

## US State Consumer Privacy Laws Overview

As of December 2024

### + Background

Unlike the European Union and some other countries, the U.S. does not have a holistic comprehensive federal law regulating [consumer](#) privacy and processing of personal information. At the federal level, the [Family Educational Rights and Privacy Act \(FERPA\)](#) governs the privacy and security of student educational records, and the [Health Insurance Portability and Accountability Act \(HIPAA\)](#) regulates the use and disclosure of protected health information by covered entities.

Comprehensive consumer privacy laws have been enacted in California, Colorado, Connecticut, Delaware, Florida, Indiana, Iowa, Kentucky, Maryland, Minnesota, Montana, Nebraska, New Hampshire, New Jersey, Oregon, Rhode Island, Tennessee, Texas, Utah, and Virginia. Delaware, Iowa, Maryland, Minnesota, New Jersey, and Tennessee's laws become effective in 2025, and Indiana's becomes effective in 2026.

The following provides an overview of the state privacy law landscape, including potential applicability of common state laws and requirements.

### + Definitions of Commonly Used Terms

**Biometric Data:** Data generated by automatic measurements of an individual's biological characteristics, such as fingerprint, voiceprint, eye retina or iris, or other unique biological patterns or characteristics. Typically, states have excluded from their definition physical and digital photographs as well as video or audio recordings.

**Consent:** A clear affirmative act signifying a consumer's freely given, specific, informed, and unambiguous agreement permitting processing of their personal data. [Note: Each state may define consent differently.]

**Consumer:** Defined as residents acting only in an individual or household context, not a commercial, agent or employment context. California also includes employees as consumers.

**Controller:** An entity that determines the purposes and means of processing personally identifiable information (PII).

**Data Processing:** Any operation or set of operations which is performed on personal data, whether by automated means or not. Processing includes collecting, storing, retrieving, using, transferring, combining, erasing, and destroying personal data.

**Data Protection Assessment/Data Protection Impact Assessment (DPA a/k/a DPIA):** A process that helps organizations identify and evaluate potential privacy risks and impacts associated with new PII processing activities and a description of how the risks can be mitigated. Most states allow controllers to use existing DPAs to comply with other states' laws of similar scope and effect, and a single DPA may address multiple sets of comparable operations that include similar activities.

**De-identification:** The processing of PII in a way that it makes it impossible to identify specific natural persons without the support of additional information (unlike anonymized data, which is impossible to restore).

**Personally Identifiable Information (PII):** Federal and state laws generally define PII as any information that identifies or is linked or is reasonably linkable to an individual. Examples include but are not limited to name, physical address, date of birth, email address, internet protocol (IP) address, etc.

**Private right of action (a/k/a private cause of action):** Allows an individual or organization to bring a lawsuit in court based on an alleged violation of a law and to seek relief to remedy that alleged violation.

**Processor:** Entity that processes PII on behalf of the controller. Processors are expected to assist the controller in meeting its obligations under the law, including its obligations pertaining to consumer rights and data processing security.

**Sensitive Personally Identifiable Information (Sensitive PII):** Encompasses data revealing racial or ethnic origin, religious beliefs, mental or physical health condition or diagnosis, sex life, sexual orientation, citizenship, or immigration status. Sensitive PII typically also includes the processing of genetic or biometric data for the purpose of uniquely identifying an individual, PII collected from a known child and precise geolocation data.

**Targeted advertising:** The display of an advertisement to a consumer in which the advertisement is selected based on PII obtained from that consumer's activities over time and across nonaffiliated websites or online applications to predict that consumer's preferences or interests.

**Universal Opt-Out Mechanisms (UOOMs):** A signal sent by a person's device or browser that instructs a website operator how to treat PII collected from that person's browser or device. The signal requests that the website operator does not track the user's activity across the internet, collect the user's PII for targeted advertising purposes or sell the user's PII. A growing acceptable

UOOM standard recently selected as the official UOOM for Colorado is called the Global Privacy Control (GPC), which allows users to signal their cookie preferences across websites.

