that is necessary to identify the consumer that requested to opt out~~, but shall, if possible, comply with request without asking for additional information~~.

(B) A controller may deny a request to opt out if the controller has a good-faith, reasonable and documented belief that the request is fraudulent. If the controller denies a request under this subparagraph, the controller shall notify the consumer or the authorized agent that the controller believes the request is fraudulent, stating in the notice ~~the reasons for the controller's belief and~~ that the controller will not comply with the request.

(6) A controller shall establish a process by means of which a consumer ~~or an authorized agent~~ may appeal the controller's refusal to take action on a request under subsection (1) of this section. The controller's process must:

(a) Allow a reasonable period of time after the consumer ~~or the authorized agent~~ receives the controller's refusal within which to appeal;

(b) Be conspicuously available to the consumer ~~or the authorized agent~~;

(c) Be similar to the manner in which a consumer ~~or authorized agent~~ must submit a request under subsection (1) of this section; and

(d) Require the controller to approve or deny the appeal within 45 days after the date on which the controller received the appeal and to notify the consumer ~~or authorized agent~~ in writing of the controller's decision and the 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.

(7) A controller that obtains personal data about a consumer from a source other than the consumer complies with the consumer's ~~or an authorized agent's~~ request to delete the personal data if the controller~~:~~

~~(a)~~ Ddeletes the data but retains a record of the deletion request and a minimal amount of data necessary to ensure that the personal data remains deleted and does not use the minimal data for any other purpose~~; or~~

Commented [MK54]: We received a request to revise the legislation to clearly state that estimating residency based on IP address is generally sufficient for determining residency and legitimacy, unless the company has a good faith basis to determine that a particular device is not associated with an Oregon resident or is otherwise illegitimate. We believe this is an area that is appropriate for DOJ guidance once legislation is enacted.

Commented [MK55]: We are taking this language out because it is redundant/surplusage. The language already states that information requested must be "necessary" to comply with the request. Necessary means that can only be requested if the controller can't comply with the request with current information.

Commented [MK56]: Deleted language is not in CO or CT. Industry noted that the deleted language actually represents a potential cybersecurity threat (explaining *why* the controller believes the requestor is an imposter consumer, cybercriminal, etc.). Not that under the revised language, the controller will still have to say they think the request is fraudulent (which would allow the consumer to show they are not), but it would not require the controller to reveal their methods of detecting fraud.

~~(b) Allows the consumer or the authorized agent to opt out of the controller's processing of the consumer's personal data except to the extent that the processing is exempt from regulation under sections 1 to 10 of this 2023 Act.~~

SECTION 5.

(1) A controller shall:

(a) Specify in the privacy notice described in subsection (4) of this section the express purposes for which the controller is collecting and processing personal data;

(b) Limit the controller's collection of personal data to only the personal data that is adequate, relevant and reasonably necessary to serve the purpose or purposes the controller specified in paragraph (a) of this subsection;

(c) Establish, implement and maintain for personal data the same safeguards described in ORS 646A.622 that are required for protecting personal information, as defined in ORS 646A.602, such that the controller's safeguards protect the confidentiality, integrity and accessibility of the personal data to the extent appropriate for the volume and nature of the personal data; and

(d) Provide an effective means by which a consumer ~~or an authorized~~ agent may revoke the consumer's consent to the controller's processing of the consumer's personal data. The means must be at least as easy as the means by which the consumer or authorized agent provided consent. Once the consumer ~~or authorized agent~~ revokes consent, the controller shall cease processing the personal data as soon as is practicable, but not later than 15 days after receiving the revocation.

(2) A controller may not:

(a) Process personal data for purposes that are not reasonably necessary for ~~or~~ and compatible with the purposes the controller specified in subsection (1)(a) of this section, unless the processing is otherwise permitted under sections 1 to 10 of this 2023 Act or unless the controller obtains the consumer's ~~or an authorized agent's~~ consent;

(b) Process sensitive data about a consumer without first obtaining the consumer's~~, or an authorized agent's,~~ consent or, if the sensitive data concerns a consumer that the controller knows or ~~constructively~~ willfully disregards ~~knows~~ knowing is a child, without processing the sensitive data in accordance with the Children's Online Privacy Protection Act of 1998, 15 U.S.C. 6501 et seq. and the regulations, rules and guidance adopted under the Act, all as in effect on the effective date of this 2023 Act;

