Maryland Online Data Privacy Act Summary

On May 9, 2024 Governor Wes Moore (D) signed SB 541, the "**Maryland Online Data Privacy Act**" into law. The Act's provisions take effect on **October 1, 2025**. However, the law specifies it will apply only prospectively and may not be applied or interpreted to have any effect on or application to any personal data processing activities before **April 1, 2026**. A non-comprehensive summary of significant elements of the Act follows:

Covered Entities	The **Maryland Online Data Privacy Act** applies to a person that conducts business in Maryland or provides products or services that are targeted to residents of Maryland and that during the preceding calendar year: (i) controller or processed the personal data of at least 35,000 consumers, excluding personal data controlled or processed for the purpose of completing a payment transaction, or; (ii) controlled or processed the personal data of at least 10,000 consumers and derived more than 20% of its gross revenue from the sale of personal data.
Covered Data	***"Biometric data"***: data generated by automatic measurements of the biological characteristics of a consumer that can be used to *uniquely authenticate* a consumer's identify including a fingerprint, a voice print, an eye retina or iris image, and any other unique biological characteristics that can be used to uniquely authenticate a consumer's identity. "Biometric data" does *not* include a digital or physical photograph, an audio or video recording, or any data generated from a digital or physical photograph or an audio or video recording, unless the data is generated to identify a specific consumer. ***"Personal data"***: any information that is linked or can be reasonably linked to an identified or identifiable consumer. "Personal data" does not include de-identified data or publicly available information. ***"Consumer Health data"***: personal data that a controller uses to identify a consumer's physical or mental health *status*. "Health data" includes data related to gender-affirming treatment or reproductive or sexual health care. "***Reproductive or Sexual Health Care"***: a health-care related service or product rendered or provided concerning a consumer's reproductive system or sexual well-being, including: a service or product provided related to an individual health condition, status, disease, diagnosis, test, or treatment; a social, psychological, behavioral, or medical intervention; a surgery or procedure; the purchase or use of a medication including a medication purchased or used for the purposes of an abortion; a service or product related to a bodily function, vital sign, or symptom; a measurement of a bodily function, vital sign, or symptom; and an abortion and medical and nonmedical services, products, diagnostics, counseling, and follow-up services for an abortion. ***"Sensitive data"***: personal data that includes (1) Data ***revealing*** race or ethnic origins; religious beliefs; consumer health data; sex life; sexual orientation; status as transgender or nonbinary; national origin; or citizenship or immigration status, (2) genetic data or biometric data, and (3) personal data of a consumer that the controller knows or ***has reason to know is a child*** (13). "***Publicly available information"***: information that a person lawfully obtains from a record of a governmental entity; reasonably believes a consumer or widely distributed media have lawfully made available to the general public; or if the consumer has not restricted the information to a specific audience, obtains from a person to whom the consumer disclosed the information. "Publicly available information" does not include biometric data collected by a business about a consumer without the consumer's knowledge.
Key	***"Consent"***: a clear affirmative act signifying a consumer's freely given, specific, informed, and