### + Applicability of State Privacy Laws to Duke

With the exception of Colorado, Delaware, Maryland, Minnesota, New Jersey and Oregon, all other state consumer privacy laws exempt institutions of higher education, nonprofits, or both. Duke qualifies for these available exemptions. However, vendor or other third-party contractual terms and conditions may override state law exemptions. Even if Duke is exempted by certain state privacy laws (higher education and/or non-profit exemptions), it should be anticipated that students, employees, alumni, donors, and research subjects will have a growing awareness of privacy laws and may have questions pursuant to the laws.

### + Applicability of State Privacy Laws to Research at Duke

With the exception of New Jersey, all state consumer privacy laws exempt personal information collected as part of a clinical trial, human subject research, or similar, so as not to preempt federal laws with privacy protections already in place. Some also exempt research that is approved, monitored and governed by an institutional review board or similar independent oversight entity. Language varies by state, and it is advisable to review the state's specific laws and reach out to Duke Privacy ([privacy@duke.edu](mailto:privacy@duke.edu)) for further information.

### + Common State Requirements

#### Data Subject Rights Commonly Found in Comprehensive State Privacy Laws

Data subjects may:

- Confirm whether a controller is processing their PII and access such data.
- Correct inaccuracies in one's PII.
- Request deletion of PII provided by or obtained about the data subject.
- Obtain a copy of the PII processed by the controller in a format that allows the consumer to transfer their PII to another controller.
- Opt out of processing for the purposes of targeted advertising, sale of PII or profiling in furtherance of solely automated decisions that produce legal or similarly significant effects impacting the data subject.

- Opt in for processing of sensitive PII (majority of but not all state privacy laws).
- Appeal any refusal by a controller to act on requests by the data subject to exercise their rights.
- Some states allow consumers to opt out of processing of their PII by using UOOMs.

### **Typical PII Disclosure Exceptions**

State privacy laws generally allow controllers and processors to disclose PII when necessary to comply with civil, criminal, regulatory inquiry, investigation, subpoena or summons by a federal, state, local or governmental authority or to cooperate with law enforcement agencies or where disclosure is essential for the life or physical safety of a consumer or other individuals.

### **Enforcement**

In most states the State Attorney General has enforcement authority. Currently one state, California, provides consumers with a private right of action, which permits an individual or organization to sue offenders in the event of a data breach or other violation and to seek financial relief or benefit to remedy the violation.

Except for Rhode Island, every state privacy law has included a “right to cure,” giving businesses an opportunity to remedy a purported violation before penalties are levied. The state cure periods typically range from 30 to 90 days. Many states plan to sunset the right-to-cure provisions, while Florida, Indiana, Iowa, Tennessee, Texas, Utah and Virginia have no cure period expiration at this time.

### **Privacy Policy/Notices**

State privacy laws generally require controllers to post or provide consumers with a “reasonably accessible, clear and meaningful” privacy notice with disclosures regarding:

- Categories of PII collected and processed
- Purpose of PII processing
- Explanation of how consumers may exercise and appeal denials of their rights
- Categories of PII shared with third parties
- Categories of third parties with whom PII is shared
- Explanation of how consumers may exercise their rights and appeal the controller’s decisions
- Sales of PII or processing for targeted advertising
- An active email address or online mechanism for the consumer to directly contact the controller.

### **Consumers Known to be Under Thirteen Years Old**

State privacy laws typically define the PII of consumers known to be under 13 years old as “sensitive PII” and require controllers to process such data in accordance with the [Children’s Online Privacy Protection Act \(COPPA\)](#).

## Information Security

State privacy laws generally require that controllers establish and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity and accessibility of PII and to secure it from unauthorized access. The degree of security should be appropriate to the volume and nature of the data. Specific safeguards, such as encryption and multifactor authentication do not tend to be enumerated.