(c) Process a consumer's personal data for the purposes of targeted a~~A~~dvertising or profiling the consumer in furtherance of decisions that produce legal effects or effects of similar significance or profiling or sell the consumer's personal data without the consumer's consent if the controller ~~has actual or constructive knowledge~~knows or willfully disregards knowing that the consumer is at least 13 years of age and not older than 15 years of age; or

Commented [MK57]: This language is unnecessary and doesn't actually accomplish anything. "Allowing the consumer…to opt out of the controller's processing" is just another way of saying "deletes the data" as processing is broad enough to encompass simply having a consumer's data. Saying this will happen except to the degree exemptions apply adds nothing to the bill, as if the exemptions apply, there is no right to delete.

Commented [MK58]: We received a request to add "where consent is required by this act" to this sentence. We think that is unnecessary, as it only make sense to provide a means to revoke consent if consent has already been given.

Commented [MK59]: A task force member raised a concern that the language here would allow processing data that is not reasonably necessary for the purposes specified in the privacy notice, because it would allow "compatible" uses. That was not our intent. We want to ensure that any purposes are both reasonably necessary and compatible with the purposes specified in the privacy notice.

Commented [MK60]: A few stakeholders commented that this standard conflicts with current COPPA and that instead it should be willful disregard to align with COPPA. We were trying to get to the same standard with constructive knowledge, but will change this here for consistency.

Commented [MK61]: We received a request to not limit this to the current version of this law, but we cannot do that under Oregon drafting conventions, because it causes a delegation problem.

Commented [MK62]: We want youth of this age range to have heightened protections (opt-in consent) for profiling as well.

Commented [MK63]: We received a request to add parental consent here, but the key here is that we want heightened protections for these young people that cannot be overridden by a parent providing consent on their behalf.

(d) Discriminate against a consumer that exercises a right provided to the consumer under sections 1 to 10 of this 2023 Act by means such as denying goods or services, charging different prices or rates for goods or services or providing a different level of quality or selection of goods or services to the consumer.

(3) Subsections (1) and (2) of this section do not:

(a) Require a controller to provide a good or service that requires personal data from a consumer that the controller does not collect or maintain; or

(b) Prohibit a controller from offering 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 ~~return for~~ connection with a consumer's voluntary participation in a bona fide loyalty, rewards, ~~club card or loyalty program or for~~ premium features, ~~or~~ discounts or club card program.

(4) A controller shall provide to consumers a reasonably accessible, clear and meaningful privacy notice that:

(a) Lists the categories of personal data, including the categories of sensitive data, that the controller processes;

(b) Describes the controller's purposes for processing the personal data;

(c) Describes how a consumer may exercise the consumer's rights under sections 1 to 10 of this 2023 Act, including how a consumer may appeal a controller's denial of a consumer's request under section 4 of this 2023 Act;

(d) Lists all categories of personal data, including the categories of sensitive data, that the controller shares with third parties;

(e) List all categories of third parties with which the controller shares personal data described in a level of detail that provides a meaningful understanding of what types of entity the third parties are, and to the extent possible, how the third parties 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 monitors;

(g) Identifies the controller, including any business name under which the controller registered with the Secretary of 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~~decisions with legal effects or with similarly serious effects~~, and a procedure by which the consumer may opt out of this type of processing; and

Commented [MK64]: This language as drafted does not align with our intent. This provision is only supposed to give a carve out for a voluntary participation in these various types of *programs*. Program modifies the entire list. Note that this is the exact language from CT, which we want to align with here.

Commented [MK65]: This language is being added to make the privacy notices more meaningful.

Commented [MK66]: We received a request to delete this requirement, as it is not required under other state laws. However, this is incredibly valuable information to consumers. Consumers who try to exercise their rights under existing Oregon laws often have difficulty identifying who a controller is, making it extremely difficult to actually obtain relief they are authorized.

Commented [MK67]: Advocates from all corners of our task force asked for a definition of this term to be added. See new definition above.

(i) Describes the method or methods the controller has established for a consumer to submit a request under section 4 (1) of this 2023 Act.