Definitions	unambiguous agreement to process personal data relating to the consumer for a particular purpose. "Consent" includes a written statement, a written statement by electronic means, or any other unambiguous affirmative action. ***"Dark pattern"***: a user interface designed or manipulated with the substantial effect of subverting user autonomy, decision making, or choice. "Dark pattern" includes any practice the Federal Trade Commission refers to as "dark pattern". ***"De-Identified Data"***: data that cannot reasonably be used to infer information about a consumer or linked to an identifiable consumer and is subject to: (i) administrative and technical measures to ensure that the data cannot be associated with a particular consumer; (ii) public commitment by the company to maintain and use data in a unidentifiable form and not attempt to reidentify data, and; (iii) legally enforceable contractual obligations that prohibit a recipient of the data from attempting reidentify the data. ***"Process"***: an operation or set of operations performed by manual or automated means on personal data or on sets of personal data. ***"Targeted Advertising"***: displaying advertisements to a consumer on a device identified by a unique identifier, where the advertisement is selected based on personal data obtained or inferred from the consumer's activities over time and across nonaffiliated websites or online applications that are unaffiliated with each other, in order to predict the consumer's preferences or interests. ***"Sale of Personal Data"***: the exchange of personal data by a controller, a processor, or an affiliate of a controller or processor to a third party for monetary or other valuable consideration. "Sale of personal data" does not include: (a) the disclosure of personal data to a processor that processes the personal data on behalf of the controller if limited to the purposes of the processing; (b) the disclosure of personal data to a third party for purposes of providing a product or service affirmatively requested by the consumer; (c) the disclosure or transfer of personal data to an affiliate of the controller; (d) the disclosure of personal data where the consumer directs the controller to disclose the personal data or intentionally these the controller to interact with a third party; (e) the disclosure of personal data that the consumer intentionally made available to the general public through a channel of mass media and did not restrict to a specific audience, or; (f) the disclosure or transfer of personal data to a third party as an asset that is part of a proposed or actual or proposed merger, acquisition, bankruptcy, or other transaction where the third party assumes control of all or part of the controller's assets.
Consumer Rights	**Access:** A consumer shall have the right to confirm whether a controller is processing the consumer's personal data. If a controller is processing a consumer's personal data, a consumer shall have the right to access the consumer's personal data. **Correction:** A consumer shall have the right to correct inaccuracies in the consumer's personal data, considering the nature of the consumer's personal data and the purposes of processing the data. **Deletion**: A consumer shall have the right to require a controller to delete personal data provided by, or obtained about, the consumer unless retention of the personal data is required by law. A controller that has obtained personal data about a consumer from a source other than the consumer shall be considered compliant with a consumer's request to delete the consumer data by retaining a cord of the deletion request and the minimum data necessary for the purpose of ensuring that the consumer's personal data remains deleted from the controller's records and is not benign used for any other purpose.

	Opt Out Rights: A consumer shall have the right to opt out of the processing of personal data for purposes of targeted advertising, the sale of personal data, or profiling in furtherance of solely automated decisions that produce legal or similarly significant effects concerning the consumer. **Portability:** If the processing of personal data is done by automated means, a consumer shall have the right to obtain a copy of the consumer's personal data processed by the controller in a portable and, to the extent technically feasible, readily usable format that allows the consumer to easily transmit the data to another controller without hindrance. **Revocation:** A controller must provide an effective mechanism for a consumer to revoke the consumer's consent that is at least as easy as the mechanism by which the consumer provided the consumer's consent. If a consumer revokes consent, the controller shall stop processing the consumer's data as soon as practicable, but not later than 30 days after receiving the request. **Third Parties:** A consumer shall have the right to obtain a list of the categories of third parties to which the controller has disclosed the consumer's personal data or a list of the categories of third parties to which the controller has disclosed any consumer's personal data if the controller does not maintain this information in a format specific to the consumer.
Business Obligations	A controller may not: • Sell sensitive data; • Process personal data in violation of state or federal laws that prohibit unlawful discrimination; Process the personal data of a consumer for the purposes of targeted advertising if the controller knew or *should have known* that the consumer is under the *age of 18 years;* • Sell the personal data of a consumer if the controller knew or should have known that the consumer is under the age of 18 years; • Unless the controller obtains the consumer's consent, a controller shall not process personal data for a purpose that is neither reasonably necessary to, nor compatible with, the disclosed purposes for which the personal data is processed, as disclosed to the consumer. **Data Minimization**: A controller shall limit the ***collection*** of personal data to what is reasonably necessary and proportionate **to provide or maintain** a specific product or service requested by the consumer to whom the data pertains. **Purpose Limitation**: Unless the controller obtains the consumer's consent, a controller shall not **process** personal data for a purpose that is neither reasonably necessary to, nor compatible with, the disclosed purposes for which the personal data is processed, as disclosed to the consumer. **Sensitive Data Limitation**: A controller may not except where the collection or processing is strictly necessary to provide or maintain a specific product or service requested by the consumer to whom the personal data pertains, collect, process or share sensitive data concerning a consumer. **Data Security**: A controller shall establish, implement, and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data appropriate to the volume and nature of the personal data at issue. **Disclosure**: If a controller sells personal data to third parties or processes personal data for targeted advertising or for the purposes of profiling the consumer in furtherance of decisions that produce legal or similarly significant effect, the controller shall clearly and conspicuously disclose the sale or processing, as well as the manner in which a consumer may exercise the right to opt out of the sale or processing. The disclosure must be prominently displayed and use clear, easy to understand, and