## Data Protection Assessment or Data Protection Impact Assessment (DPA or DPIA)

A DPA is a process that helps organizations identify and evaluate potential privacy risks and impacts associated with new PII processing activities and a description of how the risks can be mitigated. The overarching goal of a DPA is to understand the facts, benefits, trade-offs, and risks of processing people’s data. States typically require DPAs when the processing poses a “heightened risk of harm” to the consumer. Most states, except currently Iowa and Utah, require controllers to complete DPAs for the following processing activities:

- Targeted advertising
- Sales of PII
- Profiling depending on risk factors
- Processing of sensitive PII
- Processing activity that presents a heightened risk of harm to consumers.

Common elements of DPAs include the following:

- Description of the PII processing activity: categories of data, sensitivity of data, context, core purpose (standard who, what, when, where and how questions).
- The parties involved in the processing activity including the relationship between the organization and the consumer.
- Information relating to the lawfulness of processing (e.g. valid consent, contract, transparent notice, etc.).
- Information relating to consumers’ rights (privacy notices, how to exercise rights, contact information).
- Information relating to data transfers, including transfers outside of an organization.
- Sources and nature of primary risks and measures taken to mitigate or offset the risks including security measures.

## **Processing Agreement Between Controllers and Processors**

State privacy laws generally require controllers to enter contracts with data processors, which govern the processor's data processing procedures. At a high-level, contracts should stipulate clear instructions for processing PII, the nature and purpose of processing, the type of data subject to processing, the duration of processing and retention guidelines, the parties' rights and obligations and execution of contracts with sub processors that hold them to the same privacy and data protection requirements as the processors.

## **Data Minimization & Non-discrimination**

States increasingly insist on data minimization principles, where controllers limit PII collection to what is "adequate, relevant and reasonably necessary" to achieve the purposes of collection as disclosed to the consumer. Controllers may not process PII for purposes that are neither reasonably necessary nor compatible with the disclosed purpose for which PII is processed unless the controller obtains consumer consent.

State laws generally require that controllers may not process PII in violation of state and federal anti-discrimination laws or discriminate against a consumer for exercising any of their consumer rights under the laws, such as by denying goods or services, charging different prices or rates, or providing a different level of quality of goods or services.

## **HR Data Exemptions**

With the exception of California, State privacy laws exempt data collected about employees, job applicants and other human resources (HR) data. In contrast, all HR data is covered under The California Privacy Rights Act.

## **Universal Opt-Out Mechanisms (UOOMs)**

Several states require or will soon require the ability for users to signal their cookie preferences via a personal device or browser. The opt out preference signal instructs a website operator how to treat PII collected from a user's browser or device. The signal may request that a website operator not track the user's activity across the internet, collect the user's PII for targeted advertising purposes or sell the user's PII.

## **+ Examples of when to contact Duke Privacy ([privacy@duke.edu](mailto:privacy@duke.edu))**

- I have questions related to state privacy laws and their applicability to Duke.
- I received a request from a resident in another state to correct or erase personal data that is maintained by Duke or my school/department.