(5) The method described in subsection (4)(i) of this section for submitting a consumer's request to a controller must:

(a) Take into account:

(A) ~~the~~ The ways in which consumers normally interact with the controller;

(~~b~~B) ~~Be secure and reliable~~the need for secure and reliable communication relating to the request; and

(~~c~~C) ~~Permit the controller to authenticate the request~~The ability of the controller to authenticate the identity of the consumer making the request;

(~~d~~b) Provide a clear and conspicuous link to a webpage where the consumer or an authorized agent may opt out from a controller's processing of the consumer's personal data as described in section 3 (1)(d) of this 2023 Act or, solely if the ~~consumer~~ controller does not have a capacity needed for linking to a webpage, provide another method the consumer can use to opt out; and

(~~e~~c) Allow a consumer or authorized agent to send a signal to the controller that indicates the consumer's preference to opt out under section 3 (1)(d) of this 2023 Act by means of a platform, technology or mechanism that:

(A) Does not unfairly disadvantage another controller;

(B) 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;

(C) Is consumer friendly and easy for an average consumer to use;

(D) Is as consistent as possible with similar platforms, technologies or mechanisms required under federal or state laws or regulations; and

(E) Enables the controller to accurately determine whether the consumer is a resident of this state and has made a legitimate request under section 4 of this 2023 Act to opt out as described in section 3 (1)(d) of this 2023 Act.

(6) If a consumer or authorized agent uses a method described in subsection (5) of this section to opt out of a controller's processing of the consumer's personal data under section 3 (1)(d) of this 2023 Act and the decision conflicts with a consumer's voluntary participation a bona fide reward, club card or loyalty program or a program that provides premium features or discounts in return for the consumer's consent to the controller's processing of the consumer's personal data, the controller ~~shall~~ may either comply with the request to opt out or notify the consumer of the conflict and ask the consumer to affirm that the consumer intends to withdraw from the bona fide reward, club card or loyalty program or the program

Commented [MK68]: We received a request to add this language, as there may be multiple methods available for a consumer to exercise their rights.

Commented [MK69]: These changes will align our bill with all of the other state laws. The goal here is to require the method to take all of these things into account, not just (a).

Commented [MK70]: We are adding a delayed implementation of the global opt-out until July 1, 2025, to allow time for implementation. Note that Colorado's provisions on the global opt out preference signal take effect on July 1, 2024 and CT's goes into effect six months later (January 1, 2025).

This will allow Oregon to leverage the ongoing work in those states and ongoing efforts by stakeholders to develop compliance mechanisms, which will help to drive the development of mechanisms that consumers and companies may use across state lines.

See provision at the end of the bill making this change.

Commented [MK71]: Some industry stakeholders have asked whether we could include language similar to what is in Colorado's privacy law, which specifies that the AGO will maintain a list of approved opt-out mechanisms. We would prefer not to include this. Note that nothing prevents us from maintaining/sharing a list of mechanisms that we think meet the test without having a statutory requirement that we do so.

Commented [MK72]: We received a request to limit the use of a global opt-out to targeted advertising and sale, but we wish to include the opt-out for profiling as well.

Commented [MK73]: This language is being added to provide businesses with the flexibility to either recognize the opt-out signal or send a notice.

that provides premium features or discounts. If the consumer affirms that the consumer intends to withdraw, the controller shall comply with the request to opt out.

SECTION 6.

(1) A processor shall adhere to a controller's instructions and shall assist the controller in meeting the controller's obligations under sections 1 to 10 of this 2023 Act. In assisting the controller, the processor must:

(a) Enable the controller to respond to requests from consumers under section 4 of this 2023 Act by means that take into account how the processor processes personal data and the information available to the processor 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 ~~Secure of~~ the personal data it 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 ~~needs~~ to conduct and document data protection assessments.

(2) 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 when the contract expires or terminates, 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 under sections 1 to 10 of this 2023 Act;

(g) Require the processor to enter into a subcontract with ~~any~~ 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 obligations under the processor's contract with the controller; and

Commented [MK74]: We received a request to limit this "to the extent reasonably possible." This squishy standard would create opportunities for mischief and would frustrate consumers' ability to exercise their rights.

Commented [MK75]: This is just ensuring that the obligations in Section 5 flow down to the processor with more specificity, rather than having to interpret the word "secure."

Commented [MK76]: This language is more in line with the language we proposed to LC, which was identical to the language in CO and CT, but it maintains LC's preferred structure. For reference our submission to LC read:

providing necessary information to enable the controller to conduct and document data protection assessments

Commented [MK77]: This is a clarifying edit, which conforms with CO language. We want to avoid the implication that a processor would need to provide a controller with notice or an opportunity to object to subcontractors that may not be related to processor's activities on behalf of that controller.

