State of Minnesota

HOUSE OF REPRESENTATIVES

NINETY-FIRST SESSION

H. F. No. 2917

05/19/2019 Authored by Elkins and Bahner
The bill was read for the first time and referred to the Judiciary Finance and Civil Law Division

A bill for an act

relating to data privacy; requiring controllers to provide, correct, or restrict processing of personal data upon a consumer's request; requiring controllers to provide a privacy notice and document risk assessment; providing for liability and civil penalties; providing the attorney general with enforcement authority; proposing coding for new law in Minnesota Statutes, chapter 325E.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF MINNESOTA:

Section 1. **[325E.75] CONSUMER RIGHTS TO PERSONAL DATA PROCESSING.**

Subdivision 1. **Definitions.** (a) The terms used in this section have the meanings given them.

(b) "Affiliate" means a legal entity that controls, is controlled by, or is under common control with another legal entity.

(c) "Business purpose" means the processing of personal data for the controller's or its processor's operational purposes or other notified purposes, provided the processing of personal data is reasonably necessary and proportionate (i) to achieve the operational purposes for which the personal data was collected or processed, or (ii) for another operational purpose that is compatible with the context in which the personal data was collected. Business purpose includes:

(1) auditing related to a current interaction with the consumer and concurrent transactions, including but not limited to counting ad impressions, verifying positioning and quality of ad impressions, and auditing compliance with this specification and other standards;

(2) detecting security incidents; protecting against malicious, deceptive, fraudulent, or illegal activity; and prosecuting those responsible for the activity;

(3) identifying and repairing errors that impair existing or intended functionality;

(4) short-term, transient use, provided the personal data is not disclosed to another third party and is not used to build a profile about a consumer or otherwise alter an individual consumer's experience outside the current interaction, including but not limited to the contextual customization of ads shown as part of the same interaction;

(5) maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, or providing financing;

(6) undertaking internal research for technological development; or

(7) authenticating a consumer's identity.

(d) "Consent" means a clear, affirmative act, including a written statement, that establishes a specific, informed, and unambiguous indication the consumer agrees to personal data processing relating to the consumer.

(e) "Consumer" means a natural person who is a Minnesota resident. Consumer does not include a business's employee or contractor that is acting in the role of an employee or contractor.

(f) "Controller" means the natural or legal person that alone or jointly with others determines the purposes and means to process personal data.

(g) "Data broker" means a business or unit of business that knowingly collects and sells or licenses to third parties the brokered personal information of a consumer the business does not have a direct relationship with.

(h) "Deidentified data" means:

(1) data that cannot be linked to a known natural person without additional information kept separately; or

(2) data that:

(i) is modified to a degree that the risk of reidentification is small;

(ii) is subject to a controller's public commitment to not attempt to reidentify the data; and

(iii) one or more enforceable controls to prevent reidentification, including legal, administrative, technical, or contractual controls, have been applied to.

(i) "Developer" means a person who creates or modifies the instructions or programs that instruct a computer or device to perform tasks.

(j) "Identified person" or "identifiable person" means a natural person who can be directly or indirectly identified by reference to an identifier.

(k) "Personal data" means any information relating to an identified or identifiable person. Personal data does not include deidentified data.

(l) "Process" or "processing" means any operation or set of operations performed on personal data or on sets of personal data, whether or not by automated means. Process includes collecting, recording, organizing, structuring, storing, adapting or altering, retrieving, consulting, using, disclosing by transmission, disseminating or otherwise making available, aligning or combining, restricting, deleting, or destructing personal data or sets of personal data.

(m) "Processor" means a natural or legal person who processes personal data on behalf of the controller.

(n) "Profiling" means any automated processing of personal data that consists of using personal data to evaluate certain personal aspects relating to a natural person, including analyzing or predicting aspects concerning the natural person's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.

(o) "Restriction of processing" means marking stored personal data to limit the processing of the personal data in the future.

(p) "Sale" means the exchange of personal data for monetary consideration by the controller to a third party to license or sell personal data at the third party's discretion to additional third parties. Sale does not include the following:

(1) the disclosure of personal data to a processor who processes the personal data on behalf of the controller; or

(2) the disclosure of personal data to a third party with whom the consumer has a direct relationship to provide a product or service requested by the consumer or otherwise in a manner that is consistent with a consumer's reasonable expectations considering the context in which the consumer provided the personal data to the controller.

(q) "Sensitive data" means personal data revealing racial or ethnic origin, religious or philosophical beliefs, genetic data, biometric data to uniquely identify a natural person, data concerning a minor, data concerning health, or data concerning a natural person's sex life or sexual orientation.