## **Duke | Office of Audit, Risk and Compliance**

US State Consumer Privacy Laws Guidance

December 1, 2024, v.1

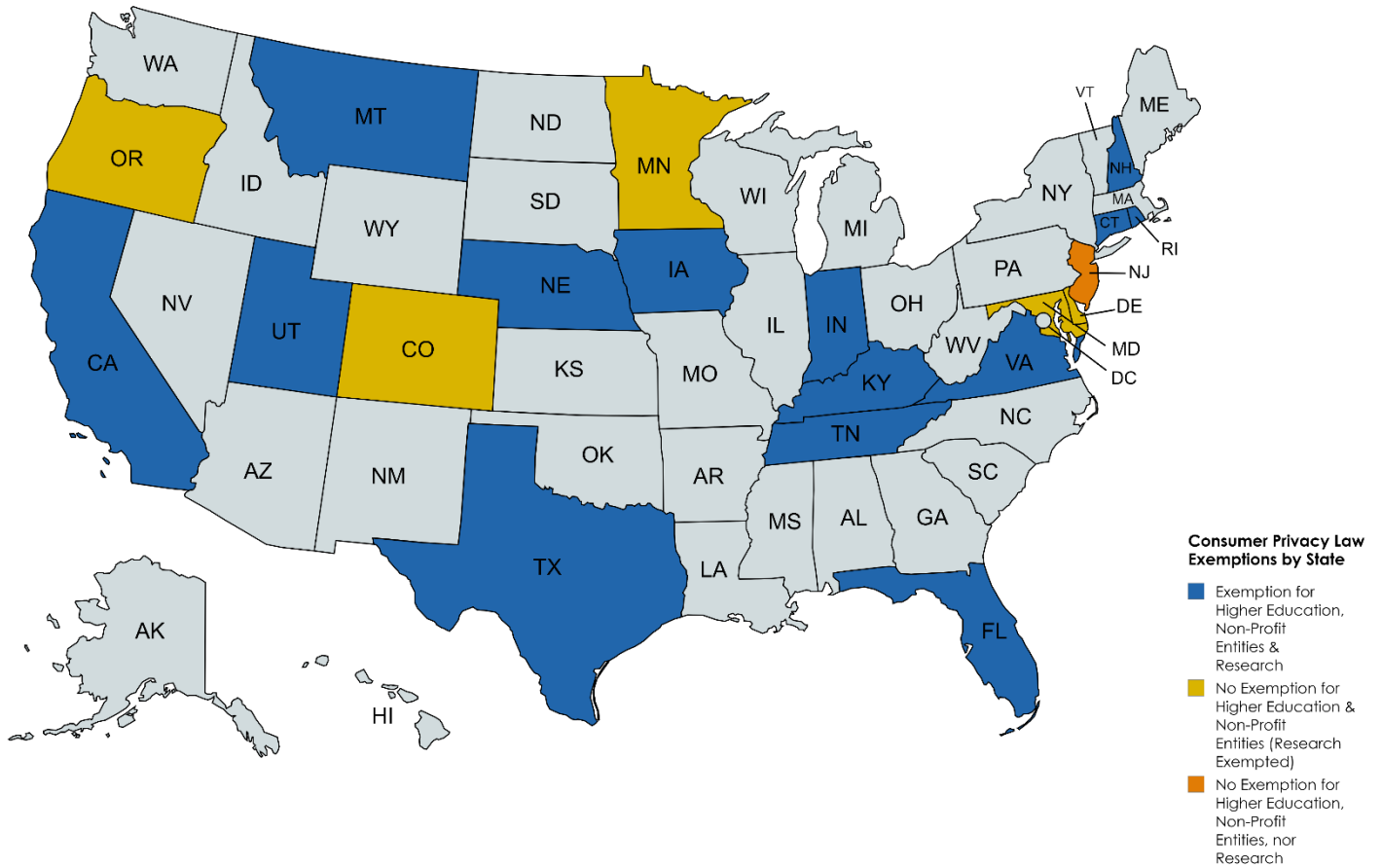
- I am engaged in a project that involves the processing (collection, storage, retrieval, transfer) of personal data from data subjects in one or more states and I seek to understand whether there are state privacy law requirements that pertain to my project.
- I believe that Duke has suffered a security incident resulting in a potential data breach containing personal data of an individual(s)
- I received a request for information pertaining to Duke's data privacy and security controls, processes, or policies\*.

*\*As a rule, Duke does not provide sponsors, vendors, or other external third parties with detailed information regarding Duke's privacy and security controls, processes or policies. As such, Duke does not complete data security questionnaires or surveys that seek to obtain information regarding Duke's security network, privacy framework or incident/breach history.*

## + State Privacy Laws Map and Overview Diagram

Click [here](#) for link to map

Click [here](#) for link to diagram



Created with mapchart.net

## + States That Do Not Exempt Higher Education Institutions and Non-Profits (Colorado, Delaware, Maryland, Minnesota, New Jersey and Oregon)

The below breakdown of State Consumer Privacy Laws is intended for informational purposes and does not imply applicability to Duke or its affiliates. Please reach out to Duke Privacy ([privacy@duke.edu](mailto:privacy@duke.edu)) for any questions pertaining to their applicability.