(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 under this 2023 Act ~~the contract~~, and require the processor to cooperate with the assessment and, at the controller's request, report the results of the assessment to the controller.

(3) This section does not relieve a controller or processor from any liability that accrues under sections 1 to 10 of this 2023 Act as a result of the controller's or processor's actions in processing personal data.

(4)

(a) For purposes of determining ~~liabilities~~ obligations under sections 1 to 10 of this 2023 Act, a person is a controller with respect to processing a set of personal data, and therefore subject to an action under section 9 of this 2023 Act to punish a violation of sections 1 to 10 of this 2023 Act, if the person:

(A) Does not need to adhere to another person's instructions to process the personal data;

(B) Does not adhere to another person's instructions with respect to processing the personal data when the person is obligated to do so; or

(C) Begins at any point to determine the purposes and means for processing the personal data, alone or in concert with another person.

(b) A determination under this subsection is a fact-based determination that must take account of the context in which a set of personal data is processed.

(c) A processor that continues to adhere to a controller's instructions with respect to a specific processing of personal data remains a processor.

~~(c) A person who is determined to be a controller is subject to an action under section 9 of this 2023 Act to punish a violation of sections 1 to 10 of this 2023 Act.~~

SECTION 7.

(1)

(a) A controller that possesses deidentified data shall:

(A) Take reasonable measures to ensure that the deidentified data cannot be associated with an individual;

(B) Publicly commit to maintaining and using deidentified data without attempting to reidentify the deidentified data; and

(C) Enter into a contract with a recipient of the deidentified data and provide in the contract that the recipient must comply with the controller's obligations under sections 1 to 10 of this 2023 Act~~;~~. ~~and~~

Commented [MK78]: This is a technical edit. We always intended it to be the requirements of this law, not the contract (which may relate to things other than privacy). Our draft language read: *under sections 1-11, inclusive, of this act*

Commented [MK79]: This is a technical edit to conform with the intent of this provision. We had everything in this subsection 4 in a single paragraph. LC broke it up but changed the meaning and made it confusing. I read the purpose of this section as meaning that during an investigation, for purpose of us determining who is a "controller" and therefore ultimately responsible for complying with this law, these are the things that we look at / consider.

Commented [MK80]: This is a clarifying edit. The language we submitted to LC was taken directly from CT and CO (pasted below). LC broke up the single paragraph into this subsection and, as a result, industry has said the intent of the section is no longer clear. In the absence of reverting to our original language, this addition helps to clarify this.

Here's our original language: *Determining whether a person is acting as a controller or processor with respect to a specific processing of data is a fact-based determination that depends upon the context in which personal data is to be processed. A person who is not limited in such person's processing of personal data pursuant to a controller's instructions, or who fails to adhere to such instructions, is a controller and not a processor with respect to a specific processing of data. A processor that continues to adhere to a controller's instructions with respect to a specific processing of personal data remains a processor. If a processor begins, alone or jointly with others, determining the purposes and means of the processing of personal data, the processor is a controller with respect to such processing and may be subject to an enforcement action under section 9 of this act.*

~~(D) Exercise reasonable oversight to monitor any contractual obligations to which a disclosure of deidentified data is subject and take appropriate steps to enforce breaches of the contractual obligations, if the controller discloses deidentified data.~~

(b) This section does not prohibit a controller from attempting to reidentify deidentified data solely for the purpose of testing the controller's methods for deidentifying data.

(c) 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 those contractual commitments.

(2) Sections 1 to 10 of this 2023 Act do not:

(a) Require a controller or processor to:

(A) Reidentify deidentified data; or

(B) Associate a consumer with personal data in order to authenticate the consumer's request under section 4 of this 2023 Act by:

(i) Maintaining data in identifiable form; or

(ii) Collecting, retaining or accessing any particular data or technology.

(b) Require a controller or processor to comply with a consumer's request under section 4 of this 2023 Act if the controller:

(A) Cannot reasonably associate the request with personal data or if the controller's attempt to associate the request with personal data would be unreasonably burdensome;

(B) Does not use personal data to recognize or respond to the specific consumer who is the subject of the personal data or associate the personal data with any other personal data about the specific consumer; and

(C) Does not sell or otherwise voluntarily disclose personal data to a third party ~~other than a processor~~, except as otherwise provided in this section.

SECTION 8.

(1)

(a) 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.