unambiguous language, to state whether the consumer's information will be sold or shared with a third party.

Third Parties: If a third party uses or shares a consumer's information in a manner inconsistent with promises made to the consumer at the time of collection of the information, the third party shall provide an affected consumer with notice of the new or changed practice before implementing the new or changed practice.

No Unlawful Discrimination: A controller shall not collect, process, or transfer personal data or publicly available data in a manner that unlawfully discriminates in or otherwise unlawfully makes unavailable the equal enjoyment of goods or services on the basis of race, color, religion, national origin, sex, sexual orientation, gender identity, or disability, unless the collection, processing, or transfer of personal data is for: (i) the controller's self-testing to prevent or mitigate unlawful discrimination; (ii) the controller's diversifying of an applicant, participant, or customer pool, or; (iii) a private club or group not open to the public, as described in § 201(E) of the Civil Rights Act of 1964. A controller shall not discriminate against a consumer for exercising a consumer right, including denying goods and services, charging different prices or rates for goods or services, or providing a different level of quality of goods and services to the consumer.

Responding to Consumer Requests: The privacy notice under subsection (D) must establish one or more secure methods for a consumer to submit a request to exercise a consumer right that takes into account: (i) the ways in which consumer normally interact with the controller; (ii) the need for secure and reliable communication of consumer request, and; (iii) the ability of the controller to verify the identity of a consumer making the request. A controller may not require a consumer to create a new account in order to exercise a consumer right. A controller may require a consumer to use an existing account to exercise a consumer right. A controller shall respond to a consumer request not later than 45 days after the controller receives the consumer request. A controller may extend the completion period by an additional 45 days if: (i) it is reasonably necessary to complete the request based on the complexity and number of the consumer's requests, and; (ii) the controller informs the consumer of the extension and the reason for the extension within the initial 45-day response period. If a controller declines to act regarding a consumer's request, the controller shall: (i) inform the consumer without undue delay, but not later than 45 days after receiving the request, of the justification for declining to act, and; (ii) provide instructions for how to appeal the decision.

A controller shall establish a process for a consumer to appeal the controller's refusal; to act on a consumer's rights within a reasonable period after the consumer receives the decision. The appeal process must be conspicuously available and similar to the process for submitting requests to initiate an action. Not later than 60 days after receiving an appeal, a controller must inform the consumer in writing of any action or not taken in response to the appeal, including a written explanation of the reasons for the decisions. If a controller denies an appeal, the controller must provide the consumer with an online mechanism, if available, through which the consumer may contact the Division of Consumer Protection to submit a complaint.

A controller shall provide information to a consumer in response to a consumer's request to exercise rights free of charge once during any 12-month period. The controller has the burden of demonstrating the manifestly unfounded, excessive, technically infeasible, or repetitive nature of a request. If requests from a consumer are manifestly unfounded, excessive, technically infeasible, or repetitive, a controller may charge the consumer a reasonable fee to cover the administrative costs of complying with the request or decline to act on the request.