### + Colorado

#### *Colorado Privacy Act (CPA)*

**Effective Date:** July 1, 2023

**Enforced By:** Colorado Attorney General

**Exemptions:** Data covered by FERPA ([Non-profit entities not exempted](#))

**Penalties:** Up to \$20,000 per violation, up to \$50,000 for violations impacting elderly persons' data.

**Applies to:** Organizations conducting business in CO and:

- 1) Controls or processes PII of over 100,000 state residents during a calendar year; or
- 2) Derives revenue or receives discounts on the price of goods or services from the sale of PII, provided that the entity also processes or controls the personal data of 25,000 or more Colorado consumers.

#### **General Requirements if Thresholds Met:**

- 1) Right to access, correct, delete, and opt out of sale of PII, targeted advertising and certain types of profiling based on one's PII.
- 2) Consent required for processing sensitive PII including consent from a child's parent or legal guardian to process a child's PII.
- 3) Controller must provide a reasonably accessible, clear, and meaningful privacy notice.
- 4) Restrict PII collection to what is adequate, relevant, and limited to specified purpose and reasonably protect the PII.
- 5) Processing activities governed by a data processing agreement that sets forth the controller's processing instructions and specified obligations.
- 6) Conduct a formal data protection assessment if PII processing presents a heightened risk of harm to consumers.
- 7) Controllers must allow consumers to use a "user-selected universal opt-out mechanism (UOOM)" as specified by the Attorney General (AG).

## + Delaware

### *Delaware Personal Data Privacy Act (DPDPA)*

**Effective Date:** January 1, 2025

**Enforced By:** Delaware Department of Justice

**Exemptions:** Exempts PII regulated by FERPA (No exemption for Higher Education Institutions or Non-profit entities except non-profits dedicated to preventing and addressing insurance crime and those that collect personal data of victims & witnesses of sexual or violent crimes)

**Penalties:** Up to \$10,000 per willful violation

**Applies to:** Applies to entities that conduct business in DE or produce products and services targeted to DE residents and who during the preceding calendar year:

- 1) Controlled or processed PII of at least 35,000 DE residents, excluding PII controlled or processed solely for the purpose of completing a payment transaction or
- 2) Controlled or processed PII of at least 10,000 DE residents and derived more than 20% of their gross revenue from the sale of PII.

### **General Requirements if Thresholds Met:**

- 1) Consumer has the right to access, correct, delete, and obtain a copy of their PII.
- 2) Consumer's consent required to process sensitive PII.
- 3) DE consumer has the right to opt out of the sale or sharing of PII for use in decision-making technology, targeted advertising, and sale of PII for profiling purposes.
- 4) DE consumer may confirm whether controller is processing consumer's data and the categories of third parties to which controller has disclosed consumer's PII.
- 5) Limit PII collection to what is adequate, relevant, and reasonably necessary in relation to disclosed purposes for which PII is processed.
- 6) Provide an accessible, meaningful, and clear privacy policy.
- 7) By January 1, 2026, allow consumers to opt out of the sale or processing of their PII for purposes of targeted advertising through an opt-out preference signal.
- 8) Controllers that control or process PII of at least 100,000 consumers must complete and update on a regular basis a data protection assessment for PII processing that presents a heightened risk of harm to consumers.
- 9) Processing agreement required between controllers and processors that stipulates how processors process consumer's PII.
- 10) Establish, implement, and maintain reasonable administrative, technical and physical data security practices to protect the confidentiality, integrity and accessibility of consumers' personal data appropriate to the volume and nature of the personal data at issue.

## **+ Maryland**

### ***Maryland Online Data Privacy Act (MODPA)***

**Effective Date:** October 1, 2025 but does not apply to PII processing activities undertaken before April 1, 2026

**Enforced By:** Maryland Attorney General

**Exemptions:** Exempts PII regulated by FERPA ([No exemption for Higher Education Institutions or Non-profit entities](#))

**Penalties:** Up to \$10,000 for the first violation and up to \$25,000 for subsequent violations plus attorney's fees.

**Applies to:** Entities conducting business in Maryland or providing products or services directed to Maryland residents and during the calendar year:

- 1) Controls or processes PII from 35,000+ MD residents; or
- 2) Controls or processes PII of 10,000+ consumers in addition to obtaining at least 20% of gross revenue from PII sales.