(b) ~~A processing~~Processing activities~~y~~ that present~~s~~ a heightened risk of harm to a consumer include: ~~if:~~

(A) ~~The controller processes~~Processing personal data for the purpose of targeted advertising;

Commented [MK81]: This is not aligned with our intent here. We are replacing it with language below in (c).

Commented [MK82]: This language is in CT and aligns with our attend, and is here to replace the deleted language above in (1)(a)(D). This is saying that a controller that has deidentified data and then discloses that data to someone else (whether that be a processor or a third party) must exercise reasonable oversight to make sure that anyone they disclosed it to is complying with contractual requirements relating to that deidentified data.

Commented [MK83]: We were asked to exclude pseudonymous data from the scope of this bill with respect to access, deletion, correction, and portability rights. We are deeply concerned that pseudonymous data does not afford consumers adequate protection, as it can be easily made personally identifiable. While this may be a good topic to explore for future legislation, we are not satisfied that a framework for adequately protecting consumers with respect to this data has been proposed.

Commented [MK84]: This is a technical edit. The definition of "third party" already excludes "processor"

Commented [MK85]: Restructuring this section to clarify that the enumerated list is illustrative, but not exclusive, of processing activities that present a heightened risk of harm to consumers.

(B) ~~The controller processes~~Processing sensitive data;

(C) ~~The controller sells the~~ Selling personal data; ~~or~~and

(D) ~~The controller uses the~~Processing personal data for purposes of profiling ~~a consumer~~, 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.

(c) A single data protection assessment may address a comparable set of processing operations that present a similar heightened risk of harm.

(2) 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. In conducting the assessment, the 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.

(3) 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 under section 9 of this 2023 Act. The Attorney General may evaluate a data protection assessment for the controller's compliance with the requirements of section 1 to 10 of this 2023 Act. If a data protection assessment the Attorney General obtains under this subsection includes information that is subject to attorney-client privilege or is work product that is subject to a privilege, the controller's provision of the data protection assessment does not waive the privilege.

(4) 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 to a data protection assessment conducted under this section.

(5) Requirements that apply to a data protection assessment under this section apply only to processing activities that occur on and after July 1, 2024, and are not retroactive.

(6) A controller shall retain for at least five years all data protection assessments the controller conducts under this section.

(7) Data protection assessments shall be confidential and is not subject to public disclosure under ORS 192.311 to 192.478.

Commented [MK86]: Exemption requested by industry because DPAs contain confidential and competitively sensitive information. Similar language is found in Colorado, Connecticut, and Virginia privacy laws.

SECTION 9.

(1)

(a) The Attorney General may serve an investigative demand upon any person that possesses, controls or has custody of any information, document or other material that the Attorney General determines is relevant to an investigation of a violation of sections 1 to 10 of this 2023 Act or that could lead to a discovery of relevant information. An investigative demand may require the person to:

(A) Appear and testify under oath at the time and place specified in the investigative demand;

(B) Answer written interrogatories; or

(C) Produce relevant documents or physical evidence for examination at the time and place specified in the investigative demand.

(b) The Attorney General shall serve an investigative demand under this section in the manner provided in ORS 646.622. The Attorney General may enforce the investigative demand as provided in ORS 646.626.

(2)

(a) An attorney may accompany, represent and advise in confidence a person that appears in response to a demand under subsection (1)(a)(A) of this section. The person may refuse to answer any question on constitutional grounds or on the basis of any other legal right or privilege, including protection against self-incrimination, but must answer any other question that is not subject to the right or privilege. If the person refuses to answer a question on grounds that the answer would be self-incriminating, the Attorney General may compel the person to testify as provided in ORS 136.617.

(b) The Attorney General shall exclude from the place in which the Attorney General conducts an examination under this subsection all persons other than the person the Attorney General is examining, the person's attorney, the officer before which the person gives the testimony and any stenographer recording the testimony.

(3)

(a) The Attorney General shall hold in confidence and not disclose to any person any documents, including data protection assessments, answers to interrogatories and transcripts of oral testimony, except that the Attorney General may disclose the documents to:

(A) The person that provided the documents or the oral testimony;

(B) The attorney or representative of the person that provided the documents or oral testimony;

(C) Employees of the Attorney General; or

(D) An official of the United States or of any state who is authorized to enforce federal or state consumer protection laws if the Attorney General first obtains a written agreement from the official in which the official agrees to abide by the confidentiality requirements of this subsection.

