Montana Consumer Data Privacy Act Summary

On May 19, 2023, Governor Greg Gianforte (R) signed SB 384, the "Montana Consumer Data Privacy Act" into law. The Act's provisions take effect on October 1, 2024. A non-comprehensive summary of significant elements of the Act follows:

Covered Entities	The **Montana Consumer Data Privacy Act** applies to persons that conduct business in the state or persons that produce products or services that are targeted to residents of the state and (a) control or process the personal data of at least 50,000 consumers, excluding personal data controlled or processed solely for the purpose of completing a payment transaction; or (b) control or process the personal data of at least 25,000 consumers and derive more than 25% of gross revenue from the sale of personal data.
Covered Data	***"Personal data"***: any information that is linked or reasonably linkable to an identified or identifiable individual. "Personal data" does not include deidentified data or publicly available information. ***"Sensitive data"***: personal data that includes: (a) racial or ethnic origin, religious beliefs, a mental or physical health diagnosis, information about a person's sex life, sexual orientation, or citizenship or immigration status; (b) the processing of genetic or biometric data for the purpose of uniquely identifying an individual; (c) personal data collected from a known child; (d) precise geolocation data.
Key Definitions	***"Consent"***: a clear affirmative act signifying a consumer's freely given, specific, informed, and unambiguous agreement to allow the processing of personal data relating to the consumer. "Consent" may include a written statement, including a statement by electronic means, or any other unambiguous affirmative action. ***"Dark Pattern:"*** a user interface designed or manipulated with the effect of substantially subverting or impairing user autonomy, decision-making, or choice. ***"De-Identified Data"***: data that cannot be used to reasonably infer information about or otherwise be linked to an identified or identifiable individual, or a device linked to that individual if the controller that possesses the data: (a) takes reasonable measures to ensure that the data cannot be associated with an individual; (b) publicly commits to process the deidentified fashion only and to not attempt to reidentify the data; and (c) contractually obligates any recipients of the data to satisfy the criteria set forth in subsections (11)(a) and (11)(b). ***"Pseudonymous Data"***: personal data that cannot be attributed to a specific individual without the use of additional information, provided the additional information is kept separately and is subject to appropriate technical and organizational measures to ensure that the personal data is not attributed to an identified or identifiable individual. ***"Targeted Advertising"***: displaying advertisements to a consumer that is selected based on personal data obtained or inferred from that consumer's activities over time and across nonaffiliated websites or online applications to predict such consumer's preferences or interests. ***"Sale of Personal Data"***: the exchange of personal data for monetary or other valuable consideration by the controller to a third party. "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; (b) the disclosure of personal data to a third party for purposes of providing a product or service requested by the consumer; (c) the disclosure or transfer of personal information to an affiliate of the controller; (d) the disclosure of personal data in which the consumer directs the controller to disclose the personal data or intentionally uses the controller to interact with a third party; (e) the disclosure of personal data that