(r) "Targeted advertising" means displaying advertisements to a consumer where the advertisement is selected based on personal data obtained or inferred over time from a consumer's:

(1) activities across nonaffiliate websites, applications, or online services to predict user preferences or interests; or

(2) visits to a website, application, or online service that a reasonable consumer would not expect to be associated with the publisher, based on lack of common branding, trademarks, or other indicators of common ownership.

Targeted advertising does not include advertising to a consumer in response to the consumer's request for information or feedback.

(s) "Third party" means a natural or legal person, public authority, agency, or body other than a consumer, controller, or an affiliate of the processor or the controller.

Subd. 2. **Application.** (a) This section applies to legal entities that conduct business in Minnesota or produce products or services that are intentionally targeted to residents of Minnesota, provided the legal entity:

(1) controls or processes data of 100,000 consumers or more; or

(2) derives over 50 percent of gross revenue from the sale of personal information, and processes or controls the personal information of 25,000 consumers or more.

(b) This section does not apply to:

(1) government entities, as defined in section 13.02, subdivision 7a;

(2) personal data sets to the extent regulated by sections 144.291 to 144.34, the federal Health Insurance Portability and Accountability Act of 1996, the federal Health Information Technology for Economic and Clinical Health Act of 2009, or the Gramm-Leach-Bliley Act of 1999; or

(3) data sets maintained solely for employment record purposes.

Subd. 3. **Responsibility.** (a) Controllers must meet the obligations under this section.

(b) Processors must adhere to the instructions of the controller and assist the controller to meet its obligations under this section.

(c) Processing by a processor must be governed by a contract between the controller and the processor that is binding on the processor and that establishes the processing instructions the processor is bound to.

Subd. 4. **Consumer rights generally.** (a) Upon a consumer's request, a controller must:

(1) confirm whether personal data concerning the consumer is being processed by the controller;

(2) confirm whether the personal data is sold to data brokers;

(3) provide information regarding where personal data concerning the consumer is being processed by the controller;

(4) provide access to personal data concerning the consumer that the controller maintains in identifiable form;

(5) provide a copy of the personal data that the controller maintains in identifiable form undergoing processing; and

(6) correct inaccurate personal data concerning the consumer that the controller maintains in identifiable form within a reasonable period.

(b) If a consumer requests more than one copy of personal data, the controller may charge a reasonable fee. The fee must be based on administrative costs. If the consumer makes the request by electronic means, and unless otherwise requested by the consumer, the information must be provided in a commonly used electronic form.

(c) A consumer must not be subject to a decision based solely on profiling which produces legal effects concerning such consumer or similarly significantly affects the consumer. Legal or similarly significant effects include but are not limited to denial of consequential services or support for financial and lending services, housing, insurance, education enrollment, criminal justice, employment opportunities, and health care services.

(d) Paragraph (c) does not apply if the decision is:

(1) necessary to enter into or perform a contract between the consumer and a controller;

(2) authorized by federal or state law the controller is subject to and that incorporates suitable measures to safeguard the consumer's rights and legitimate interests, as indicated by the risk assessments required under subdivision 12; or

(3) based on the consumer's consent.

(e) Notwithstanding paragraph (d), the controller must implement suitable measures, including providing human review of the decision, to safeguard the consumer's rights and legitimate interests with respect to decisions based solely on profiling, to express the consumer's point of view with respect to the decision, and to contest the decision.

Subd. 5. **Request for data deletion.** (a) Upon a consumer's request, the controller must delete the consumer's personal data without undue delay if:

(1) the personal data is no longer necessary to the purposes the personal data was collected or otherwise processed for;

(2) the consumer withdraws consent to processing that requires consent under subdivision 12, and there are no other legitimate grounds for the processing;

(3) the consumer objects to the processing under subdivision 8 and (i) no overriding legitimate grounds for the processing exist, or (ii) the processing is for direct marketing purposes;

(4) the personal data has been unlawfully processed; or

(5) the personal data must be deleted to comply with a legal obligation under federal, state, or local law the controller is subject to.

(b) If the controller is required under this section to delete personal data that has been disclosed to third parties by the controller, including data brokers that received the data through a sale, the controller must take reasonable steps, which may include technical measures, to inform other controllers processing the personal data that the consumer has requested the deletion by the other controllers of any links to, or copy or replication of, the personal data. Compliance with this obligation must consider available technology and the cost of implementation.