(b)

(A) The Attorney General may use any of the materials described in paragraph (a) of this subsection in any investigation the Attorney General conducts under this section or in any action or proceeding the Attorney General brings or initiates in a court or before an administrative agency in connection with the investigation.

~~**(B) Notwithstanding the prohibition against disclosure in paragraph (a) of this subsection, the Attorney General may disclose a document to a committee of the Legislative Assembly in any manner and for any purpose the Attorney General deems appropriate.**~~

(4)

(a) The Attorney General may bring an action to seek a civil penalty of not more than $7,500 for each violation of sections 1 to 10 of this 2023 Act or to enjoin a violation or obtain other equitable relief. The Attorney General shall bring the action in the circuit court for Multnomah County or the circuit court of a county where any part of the violation occurred.

(b) If a court finds that a director, member, officer, employee or agent of a controller violated sections 1 to 10 of this 2023 Act through an act or omission, the court may find that the controller committed the violation or the court may find that both the controller and the director, member, officer, employee or agent committed the violation and may impose separate civil penalties on each.

(c) A court may award reasonable attorney fees, expert witness fees and costs of investigation to the Attorney General if the Attorney General prevails in an action under this subsection. The court may award reasonable attorney fees to a defendant that prevails in an action under this subsection if the court finds that the Attorney General had no objectively reasonable basis for asserting the claim or for appealing an adverse decision of the trial court.

(d) The Attorney General shall deposit the proceeds of any recovery under this subsection into the Department of Justice Protection and Education Revolving Account, as provided in ORS 180.095.

Commented [MK87]: Industry has requested that we delete this provision in order to ensure that data protection assessments remain confidential. We do not think it is necessary to keep this provision, as our legislative committees generally don't act as investigative bodies. We had pulled this language from the False Claims Act, but it makes more sense in that context because that law is about defrauding the government.

Commented [MK88]: Industry has requested that we remove director, officer, employee and agent liability. There is no similar provision in any of the comprehensive state privacy laws that have gone or will go into effect. However, our state False Claims Act statute includes this language (that is where we pulled this from). This is also an important way to ensure accountability.

(5) Before bringing an action under subsection (4) of this section, the Attorney General shall notify a controller of a violation of sections 1 to 10 of this 2023 Act 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.

(6) The Attorney General shall bring an action under subsection (4) of this section within five years after the date of the last act of a controller that constituted the violation for which the Attorney General seeks relief.

(7) The remedies available to the Attorney General under subsection (4) of this section are in addition to and not in lieu of any other relief available to the Attorney General or another person under other applicable provisions of law. A claim available under another provision of law may be joined to the Attorney General's claim under subsection (4) of this section.

SECTION 10.

(1)

(a) A consumer or a class of consumers that suffers an ~~ascertainable loss of money or property~~injury as a result of a controller's violation of sections 1 to 10 of this 2023 Act may bring an action in a circuit court of this state.

(b) A court may award a prevailing plaintiff in an action under paragraph (a) of this subsection:

(A) Compensatory damages;

(B) Injunctive or declaratory relief; and

(C) Reasonable attorney fees and costs.

(2) A consumer or class of consumers that brings an action under subsection (1) of this section shall mail a copy of the complaint or initial pleading to the Attorney General upon bringing the action and shall mail to the Attorney General a copy of any judgment the consumer or class of consumers obtains. A consumer's failure to mail a copy of the complaint is not a jurisdictional defect, but the court may not enter judgment for the plaintiff until the plaintiff files proof of mailing with the court. An affidavit or return receipt is adequate proof of mailing.

(3) A plaintiff shall commence an action under subsection (1) of this section within two years after the plaintiff discovers or, with an exercise of reasonable care, should have discovered an ~~ascertainable loss of money or property~~injury.

(4) A plaintiff may bring an action under this section only for a controller's violation of section 3, 4 or 5 of this 2023 Act.

SECTION 11. ORS 180.095 is amended to read:

Commented [MK89]: If the legislature were to decide to include a private right of action in this bill, use of the word "injury" is more aligned with the reality of how privacy violations work. Private parties would still have to establish "an injury" under Oregon law but we would be leaving it to courts to decide what that means. Note that "an injury" is the language used in 646.641.

Commented [MK90]: Same comment as above

Commented [MK91]: This is the most contentious provision of the bill. Industry overwhelmingly has asked us to remove the private right of action, while privacy advocates continue to push for its inclusion. More discussion with our bill's chief sponsors is needed here and several other areas where the task force did not reach consensus.