### **General Requirements if Thresholds Met:**

- 1) Consumer has the right to access, correct, delete, and obtain a copy of their PII.
- 2) Consumer has the right to opt out of sales of their PII and use of PII for targeted advertising or profiling.
- 3) Controller is to provide a reasonably accessible, meaningful, and clear privacy policy notice.
- 4) Controllers must limit their collection "to what is reasonably necessary and proportionate to provide or maintain a product or service requested by the consumer to whom the data pertains."
- 5) Controllers may not process sensitive PII, regardless of consumer consent, except when doing so is "strictly necessary" to "provide or maintain a specific product or service requested by the consumer."
- 6) Controllers are prohibited from selling sensitive PII regardless of whether a consumer consents.
- 7) Establish, implement, and maintain reasonable administrative, technical and physical data security practices to protect the confidentiality, integrity and accessibility of personal data and to secure it from unauthorized access.
- 8) Conduct a data protection impact assessment on the processing of PII that presents a heightened risk of harm to the consumer.
- 9) Processing agreement required between controllers and processors that stipulates how processors process consumer's PII.

- 10) Controllers must allow consumers to communicate privacy preferences automatically through online universal opt-out mechanisms (UOOMs).

## + Minnesota

### *Minnesota Consumer Data Privacy Act (Minnesota Act)*

**Effective Date:** July 31, 2025

**Enforced By:** Attorney General

**Exemptions:** Exempts data covered by FERPA. (No exemptions for Higher Education Institutions and Non-profit entities, except non-profits established to detect and prevent insurance fraud are exempted. Excludes small businesses as defined by the SBA.)

**Penalties:** Up to \$7,500 per violation

**Applies to:** Controllers who either conduct business in MN or produce products or services targeted to residents of MN and who, within a calendar year either:

- 1) Control or process the PII of at least 100,000 unique MN consumers; or
- 2) Control or process 25,000 unique MN consumers' PII and derive over 25% of gross revenue from the sale of PII.

#### **General Requirements if Thresholds Met:**

- 1) Consumer has the right to access, correct, delete, and obtain a copy of their PII.
- 2) Requires consumer consent to process sensitive PII.
- 3) Requires controllers to maintain data inventories and document and maintain a description of policies and procedures adopted by the controller to comply with the Act's provisions (unique to MN).
- 4) Requires controllers to recognize UOOMs for consumers to opt out of sales and targeted advertising.
- 5) Consumer has a right to obtain a list of categories of third parties to which the controller has disclosed consumer's PII.
- 6) Statutorily provides that controllers do **not** have to produce sensitive PII such as SSNs, driver's license numbers and biometric data in response to a consumer's request to access their data.
- 7) Consumers have the right to question the results of a controller's profiling and challenge inaccurate information.
- 8) Controller may not retain PII that is no longer relevant and reasonably necessary for the purposes for which the data was collected and processed, unless retention is otherwise required by law or permitted under an exception.

- 9) Processing agreement required between controllers and processors that stipulates how processors process consumer's PII.
- 10) Requires controllers to conduct data protection impact assessments for processing activities that present a heightened risk of harm to consumers. Includes targeted advertising, sale of PII, processing sensitive PII and profiling if it presents a reasonably foreseeable risk of unfair or deceptive or unlawful disparate impact on consumers.
- 11) Establish and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity and accessibility of PII that are appropriate for PII volume and type.

