Minnesota Consumer Data Privacy Act Summary

On May 24, 2024 Governor Tim Walz (D) signed HF 4757, the "**Minnesota Consumer Data Privacy Act**" into law. The Act's provisions take effect on **July 31, 2025**. A non-comprehensive summary of significant elements of the Act follows:

Covered Entities	The **Minnesota Consumer Data Privacy Act** applies to legal entities that conduct business in Minnesota or produce products or services that are targeted to residents of Minnesota and satisfy one or more of the following thresholds: (i) during a calendar year, controls or processes personal data of 100,000 consumers or more, excluding personal data controlled or processed solely for the purpose of completing a payment transaction, or; (ii) derives over 25% of gross revenue from the sale of personal data and processes or controls personal data of 25,000 consumers or more. Provides an exemption for small businesses but still requires a consumer's prior consent before their sensitive data can be sold.
Covered Data	***"Biometric data"***: data generated by automatic measurements of an individual's biological characteristics, including a fingerprint, a voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that are used to identify a specific individual. "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 individual. **"*Specific geolocation data*":** means information derived from technology, including but not limited to global positioning system level latitude and longitude coordinates or other mechanisms, that directly identifies the geographic coordinates of a consumer or a device linked to a consumer with an accuracy of more than three decimal degrees of latitude and longitude or the equivalent in an alternative geographic coordinate system, or a street address derived from the coordinates. Specific geolocation data does not include the content of communications, the contents of databases containing street address information which are accessible to the public as authorized by law, or any data generated by or connected to advanced utility metering infrastructure systems or other equipment for use by a public utility. ***"Personal data"***: any information that is linked or reasonably linkable to an identified or identifiable natural person. Personal data does not include de-identified data or publicly available information. *"**Pseudonymous data**"***:** personal data that cannot be attributed to a specific natural person without the use of additional information, provided that the additional information is kept separately and is subject to appropriate technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person. "***Publicly available information"***: information that is lawfully made available from federal, state, or local government records, or widely distributed media or a controller has a reasonable basis to believe has lawfully been made available to the general public. ***"Sensitive data"***: a form of personal data revealing racial or ethnic origin, religious beliefs, mental or physical health condition or diagnosis, sexual orientation, or citizenship or immigration status, the processing of biometric data or genetic information for the purpose of uniquely identifying an individual, the personal data of a known child, or specific geolocation data.
Key Definitions	***"Consent"***: any freely given, specific, informed and unambiguous indication of the consumer's wishes by which the consumer signifies agreement to the processing of personal data relating to the consumer. Acceptance of a general or broad terms of use or similar document that contains descriptions or

	personal data processing along with other, unrelated information does not constitute consent. Hover over, muting, pausing, or closing a given piece of content does not constitute consent. A consent is not valid when the consumer's indication has been obtained by a dark pattern. A consumer may revoke consent previously given. ***"Dark Pattern"***: a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision making, or choice. ***"De-Identified Data"***: data that cannot reasonably be used to infer information about or otherwise be linked to an identified or identifiable natural person or a device linked to an identified or identifiable natural person, provided that the controller that possesses the data: (i) takes reasonable measures to ensure that the data cannot be associated with a natural person (ii) publicly commits to process the data only in a de-identified fashion and not attempt to reidentify the data, and; (iii) contractually obligates any recipients of the information to comply with all provisions regarding de-identified data. ***"Process"***: any operation or set of operations that are performed on personal data or on sets of personal data, whether or not by automated means, including but not limited to the collection, use, storage, disclosure, analysis, deletion or modification of personal data. ***"Targeted Advertising"***: displaying advertisements to a consumer 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 to predict the 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 data to an affiliate of the controller; (d) the disclosure of information that the consumer intentionally made available to the general public via a channel of mass media and did not restrict to a specific audience; (e) the disclosure or transfer of personal data to a third party as an asset that is part of a completed or proposed merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the controller's assets, or; (f) the exchange of personal data between the producer of a good or service and authorized agents of the producer who sell and service the good and services, to enable the cooperative provisioning of goods and services by both the producer and the producer's agents.
Consumer Rights	**Access:** A consumer has the right to confirm whether a controller is processing personal data concerning the consumer and access the categories of personal data the controller is processing. **Affirmative Consent:** A controller shall not process sensitive data concerning a consumer without obtaining the consumer's consent, or, in the case of the processing of personal data concerning a known child, without obtaining consent from the child's parent or lawful guardian, in accordance with COPPA, and its implementing regulations, rules, and exemptions. **Correction:** A consumer has the right to correct inaccurate personal data concerning the consumer, taking into account the nature of the personal data and the purposes of processing the personal data. **Deletion**: A consumer has the right to delete personal data concerning the consumer. **Portability:** A consumer has the right to obtain personal data concerning the consumer, which the consumer previously provided to the controller, in a portable and, to the extent technically feasible,