If a controller is unable to authenticate a request to exercise a consumer right using commercially

	reasonable efforts, the controller may not be required to comply with a request to initiate an action and shall provide notice to the consumer that the controller is unable to authenticate the request to exercise the right until the consumer provides additional information reasonably necessary to authenticate the consumer and the consumer's request to exercise the consumer's rights. **Transparency**: A controller shall provide a consumer with a reasonably accessible, clear, and meaningful privacy notice that includes: (i) the categories of personal data processed by the controller, including sensitive data; (ii) the controller's purpose for processing personal data; (iii) how a consumer may exercise their consumer rights, including how a consumer may appeal a controller's decision regarding the consumer's request or may revoke consent; (iv) the categories of third parties with which the controller shares personal data with a level of detail that enables a consumer to understand the type of, business model of, or processing conducted by each third party; (v) the categories of personal data, including sensitive data, that the controller shares with third parties, and; (vi) an active e-mail address or other online mechanism that a consumer may use to contact the controller. **Universal Opt-Out Mechanisms:** On or before October 1, 2025, a controller may allow a consumer to opt out of any processing of the consumer's personal data for the purposes of targeted advertising, ***or*** any sale of personal data, through an opt-out preference signal sent, with the consumer's consent, by a platform, technology, or mechanism to the controller indicating the consumer's intent to opt out of the processing or sale. A platform, technology, or mechanism must: (i) be consumer-friendly and easy-to-use by the average consumer; (ii) use clear, easy-to-understand, and unambiguous language; (iii) be as consistent as possible with any other similar platform, technology or mechanism required by any federal or state law or regulation; (iv) enable the controller to reasonably determine whether the consumer is a resident of Maryland and has made a legitimate request to opt out of the sale of the consumer's personal data or targeted advertising, and; (v) require a consumer to make an affirmative, unambiguous, and voluntary choice in order to opt out of the any processing of the consumer's personal data. A platform, technology, or mechanism may not unfairly disadvantage another controller or use a default setting to opt a consumer out of any processing of the consumer's personal data. If a consumer's decision to opt out of the processing of the consumer's personal data for the purposes of targeted advertising, or the sale of personal data through an opt-out preference signal sent conflicts with the consumer's existing controller-specific privacy setting or the consumer's voluntary participation ina controller's bona fide loyalty, rewards, premium features, discounts, or club card program, the controller may notify the consumer of a conflict and provide the choice to confirm controller-specific privacy settings or participation. A controller that recognizes signals approved by other states shall be considered in compliance.
Data Protection Assessments	A data protection assessment shall apply to processing activities that occur on or after October 1, 2025. A data protection assessment is *not* required for processing activities that occur before October 1, 2025. A controller shall conduct and document, on a regular basis, a data protection assessment for each of the controller's processing activities that present a heightened risk of harm to a consumer, ***including an assessment for each algorithm that is used***. A data protection assessment must identify and weigh the benefits that may flow directly and indirectly from the processing to the controller, the consumer, other interested parties, and the public against: (i) the potential risks to the rights of the consumer associated with the processing as mitigated by safeguards that may be employed by the controller to reduce these risks, and; (ii) the necessity and proportionality of processing unrelated to the stated purpose of the processing. A controller shall factor into a data protection assessment: (i) the use of de-identified data; (ii) the reasonab;e expectations of consumers; (iii) the context of the processing, and; (iv) the relationship