## **+ New Jersey**

### ***New Jersey Data Privacy Act (NJPA)***

**Effective Date:** January 16, 2025

**Enforced By:** New Jersey Attorney General

**Exemptions:** No exemptions for Higher Education Institutions and Non-profit entities, nor PII regulated by FERPA.

**Penalties:** Up to \$10,000 for the first violation, up to \$20,000 for subsequent violations plus attorney's fees.

**Applies to:** Controllers conducting business in NJ or producing products or services targeted to NJ residents (consumers) and that during a calendar year either:

- 1) Control or process PII of at least 100,000 consumers except PII processed solely for completing payment transactions; or
- 2) Control or process PII of at least 25,000 consumers while deriving revenue or receiving a discount on the price of any goods or services, from selling PII.

### **General Requirements if Thresholds Met:**

- 1) Consumer has the right to access, correct, delete, and obtain a copy of their PII.
- 2) Consumer has the right to opt out of data processing for targeted advertising, PII sales, or profiling.
- 3) Requires controllers to provide consumers with a "reasonably accessible, clear and meaningful" privacy notice.
- 4) Requires controllers to clearly disclose to consumers if they sell PII to third parties or process PII for targeted advertising or profiling and provide a clear method for consumers to opt out.

- 5) Requires consumer consent to process sensitive PII. Unique to NJ, sensitive PII encompasses potentially all a consumer's financial information to the extent it is not covered by the Gramm-Leach-Bliley Act.
- 6) Provide a mechanism for a consumer to revoke consent to process PII and cease processing within 15 days of consent revocation.
- 7) Processing agreement required between controllers and processors that stipulates how processors process consumer's PII.
- 8) Requires controllers to conduct data protection impact assessments for processing activities that present a heightened risk of harm to consumers. Includes targeted advertising, sale of PII, processing sensitive PII and profiling if the profiling presents a reasonably foreseeable risk of unfair or deceptive treatment or unlawful disparate impact on consumers.
- 9) Establish and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity and accessibility of PII and to secure it from unauthorized access.
- 10) By July 15, 2025, allows consumers to opt out of profiling in furtherance of decisions that produce legal or similarly significant effects (unique to NJ) and like other state laws to opt out of targeted advertising and sale of personal data by using UOOMs. Prohibits UOOMs configured for opt in by default.

## **+ Oregon**

### **Oregon Consumer Privacy Act:**

**Effective Date:** July 1, 2024

**Enforced By:** Oregon Attorney General

**Exemptions:** Exempts data covered by FERPA. (No exemptions for Higher Education Institutions and Non-profit entities, except non-profits established to detect and prevent insurance fraud or provide programming to radio/television networks, are exempted.)

**Penalties:** Up to \$7,500 per violation

**Applies to:** Organizations that conduct business in Oregon or produces products or services that are targeted to residents of Oregon and during a calendar year:

- 1) Controls or processes PII of at least 100,000 Oregon residents, excluding PII controlled or processes solely for the purpose of completing a payment transaction; or
- 2) Controls or processes PII of not less than 25,000 Oregon residents and derives more than 25% of its gross revenue from the sale of PII.

### **General Requirements if Thresholds Met:**

- 1) Consumer has the right to access, correct, delete and obtain a copy of their PII.
- 2) Requires consumer consent to process sensitive PII.
- 3) Consumer may revoke previous consent to process their PII. Revocation must be honored within 15 days of request receipt.
- 4) Consumer may opt out of their PII processing for purposes of targeted ads, sale of PII (whether for monetary or other valuable consideration), or profiling that produces legal or similarly significant effects for the consumer.
- 5) Unlike most other state privacy laws, Oregon requires controllers to disclose, to the extent possible, how third parties may process PII shared with them by the controller.
- 6) Establish, implement and maintain reasonable administrative, technical and physical data security practices to protect the confidentiality, integrity and security of consumers' PII.
- 7) Requires controllers to conduct data protection impact assessments for processing activities that present a heightened risk of harm to consumers. Includes targeted advertising, sale of PII, processing sensitive PII and profiling if the profiling presents a reasonably foreseeable risk of unfair or deceptive treatment or unlawful disparate impact on consumers.
- 8) Controllers are to provide a reasonably accessible, clear and meaningful privacy notice.
- 9) Processing agreement required between controllers and processors.
- 10) Allow consumers to opt out of processing of their PII by using UOOMs.