325M.13 RESPONSIBILITY ACCORDING TO ROLE.

(a) Controllers and processors are responsible for meeting the respective obligations established under sections 325M.10 to 325M.21.

(b) Processors are responsible under sections 325M.10 to 325M.21 for adhering to the instructions of the controller and assisting the controller to meet the controller's obligations under sections 325M.10 to 325M.21. Assistance under this paragraph shall include the following:

(1) 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 pursuant to section 325M.14; and

(2) 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 processing the personal data and in relation to the notification of a breach of the security of the system pursuant to section 325E.61, and shall provide information to the controller necessary to enable the controller to conduct and document any data privacy and protection assessments required by section 325M.18.

(c) 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 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:

(1) ensure that each person processing the personal data is subject to a duty of confidentiality with respect to the data; and

(2) engage a subcontractor only (i) after providing the controller with an opportunity to object, and (ii) pursuant to a written contract in accordance with paragraph (e) that requires the subcontractor to meet the obligations of the processor with respect to the personal data.

(d) 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.

(e) 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 include the requirements imposed by this paragraph, paragraphs (c) and (d), as well as the following requirements:

(1) 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;

(2) 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 sections 325M.10 to 325M.21; and

(3) 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 sections 325M.10 to 325M.21. 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.

(f) In no event shall any contract relieve a controller or a processor from the liabilities imposed on a controller or processor by virtue of the controller's or processor's roles in the processing relationship under sections 325M.10 to 325M.21.

(g) Determining whether a person is acting as a controller or processor with respect to a specific processing of data is a fact-based determination that depends upon the context in which personal data are to be processed. A person that is not limited in the person's processing of personal data pursuant to a controller's instructions, or that fails to adhere to a controller's instructions, is a controller and not a processor with respect to a specific processing of data. A processor that continues to adhere to a controller's instructions with respect to a specific processing of personal data remains a processor. If a processor begins, alone or jointly with others, determining the purposes and means of the processing of personal data, the processor is a controller with respect to the processing.

History: *2024 c 121 art 5 s 5*

NOTE: This section, as added by Laws 2024, chapter 121, article 5, section 5, is effective July 31, 2025, except that postsecondary institutions regulated by the Office of Higher Education are not required to comply until July 31, 2029. Laws 2024, chapter 121, article 5, section 14.