	between the controller and the consumer whose personal data will be processed. The Division of Consumer Protection may require that a controller make available to the Division of Consumer Protection a data protection assessment that is relevant to an investigation. The Division of Consumer Protection may evaluate a data protection assessment for compliance. A data protection assessment is confidential and exempt from disclosure under the federal Freedom of Information Act or the Public Information Act. A single data protection assessment may address a comparable set of processing operations that include similar activities.
Controller / Processor Distinction	**A processor shall adhere to the contract and instructions of a controller and assist the controller** in meeting its obligations under the Maryland Online Data Privacy Act, including: (i) by appropriate technical and organizational measures as much as reasonably practicable to fulfill the controller's obligation to respond to consumer rights request, considering the nature of processing and the information available to the processor; (ii) by assisting the controller in meeting the controller's obligations in relation to the security of processing the personal data and in relation to the notification of a breach of a security system, and; (iii) providing necessary information to enable the controller to conduct and document data protection assessments. A contract between a controller and a processor shall govern the processor's data processing procedures with respect to processing performed on behalf of the controller. The contract shall be binding and shall clearly set forth instructions for processing personal data, the nature and purpose of processing, the type of data subject to processing, the duration of processing, and the rights and obligations of both parties. The contract shall require that the processor: (i) ensure that each person processing personal data is subject to a duty of confidentiality with respect to the personal data; (ii) establish, implement, and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data, considering the volume and nature of the personal data; (iii) stop processing data on request by the controller made in accordance with a consumer's authenticated request; (iv) at the controller's direction, delete or return all personal data to the controller as requested at the end of the provision of service, unless retention of the personal data is required by law; (v) on the reasonable request of the controller, make available to the controller all information in the processor's possession necessary to demonstrate the processor's compliance with the obligations of the Act; (vi) after providing the controller an opportunity to object, engage a subcontractor to assist with processing personal data on the controller's behalf only in accordance with a written contract that requires the subcontractor to meet the processor's obligations regarding the personal data under the processor's contract with the controller, and; (vii) allow and cooperate with reasonable assessments by the controller, the controller's designated assessor, or a qualified and independent assessor arranged for by the processor to assess the processor's policies and technical and organizational measures in support of the obligations of the Act. On request, the processor shall provide a report of an assessment to the controller.
Exceptions and Exemptions	The Maryland Online Data Privacy Act shall not be construed to restrict a controller's or processor's ability to: (a) comply with laws; (b) comply with inquiries by government authorities; (c) cooperate with law-enforcement agencies; (d) prepare for and defend legal claims; (e) provide a product or service specifically requested by a consumer; (f) perform under a contract to which the consumer is A party, including fulfilling the terms of a written warranty; (g) take steps at the request of the consumer before entering into a contract; (h) protect interests essential for life or physical safety of a consumer or another individual and when the processing cannot be manifestly based on another legal basis; (i) prevent, detect and protect against security incidents; (j) preserve the integrity or security of systems; (j) assist another controller, processor, or third party with an obligation under the Act.

	Data exempt from the Maryland Online Data Privacy Act includes: protected information under HIPAA, the Health Care Quality Improvement Act of 1986, the Patient Safety and Quality Improvement Act, the Fair Credit Reporting Act, GLBA, the Driver's Privacy Protection Act of 1994, FERPA, the Farm Credit Act, and COPPA. Organizations that comply with COPPA's VPC requirements satisfy the Act's parental consent requirements.
Enforcement	Violations of the Maryland Online Data Privacy Act constitute an unfair, abusive or deceptive trade practice subject to enforcement and penalties under the Maryland Consumer Protection Act. **Right to Cure**: Before initiating an action, the Division of Consumer Protection of Consumer Protection may issue a notice of violation to the controller or processor if the Division of Consumer Protection determines that a cure is possible. If the Division of Consumer Protection issues a notice of violation, the controller or processor shall have at least 60 days to cure the violation after the receipt of the notice. If the controller or processor fails to cure the violation within the time period specified by the Division of Consumer Protection, the Division of Consumer Protection may bring an enforcement action. In determining whether to grant a controller or processor an opportunity to cure an alleged violation, the Division of Consumer Protection may consider: (i) the number of violations; (ii) the size and complexity of the controller or processor; (iii) the nature and extent of the controller's or processor's processing activities; (iv) the likelihood of injury to the public; (v) the safety of persons or property; (vi) whether the alleged violation was likely caused by human or technical error, and; (vii) the extent to which the controller or processor has violated the Act or similar laws in the past. The Maryland Online Data Privacy Act does not prevent a consumer from pursuing any other remedy provided by law.