	readily usable formation that allows the consumer to transmit the data to another controller without hindrance, where the processing is carried out by automated means. **Profiling:** If a consumer's personal data is profiled in furtherance of decisions that produce legal effects concerning consumer or similarly significant effects concerning a consumer, the consumer has the right to question the result of the profiling, to be informed of the reason that the profiling resulted in the decision, and, if feasible, to be informed of what actions the consumer might have taken to secure a different decision and the actions that the consumer might take to secure a different decision in the future. The consumer has the right to review the consumer's personal data used in the profiling. If the decision is determined to have been based upon inaccurate personal data, taking into account the nature of the personal data and the purposes of the processing of the personal data, the consumer has the right to have the data corrected and the profiling decision reevaluated based upon the corrected data. **Opt Out Rights**: A consumer has the right to opt out of the processing or personal data concerning the consumer for purposes of targeted advertising, the sale of personal data, or profiling in furtherance of automated decisions that produce legal effects concerning a consumer or similarly significant effects concerning the consumer. **Revocation:** A controller shall provide an effective mechanism for a consumer, or in the case of the processing of personal data concerning a known child, the child's parent or lawful guardian, to revoke previously given consent. The mechanism provided must be at least as easy as the mechanism by which the consent was previously given. Upon revocation of consent, a controller shall cease to process the applicable data as soon as practicable, but not later than 15 days after the receipt of such request. **Third Parties:** A consumer has a right to obtain a list of the specific third parties to which the controller has disclosed the consumer's personal data. If the controller does not maintain the information in a format specific to the consumer, a list of specific third parties to whom the controller has disclosed any consumer's personal data may be provided instead.
Business Obligations	**Avoid Secondary Use**: A controller may not process personal data for purposes that are not reasonably necessary to, or compatible with, the purposes for which the personal data are processed, as disclosed to the consumer, unless the controller obtains the consumer's consent. **Consumers Between 13 and 16 Years of Age:** A controller may not process the personal data of a consumer for purposes of targeted advertising, or sell the consumer's personal data, without the consumer's consent, under circumstances where the controller knows that the consumer is between the ages of 13 and 16. **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, including the maintenance of an inventory of the data that must be managed to exercise these responsibilities. The data security practices shall be appropriate to the volume and nature of the personal data at issue. **Disclosure**: If a controller sells personal data to third parties, processes personal data for targeted advertising, or engages in profiling in furtherance of decisions that produce legal effects concerning consumer or similarly significant effects concerning a consumer, the controller must disclose the processing in the privacy notice and provide access to a clear and conspicuous method outside the privacy notice for a consumer to opt out of the sale, processing, or profiling in furtherance of decisions that produce legal effects concerning consumer or similarly significant effects concerning a consumer.

	This method may include but is not limited to an internet hyperlink clearly labeled “Your Opt-Out Rights” or “Your Privacy Rights” that directly effectuates the opt-out request or take consumers to a web page where the consumer can make the opt-out request. **No Unlawful Discrimination:** A controller shall not process personal data on the basis of a consumer’s or a class of consumers’ actual or perceived race, color, ethnicity, religion, national origin, sex, gender, gender identity, sexual orientation, familial status, lawful source of income, or disability in a manner that unlawfully discriminates against the consumer or class of consumers with respect to the offering or provision of: housing, employment, credit, or education; or the goods, services, facilities, privileges, advantages, or accommodations of any place of public accommodation. A controller may not discriminate against a consumer for exercising any consumer rights, including denying goods or services to the consumer, charging different prices or rates for goods or services, and providing a different level of quality of goods and services to the consumer. **Purpose Specification:** A controller must limit the collection of personal data to what is adequate, relevant, and reasonably necessary to or compatible with, the purposes for which the personal data are processed, as disclosed to the consumer, unless the controller obtains the consumer’s consent. **Responding to Consumer Requests**: A controller must provide one or more secure and reliable means for consumers to submit a request to exercise the consumer's rights under this section. The means made available must take into account the ways in which consumers interact with the controller and the need for secure and reliable communication of the requests. A controller may not require a consumer to create a new account in order to exercise a right, but a controller may require a consumer to use an existing account to exercise the consumer's rights under this section.A controller must comply with a request to exercise the right as soon as feasibly possible, but no later than 45 days of receipt of the request.A controller must inform a consumer of any action taken on a request without undue delay and in any event within 45 days of receipt of the request. That period may be extended once by 45 additional days where reasonably necessary, taking into account the complexity and number of the requests. The controller must inform the consumer of any extension within 45 days of receipt of the request, together with the reasons for the delay. If a controller does not take action on a consumer's request, the controller must inform the consumer without undue delay and at the latest within 45 days of receipt of the request of the reasons for not taking action and instructions for how to appeal the decision. Information must be provided by the controller free of charge up to twice annually to the consumer. Where requests from a consumer are manifestly unfounded or excessive, in particular because of the repetitive character of the requests, the controller may either charge a reasonable fee to cover the administrative costs of complying with the request, or refuse to act on the request. The controller bears the burden of demonstrating the manifestly unfounded or excessive character of the request. A controller is not required to comply with a request to exercise any of the rights if the controller is unable to authenticate the request using commercially reasonable efforts. In such cases, the controller may request the provision of additional information reasonably necessary to authenticate the request. A controller is not required to authenticate an opt-out request, but a controller may deny an opt-out request if the controller has a good faith, reasonable, and documented belief that the request is fraudulent. If a controller denies an opt-out request because the controller believes a request is fraudulent, the controller must notify the person who made the request that the request was denied due to the controller's belief that the request was fraudulent and state the controller's basis for that belief. A controller must establish an internal process whereby a consumer may appeal a refusal to take action on a request within a reasonable period of time after the consumer's receipt of the notice sent by the controller. The appeal process must be conspicuously available. Within 45 days of receipt of an appeal, a controller must inform the consumer of any action taken or not taken in response to the appeal, along