180.095. (1) The Department of Justice Protection and Education Revolving Account is created in the General Fund. All moneys in the account are continuously appropriated to the Department of Justice and may be used to pay for only the following activities:

(a) Restitution and refunds in proceedings described in paragraph (c) of this subsection;

(b) Consumer and business education relating to the laws governing antitrust and unlawful trade practices; and

(c) Personal services, travel, meals, lodging and all other costs and expenses incurred by the department in investigating, preparing, commencing and prosecuting the following actions and suits, and enforcing judgments, settlements, compromises and assurances of voluntary compliance arising out of the following actions and suits:

(A) Actions and suits under the state and federal antitrust laws;

(B) Actions and suits under ORS 336.184 and 646.605 to 646.656;

(C) Actions commenced under ORS 59.331; [*and*]

(D) Actions and suits under ORS 180.750 to 180.785[.]**; and**

(E) Actions commenced under section 9 of this 2023 Act.

(2) Moneys in the Department of Justice Protection and Education Revolving Account are not subject to allotment. Upon request of the Attorney General, the State Treasurer shall create subaccounts within the account for the purposes of managing moneys in the account and allocating those moneys to the activities described in subsection (1) of this section.

(3) Except as otherwise provided by law, all sums of money received by the Department of Justice under a judgment, settlement, compromise or assurance of voluntary compliance, including damages, restitution, refunds, attorney fees, costs, disbursements and other recoveries, but excluding civil penalties under ORS 646.642, in proceedings described in subsection (1)(c) of this section shall, upon receipt, be deposited with the State Treasurer to the credit of the Department of Justice Protection and Education Revolving Account. However, if the action or suit was based on an expenditure or loss from a public body or a dedicated fund, the amount of such expenditure or loss, after deduction of attorney fees and expenses awarded to the department by the court or agreed to by the parties, if any, shall be credited to the public body or dedicated fund and the remainder thereof credited to the Department of Justice Protection and Education Revolving Account.

(4) If the Department of Justice recovers restitution or refunds in a proceeding described in subsection (1)(c) of this section, and the department cannot determine the persons to whom the restitution or refunds should be paid or the amount of the restitution or refund payable to individual claimants is de minimis, the restitution or refunds may not be deposited in the Department of Justice Protection and Education Revolving Account and shall be deposited in the General Fund.

(5) Before April 1 of each odd-numbered year, the Department of Justice shall report to the Joint Committee on Ways and Means:

(a) The department's projection of the balance in the Department of Justice Protection and Education Revolving Account at the end of the biennium in which the report is made and at the end of the following biennium;

(b) The amount of the balance held for restitution and refunds;

(c) An estimate of the department's anticipated costs and expenses under subsection (1)(b) and (c) of this section for the biennium in which the report is made and for the following biennium; and

(d) Any judgment, settlement, compromise or other recovery, the proceeds of which are used for purposes other than:

(A) For deposit into the Department of Justice Protection and Education Revolving Account; or

(B) For payment of legal costs related to the judgment, settlement, compromise or other recovery.

(6) The Joint Committee on Ways and Means, after consideration of recommendations made by the Department of Justice, shall use the information reported under subsection (5) of this section to determine an appropriate balance for the revolving account.

SECTION 12. Section 9 of this 2023 Act is amended to read:

Sec. 9 (1)

(a) The Attorney General may serve an investigative demand upon any person that possesses, controls or has custody of any information, document or other material that the Attorney General determines is relevant to an investigation of a violation of sections 1 to 10 of this 2023 Act or that could lead to a discovery of relevant information. An investigative demand may require the person to:

(A) Appear and testify under oath at the time and place specified in the investigative demand;

(B) Answer written interrogatories; or

(C) Produce relevant documents or physical evidence for examination at the time and place specified in the investigative demand.

(b) The Attorney General shall serve an investigative demand under this section in the manner provided in ORS 646.622. The Attorney General may enforce the investigative demand as provided in ORS 646.626.

(2)

(a) An attorney may accompany, represent and advise in confidence a person that appears in response to a demand under subsection (1)(a)(A) of this section. The person may refuse

Commented [MK92]: Per the operative dates in Section 13, this section would replace section 9 1 year after the bill's operative date. This would sunset the notice and right to cure provision found at 9(5).

Industry has requested that we not sunset the notice and right to cure. We believe this would hinder our ability to enforce the law and would create unnecessary bureaucracy.

