325M.18 DATA PRIVACY POLICIES; DATA PRIVACY AND PROTECTION ASSESSMENTS.

(a) A controller must document and maintain a description of the policies and procedures the controller has adopted to comply with sections 325M.10 to 325M.21. 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 sections 325M.10 to 325M.21; and

(2) a description of the controller's data privacy policies and procedures which reflect the requirements in section 325M.16, and any policies and procedures designed to:

(i) reflect the requirements of sections 325M.10 to 325M.21 in the design of the controller's systems;

(ii) identify and provide personal data to a consumer as required by sections 325M.10 to 325M.21;

(iii) 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 the responsibilities under this item;

(iv) limit the collection of personal data to what is adequate, relevant, and reasonably necessary in relation to the purposes for which the data are processed;

(v) prevent the retention of 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 or permitted under section 325M.19; and

(vi) identify and remediate violations of sections 325M.10 to 325M.21.

(b) A controller must conduct and document a data privacy and protection assessment for each of the following processing activities involving personal data:

(1) the processing of personal data for purposes of targeted advertising;

(2) the sale of personal data;

(3) the processing of sensitive data;

(4) any processing activities involving personal data that present a heightened risk of harm to consumers; and

(5) the processing of personal data for purposes of profiling, where the profiling presents a reasonably foreseeable risk of:

(i) unfair or deceptive treatment of, or disparate impact on, consumers;

(ii) financial, physical, or reputational injury to consumers;

(iii) 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

(iv) other substantial injury to consumers.

(c) 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.

(d) A data privacy and protection assessment must identify and weigh the benefits that may flow directly and indirectly from the processing to the controller, consumer, other stakeholders, and the public against the potential risks to the rights of the consumer associated 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 the consumer whose personal data will be processed, must be factored into this assessment by the controller.

(e) A data privacy and protection assessment must include the description of policies and procedures required by paragraph (a).

(f) 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 made under this paragraph. The attorney general may evaluate the data privacy and protection assessments for compliance with sections 325M.10 to 325M.21. Data privacy and protection assessments are classified as nonpublic data, as defined by section 13.02, subdivision 9. The disclosure of a data privacy and protection assessment pursuant to a request from the attorney general under this paragraph does not constitute a waiver of the attorney-client privilege or work product protection with respect to the assessment and any information contained in the assessment.

(g) 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.

(h) A single data protection assessment may address multiple sets of comparable processing operations that include similar activities.

History: *2024 c 121 art 5 s 10*

NOTE: Postsecondary institutions regulated by the Office of Higher Education are not required to comply with this section until July 31, 2029. Laws 2024, chapter 121, article 5, section 14.