	with a written explanation of the reasons in support thereof. That period may be extended by 60 additional days where reasonably necessary, taking into account the complexity and number of the requests serving as the basis for the appeal. The controller must inform the consumer of any extension within 45 days of receipt of the appeal, together with the reasons for the delay. When informing a consumer of any action taken or not taken in response to an appeal, the controller must provide a written explanation of the reasons for the controller's decision and clearly and prominently provide the consumer with information about how to file a complaint with the Office of the Attorney General. The controller must maintain records of all appeals and the controller's responses for at least 24 months and shall, upon written request by the attorney general as part of an investigation, compile and provide a copy of the records to the attorney general. **Consumer Request Limitations**: A controller must not disclose certain information about a consumer and instead inform them with sufficient particularity that the controller has collected that type of information. The type of information includes: SSN, driver's license number or other government ID number; financial account number; health insurance account number or medical ID number; account password, security questions, or answers; or biometric data. A controller is also not required to reveal any trade secret in response to a consumer request. **Retention:** A controller may not retain personal data that is no longer relevant and reasonably necessary in relation to the purposes for which the data were collected and processed unless retention of the data is otherwise required by law. **Transparency**: Controllers shall provide consumers with a reasonably accessible, clear, and meaningful privacy notice that includes (i) the categories of personal data processed by the controller; (ii) the purposes for which the categories of personal data are processed; (iii) an explanation of the consumer's rights and how and where consumers may exercise those rights, including how a consumer may appeal a controller's action with regard to the consumer's request; (iv) the categories of personal data that the controller sells or shares with third parties, if any; (v) the categories of third parties, if any, with whom the controller sells or shares personal data; (vi) the controller's contact information, including an active email address or other online mechanism that the consumer may use to contact the controller; (vii) a description of the controller's retention policies for personal data, and; (viii) the date the privacy notice was last updated. Whenever a controller makes a material change to the controller's privacy notice or practices, the controller must notify consumers affected by the material change with respect to any prospectively collected personal data and provide a reasonable opportunity for consumers to withdraw consent to any further materially different collection, processing, or transfer of previously collected personal data under the changed policy. A controller is not required to provide a separate Minnesota-specific privacy notice or section of a privacy notice if the controller's general privacy notice contains all the information required by this section. **Universal Opt-Out Mechanisms:** a controller must recognize a consumer's opt-out preference signals regarding targeted advertising and the sale of their data. The Act is technology agnostic about the type of UOOM but specifies that any platform, technology, or mechanism must adhere to five requirements.
Data Protection Assessments	A controller must document and maintain a description of the policies and procedures the controller has adopted to comply with this chapter. The description must include, where applicable: (1) the name and contact information for the controller's chief privacy officer or other individual with primary responsibility for directing the policies and procedures implemented to comply with the provisions of