(c) This subdivision does not apply to the extent processing is necessary to:

(1) exercise the right to free speech;

(2) comply with a legal obligation that requires processing by federal, state, or local law the controller is subject to, or perform a task carried out in the public interest or in the exercise of official authority vested in the controller;

(3) support the public interest in the area of public health, provided the processing is (i) subject to suitable and specific measures that safeguard the rights of the consumer, and (ii) processed by or under the responsibility of a professional subject to confidentiality obligations under federal, state, or local law;

(4) archive for purposes in the public interest, scientific or historical research purposes, or statistical purposes, if the deletion of the personal data is likely to render impossible or seriously impair achievement of the processing's objectives; or

(5) establish, exercise, or defend a legal claim.

Subd. 6. **Request to restrict processing.** (a) Upon a consumer's request, the controller must restrict processing if:

(1) the consumer contests the accuracy of the personal data. The controller may restrict processing for the period of time needed for the controller to verify the accuracy of the personal data;

(2) the processing is unlawful, and the consumer opposes the deletion of the personal data and requests that processing is restricted instead;

(3) the controller no longer needs the personal data for processing, but the personal data is required by the consumer to establish, exercise, or defend a legal claim; or

(4) the consumer objects to processing under subdivision 8, pending verification of whether the legitimate grounds of the controller override the consumer's objection.

(b) If personal data is subject to a processing restriction under this subdivision, the personal data must, with the exception of storage, be processed only:

(1) with the consumer's consent;

(2) to establish, exercise, or defend a legal claim;

(3) to protect the rights of another natural or legal person; or

(4) for reasons of important public interest under federal, state, or local law.

(c) If a consumer obtains a processing restriction under this subdivision, the controller must inform the consumer before lifting the processing restriction.

Subd. 7. **Request for personal data.** (a) Upon a consumer's request, the controller must provide the consumer in a structured, commonly used, and machine-readable format any personal data concerning the consumer that the controller maintains and that the consumer has provided to the controller if:

(1) processing the personal data requires consent under subdivision 12, processing the personal data is necessary for the performance of a contract the consumer is a party to, or at the request of the consumer prior to entering into a contract; and

(2) the processing is carried out by automated means.

(b) Controllers must transmit the personal data requested under this subdivision (1) directly from one controller to another where technically feasible, and (2) to another controller without hindrance from the controller the personal data was provided to.

(c) Requests for personal data under this subdivision must be without prejudice to subdivision 5.

(d) The rights provided under this subdivision do not apply to processing necessary to perform a task carried out in the public interest or in the exercise of official authority vested in the controller, and must not adversely affect the rights of others.

Subd. 8. **Objection to processing.** A consumer may object at any time, on grounds relating to the consumer's particular situation, to processing personal data concerning the consumer. When a consumer objects to targeted advertising, which includes the sale of personal data concerning the consumer to third parties for direct targeted advertising, the controller is prohibited from processing the personal data subject to the objection for direct targeted advertising and must communicate the consumer's objection regarding any further processing of the consumer's personal data to any third parties to whom the controller sold the consumer's personal data for direct targeted advertising unless communication proves impossible or involves disproportionate effort. Third parties must honor objection requests under this subdivision received from third-party controllers. If a consumer objects to processing for any purpose other than targeted advertising, the controller may continue processing the personal data subject to the objection if the controller demonstrates a compelling legitimate ground to process the personal data.

Subd. 9. **Third parties.** A controller must communicate any correction, deletion, or restriction of processing carried out under this section to each third-party recipient, including third parties that received the data through a sale, the personal data has been disclosed to unless communication proves impossible or involves disproportionate effort. The controller must inform the consumer about third-party recipients, if any, that have received the consumer's personal data if the consumer requests the information.

Subd. 10. **Timely action.** (a) A controller must provide information on action taken in response to a consumer request under this section within 30 days of the date the request is received. That period may be extended for 60 additional days if necessary due to the complexity and number of the requests. The controller must inform the consumer of the extension and the reasons for the delay within 30 days of the date the request is received. If the consumer makes the request by electronic means, the information must be provided by electronic means if possible or unless otherwise requested by the consumer.

(b) If a controller does not take action on a consumer's request, the controller must inform the consumer within 30 days of the date the request is received of the reasons for not taking action and any possibility for internal review of the controller's decision.

(c) Information provided under this section must be provided by the controller free of charge to the consumer. If a request from a consumer is manifestly unfounded, excessive, or repetitive, the controller may:

(1) charge a reasonable fee based on the administrative costs to provide the information or communication or take the action requested; or

(2) refuse to act on the request.

The controller bears the burden of demonstrating that the request is manifestly unfounded or excessive.

(d) If the controller has reasonable doubts concerning the identity of the consumer making a request under this section, the controller may request that the consumer provide additional information necessary to confirm the consumer's identity.