	the consumer intentionally made available to the public via a channel of mass media and did not restrict to a specific audience OR the disclosure or transfer of personal data to a third party as an asset that is part of a proposed or actual merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the controller's assets.
Consumer Rights	• **Access:** A consumer has the right to confirm whether a controller is processing the consumer's personal data and to access the consumer's personal data unless such confirmation or access would require the controller to reveal a trade secret. • **Correction:** A consumer has the right to correct inaccuracies in the consumer's personal data, considering the nature of the personal data and the purposes of the processing of the consumer's personal data. • **Deletion**: A consumer has the right to delete personal data about the consumer. • **Portability:** A consumer has the right to obtain a copy of the consumer's personal data previously provided by the consumer to the controller in a portable and, to the extent technically feasible, readily usable format that allows the consumer to transmit the personal data to another controller without hindrance, where the processing is carried out by automated means, provide the controller is not required to reveal any trade secret. • **Opt Out Rights**: A consumer has the right to opt out of the processing of the consumer's personal data for the purposes of targeted advertising,the sale of the consumer's personal data, and profiling in furtherance of solely automated decisions that produce legal or similarly significant effects concerning the consumer. • **Revocation**: A controller shall 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 and, on revocation of the consent, cease to process the personal data as soon as practicable, but no later than 45 days after the receipt of the request.
Business Obligations	• **Responding to Consumer Requests**: A controller shall respond to a consumer without undue delay, but not later than 45 days of receipt of a request. The controller may extend the response period by 45 additional days when reasonably necessary, considering the complexity and number of the consumer's requests, provided the controller informs the consumer of the extension with the initial 45-day response period and the reason for the extension. If a controller declines to act regarding the consumer's request, the controller shall inform the consumer without undue delay, but not later than 45 days after receipt of the request, of the justification for declining to act and provide instructions for how to appeal the decision. A consumer has the right to a free response once during any 12-month period. The controller bears the burden of demonstrating the manifestly unfounded, excessive, repetitive, or technically unfeasible nature of any denied requests and may charge the consumer a reasonable fee to cover such administrative costs or decline to act on such requests. A controller shall establish a process for a consumer to appeal the controller's refusal to take action on a request within a reasonable period of time after the consumer's receipt of the decision. The appeal process shall be conspicuously available and similar to the process for submitting requests to initiate action pursuant to this section. Within 60 days of receipt of an appeal, a controller shall inform the consumer in writing of any action taken in response to the appeal and provide the consumer with an online mechanism, if available, or other method through which the consumer may contact the attorney general to submit a complaint. • **Data Minimization**: A controller shall limit the collection of personal data to what is adequate, relevant, and reasonably necessary in relation to the purposes for which such data is processed. • **Avoid Secondary Use**: A controller shall not process personal data for purposes that are not reasonably necessary to or compatible with the disclosed purposes for which the personal data is processed, as disclosed to the consumer, unless the controller obtains the consumer's consent. • **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. • **No Unlawful Discrimination:** A controller shall not process personal data in violation of state and federal laws that prohibit unlawful discrimination against a consumer. A controller shall not discriminate against a consumer for exercising any consumer rights. • **Transparency**: A controller shall provide consumers with a reasonably accessible, clear, and meaningful privacy notice that includes: (a) the categories of personal data processed by the controller; (b) the purpose for processing personal data; (c) the categories of personal data that the controller shares with third parties, if any; (d) the categories of third parties, if any, with which the controller shares personal data; (e) an active e-mail address or other mechanism that the consumer ma use to contact the controller; and (f) how consumers may exercise their consumer rights, including how a consumer may appeal a controller's decision with regard to the consumer's request. • **Purpose Specification:** A controller shall not process personal data for purposes other than those expressly listed unless otherwise allowed by this part. Personal data processed by a controller may be processed to the extent that the processing is: (a) reasonably necessary and proportionate and (b) adequate, relevant, and limited to what is necessary in relation to the specific listed purposes. • **Disclosure**: A controller shall clearly and conspicuously disclose if the controller sells personal data to third parties or processes personal data for targeted advertising in addition to the manner in which a consumer may exercise the right to opt out of such activity.
Data Protection Assessments	A controller shall conduct and document a data protection assessment for each of the controller's processing activities that presents a heightened risk of harm to a consumer. Processing that presents a heightened risk of harm to a consumer includes: (a) the processing of personal data for the purposes of targeted advertising; (b) the sale of personal data; (c) the processing of personal data for the purposes of profiling in which the profiling presents a reasonably foreseeable risk of unfair or deceptive treatment of unlawful disparate impact on consumers, financial, physical or reputational injury to consumers or a physical or other form of intrusion on the solitude or seclusion or the private affairs or concerns of consumers in which the intrusion would be offensive to a reasonable person, or other substantial injury to consumers, and; (d) the processing of sensitive data. Data protection assessments must identify and weigh the benefits that may flow, directly and indirectly, from the processing to the controller, the consumer, other stakeholders, and the public against the potential risks to the rights of the consumer associated with the processing, as mitigated by the safeguards that can be employed by the controller to reduce the risks. The use of de-identified data and the reasonable expectations of consumers, as well as the context of the processing and the relationship between the controller and the consumer, must be factored into this assessment. The attorney general may require that a controller disclose any data protection assessment that is relevant to an investigation being conducted by the attorney general and reporter and the controller shall make assessment available. The attorney general may evaluate the assessment for compliance. Data protection assessments are confidential and exempt from disclosure under the Freedom of Information Act.
Controller / Processor Distinction	• **A processor shall adhere to the instructions of a controller and assist the controller** in meeting its obligations to include: (a) considering the nature of processing and the information available to the processor by appropriate technical and organizational measures as much as reasonably practicable to fulfill the controller's obligation to respond to consumer rights requests; (b) considering the nature of processing and the information available to the processor 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 security of the system of the processor to meet the controller's obligations; and (c) 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. The contract is binding and shall clearly set forth instructions for processing 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 must also require that the processor: (a) ensure that each person processing personal data is subject to a duty of confidentiality; (b) delete or return all personal data to the controller as requested at the end of the provision of services, unless retention of the personal data is required by law; (c) make available to the controller all information in its possession necessary to demonstrate the processor's compliance with obligations; (d) allow, and cooperate with reasonable assessments by the controller or the controller's designated assessor, or the processor may arrange for a qualified and independent assessor to conduct an assessment of the processor's policies and technical organization measures in support of the obligations using an appropriate and accepted control standard or framework and assessment procedure for the assessments; a processor shall provide a report of each assessment upon controller request; and (e) engage a subcontractor pursuant to a written contract that requires the subcontractor to meet the obligations of the processor. • **Additional Teen Privacy Protections**: A controller may not process the personal data of a consumer for the purposes of targeted advertising or sell the consumer's personal data without the consumer's consent under circumstances in which a controller has actual knowledge that the consumer is at least 13 years of age but younger than 16 years of age.
Exceptions and Exemptions	• A controller may disclose pseudonymous data or de-identified data with an exercise of reasonable oversight to monitor compliance with any contractual commitments and shall take appropriate steps to address any breaches of those contractual commitments. • The Montana Consumer 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 requested by a consumer; (f) perform under a contract to which a consumer is a party, including fulfilling the terms of a written warranty; (g) take stateps at the request of a consumer prior to entering a contract; (h) take immediate steps to protect an interest that is essential for the life or physical safety of the consumer or another individual and when the processing cannot be manifestly based on another legal basis; (i) prevent, detect, protect against or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities, or any illegal activity, preserve the integrity or security of systems, or investigate, report, or prosecute those responsible for any of these actions; (j) engage 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 or governed by an institutional review board; (k) assist another controller, processor, or third party with obligations, and (l) process personal data for reasons of public interest in public health, community health, or population health, under certain restrictions. • Data exempt from the Montana Consumer Data Privacy Act includes: nonprofit organizations, institutions of higher education, protected information under HIPAA, the Health Care Quality Improvement Act of 1986, the Patient Safety and Quality Improvement Act, the Fair Credit Reporting Act, the Driver's Privacy Protection Act of 1994, FERPA, the Farm Credit Act, and COPPA.
Enforcement	• The Montana Consumer Data Privacy Act does not provide the basis for, or be subject to, a private right of action to violations of this Act. • **Right to Cure**: The attorney general has exclusive authority to enforce violations of the Montana Consumer Data Privacy Act and shall provide a controller 60 days' written notice identifying specific provisions being violated. The 60-day cure period has a sunset date of April 1, 2026.