	this chapter; and (2) a description of the controller's data privacy policies and procedures which reflect the relevant requirements under the Act. A controller must conduct and document a data privacy and protection assessment for each of the following processing activities involving personal data: (i) the processing of personal data for purposes of targeted advertising; (ii) the sale of personal data; (iii) the processing of sensitive data; (iv) any processing activities involving personal data that present a heightened risk of harm to consumers, and; (v) the processing of personal data for purposes of profiling, where the profiling presents a reasonably foreseeable risk of: (a) unfair or deceptive treatment of, or disparate impact on, consumers; (b) financial, physical, or reputational injury to consumers; (c) a physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of consumers, where the intrusion would be offensive to a reasonable person, or; (d) other substantial injury to consumers. A data privacy and protection assessment must take into account the type of personal data to be processed by the controller, including the extent to which the personal data are sensitive data, and the context in which the personal data are to be processed. A data privacy and protection assessment must identify and weigh the benefits that may flow directly or indirectly from the processing to the controller, consumer, other stakeholders, and the public against the potential risks to the rights of the consumer associate with the processing, as mitigated by safeguards that can be employed by the controller to reduce the potential risks. The use of deidentified data and the reasonable expectations of consumers, as well as the context of the processing and the relationship between the controller and consumer whose personal data will be processed, must be factored into this assessment by the controller. As part of a civil investigative demand, the attorney general may request, in writing, that a controller disclose any data privacy and protection assessment that is relevant to an investigation conducted by the attorney general. The controller must make a data privacy and protection assessment available to the attorney general upon a request. The attorney general may evaluate the data privacy and protection assessments for compliance. Data privacy and protection assessments are classified as nonpublic data. Data privacy and protection assessments or risk assessments conducted by a controller for the purpose of compliance with other laws or regulations may qualify under this section if the assessments have a similar scope and effect.A single data protection assessment may address multiple sets of comparable processing operations that include similar activities.
Controller / Processor Distinction	**Processors are responsible for adhering to the instruction of the controller and assisting the controller to meet the controller's obligations under the Minnesota Consumer Data Privacy Act**, including: (i) taking into account the nature of the processing, the processor shall assist the controller by appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of the controller's obligation to respond to consumer requests to exercise their rights, and; (ii) taking into account the nature of processing and the information available to the processor, the processor shall assist the controller in meeting the controller's obligations in relation to the security of the system and shall provide information to the controller necessary to enable the controller to conduct and document any data privacy and protection assessments required. A contract between a controller and 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 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 shall also require that the processor: (i) ensure that each person processing the personal data is subject to a duty of confidentiality with respect to the data, and; (ii) engage a subcontractor only after providing the controller with an opportunity to object and pursuant to a written contract that requires

	the subcontractor to meet the obligations of the processor with respect to the personal data. Taking into account the context of processing, the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk and establish a clear allocation of the responsibilities between the controller and the processor to implement the technical and organizational measures. Processing by a processor shall be governed by a contract between the controller and the processor that is binding on both parties and that sets out the processing instructions to which the processor is bound, including the nature and purpose of the processing, the type of personal data subject to the processing, the duration of the processing, and the obligations and rights of both parties. The contract shall also include: (i) at the choice of the controller, the processor shall 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; (ii) upon a reasonable request from the controller, the processor shall make available to the controller all information necessary to demonstrate compliance with the obligations in this chapter; and (iii) the processor shall allow for, and contribute to, reasonable assessments and inspections by the controller or the controller's designated assessor. Alternatively, the processor may arrange for a qualified and independent assessor to conduct, at least annually and at the processor's expense, an assessment of the processor's policies and technical and organizational measures in support of the obligations under this chapter. The assessor must use an appropriate and accepted control standard or framework and assessment procedure for assessments as applicable, and shall provide a report of an assessment to the controller upon request.
Exceptions and Exemptions	The obligations imposed on controllers or processors under the Minnesota Consumer Data Privacy Act do not restrict a controller's or a 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, perform a contract to which the consumer is a party, including fulfilling the terms of a written warranty, or take steps at the request of a consumer prior to entering into a contract; (f) protect interests essential for life or physical safety of the consumer or of another natural person; (g) prevent, detect and protect against security incidents, preserve the security of systems, or investigate, report or prosecute those responsible for any such action; (h) assist another controller, processor, or third party with obligations; (i) engage in scientific, historical, or statistical research in the public interest; (j) process personal data for the benefit of the public in the areas of public health, community health, or population health. The Minnesota Consumer Data Privacy Act excludes : protected information under HIPAA, the Health Care Quality Improvement Act of 1986, the Patient Safety and Quality Improvement Act, the Fair Credit Reporting Act, Gramm-Leach-Bliley, the Driver's Privacy Protection Act of 1994, FERPA, the Farm Credit Act, and COPPA.
Enforcement	The Minnesota Consumer Data Privacy Act does not establish a private right of action. **Right to Cure**: In the event that a controller or processor violates this chapter, the attorney general, prior to filing an enforcement action under paragraph (b), must provide the controller or processor with a warning letter identifying the specific provisions of this chapter the attorney general alleges have been or are being violated. If, after 30 days of issuance of the warning letter, the attorney general believes the controller or processor has failed to cure any alleged violation, the attorney general may bring an enforcement action.The right to cure sunsets on January 31, 2026.