Note that nothing in this law would prohibit the AG from providing notice and right to cure if the AG believed that was the appropriate thing to do under a particular set of circumstances. Further, we do provide notices and opportunities to cure under a variety of laws we enforce.

to answer any question on constitutional grounds or on the basis of any other legal right or privilege, including protection against self-incrimination, but must answer any other question that is not subject to the right or privilege. If the person refuses to answer a question on grounds that the answer would be self-incriminating, the Attorney General may compel the person to testify as provided in ORS 136.617.

(b) The Attorney General shall exclude from the place in which the Attorney General conducts an examination under this subsection all persons other than the person the Attorney General is examining, the person's attorney, the officer before which the person gives the testimony and any stenographer recording the testimony.

(3)

(a) The Attorney General shall hold in confidence and not disclose to any person any documents, including data protection assessments, answers to interrogatories and transcripts of oral testimony, except that the Attorney General may disclose the documents to:

(A) The person that provided the documents or the oral testimony;

(B) The attorney or representative of the person that provided the documents or oral testimony;

(C) Employees of the Attorney General; or

(D) An official of the United States or of any state who is authorized to enforce federal or state consumer protection laws if the Attorney General first obtains a written agreement from the official in which the official agrees to abide by the confidentiality requirements of this subsection.

(b)

(A) The Attorney General may use any of the materials described in paragraph (a) of this subsection in any investigation the Attorney General conducts under this section or in any action or proceeding the Attorney General brings or initiates in a court or before an administrative agency in connection with the investigation.

(B) Notwithstanding the prohibition against disclosure in paragraph (a) of this subsection, the Attorney General may disclose a document to a committee of the Legislative Assembly in any manner and for any purpose the Attorney General deems appropriate.

(4)

(a) The Attorney General may bring an action to seek a civil penalty of not more than $7,500 for each violation of sections 1 to 10 of this 2023 Act or to enjoin a violation or obtain other equitable relief. The Attorney General shall bring the action in the circuit court for Multnomah County or the circuit court of a county where any part of the violation occurred.

(b) If a court finds that a director, member, officer, employee or agent of a controller violated sections 1 to 10 of this 2023 Act through an act or omission, the court may find that the controller committed the violation or the court may find that both the controller and the director, member, officer, employee or agent committed the violation and may impose separate civil penalties on each.

(c) A court may award reasonable attorney fees, expert witness fees and costs of investigation to the Attorney General if the Attorney General prevails in an action under this subsection. The court may award reasonable attorney fees to a defendant that prevails in an action under this subsection if the court finds that the Attorney General had no objectively reasonable basis for asserting the claim or for appealing an adverse decision of the trial court.

(d) The Attorney General shall deposit the proceeds of any recovery under this subsection into the Department of Justice Protection and Education Revolving Account, as provided in ORS 180.095.

[*(5) Before bringing an action under subsection (4) of this section, the Attorney General shall notify a controller of a violation of sections 1 to 10 of this 2023 Act 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.*]

[*(6)*] **(5)** The Attorney General shall bring an action under subsection (4) of this section within five years after the date of the last act of a controller that constituted the violation for which the Attorney General seeks relief.

[*(7)*] **(6)** The remedies available to the Attorney General under subsection (4) of this section are in addition to and not in lieu of any other relief available to the Attorney General or another person under other applicable provisions of law. A claim available under another provision of law may be joined to the Attorney General's claim under subsection (4) of this section.

SECTION 13.

(1) Sections 1 to 9 of this 2023 Act and the amendments to ORS 180.095 by section 11 of this 2023 Act become operative on July 1, 2024.

(2) Section 5(5)(c) of this 2023 Act becomes operative on July 1, 2025.

(~~2~~3) Section 10 of this 2023 Act becomes operative on ~~January~~ July 1, 2026.

(~~3~~4) The amendments to section 9 of this 2023 Act by section 12 of this 2023 Act become operative on ~~January~~ July 1, 2025.

Commented [MK93]: This delays implementation for the global opt-out. See comments above in Section 5(5)(c) for further explanation.

Commented [MK94]: Per our comments above, industry has requested that the private right of action be eliminated. If that were to happen, this provision would need to be removed.

Commented [MK95]: This date was incorrect in our LC submission. We intended for the private right of action to go into effect two years after the effective date of the Act.

Commented [MK96]: This date was incorrect in our LC submission. We intended for the notice and right to cure to sunset one year after the law becomes operative.