Subd. 11. **Notice.** (a) Controllers must make available, in a form that is reasonably accessible to consumers, a clear privacy notice that includes:

(1) the categories of personal data the controller collects;

(2) the purposes the categories of personal data are used and disclosed to third parties for, if any;

(3) the rights consumers may exercise under this section;

(4) the categories of personal data the controller shares with third parties, if any; and

(5) the categories of third parties, if any, the controller shares personal data with.

(b) Controllers that engage in profiling must disclose the profiling to the consumer at or before the time personal data is obtained. The disclosure must include information regarding the logic involved, and the significance and potential consequences of the profiling.

(c) If a controller sells personal data to data brokers or processes personal data for targeted advertising, it must disclose in a clear and prominent manner the processing and the manner in which a consumer may exercise the right to object to the processing.

Subd. 12. **Risk assessment.** (a) Controllers must conduct risk assessments of each processing activity the controller engages in that involves personal data, and must conduct an additional risk assessment any time a change in processing occurs that materially increases the risk to consumers. Risk assessments must consider the type of personal data processed by the controller, including the extent to which the personal data is sensitive data or otherwise sensitive in nature, and the context in which the personal data is processed.

(b) Risk assessments must identify and weigh the benefits that may flow directly and indirectly to the controller, consumer, other stakeholders, and the public from the processing against the potential risks, as mitigated by safeguards that can be employed by the controller to reduce the risks, to the rights of the consumer associated with the processing. The use of deidentified data and the reasonable expectations of consumers must be included in the controller's assessment.

(c) If the risk assessment determines that the potential risks to the rights of the consumer in processing the personal data of the consumer outweigh the interests of the controller, consumer, other stakeholders, and the public, the controller may engage in processing only if the consumer provides consent. Consent must be as easy to withdraw as it is to provide.

(d) Processing for a business purpose is presumed permissible unless:

(1) it involves processing sensitive data; and

(2) the risk of processing cannot be reduced through the use of appropriate administrative and technical safeguards.

(e) The controller must make the risk assessment available to the attorney general upon request. Risk assessments are nonpublic data, as defined in section 13.02, subdivision 9.

Subd. 13. **Deidentified data.** A controller or processor that uses deidentified data must exercise reasonable oversight to monitor compliance with any contractual commitments the deidentified data is subject to, and must take appropriate steps to address any breach of a contractual commitment.

Subd. 14. **Exemptions.** (a) The obligations imposed on controllers or processors under this section do not restrict a controller's or processor's ability to:

(1) comply with federal, state, or local laws;

(2) comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, local, or other governmental authorities;

(3) cooperate with law enforcement agencies concerning conduct or activity that the controller or processor reasonably and in good faith believes may violate federal, state, or local law;

(4) investigate, exercise, or defend legal claims; or

(5) prevent or detect identity theft, fraud, or other criminal activity.

(b) A controller or processor that discloses personal data to a third-party controller or processor in compliance with this section does not violate this section if the third-party

recipient processes the personal data in violation of this section, provided that, at the time the personal data was disclosed, the disclosing controller or processor did not have actual knowledge that the third-party recipient intended to commit a violation. A third-party recipient that receives personal data from a controller or processor is not liable under this section for the obligations of a controller or processor it provides services to.

(c) This section does not require a controller or processor to:

(1) reidentify deidentified data;

(2) retain personal data concerning a consumer that it would not otherwise retain in the ordinary course of business; or

(3) comply with a request to exercise under this section if the controller is unable to verify, using commercially reasonable efforts, the identity of the consumer making the request.

(d) Obligations imposed on controllers and processors under this section do not:

(1) adversely affect the rights of any person;

(2) apply to processing personal data by a natural person in the course of a personal or household activity;

(3) apply if compliance by the controller or processor would violate an evidentiary privilege; or

(4) prevent a controller or processor from providing personal data concerning a consumer to a person covered by an evidentiary privilege as part of a privileged communication.

Subd. 15. **Liability.** (a) If more than one controller or processor, or both a controller and a processor, involved in the same processing violates this section, liability must be allocated among the parties on a comparative fault basis unless the liability is otherwise allocated in a contract between the parties.

(b) A controller or processor violates this section if the controller or processor fails to cure any alleged breach of this section within 30 days of the date notice of alleged noncompliance is received. A controller or processor that violates this section is subject to a civil penalty of not more than $2,500 for each violation or $7,500 for each intentional violation.

Subd. 16. **Enforcement.** The attorney general may enforce this section under section 8.31. The attorney general may recover costs and disbursements, including costs of

investigation and reasonable attorney fees. Nothing in this section serves as the basis for a private right of action.

EFFECTIVE DATE. This section is effective December 31, 2020.