325M.19 LIMITATIONS AND APPLICABILITY.

(a) The obligations imposed on controllers or processors under sections 325M.10 to 325M.21 do not restrict a controller's or a processor's ability to:

(1) comply with federal, state, or local laws, rules, or regulations, including but not limited to data retention requirements in state or federal law notwithstanding a consumer's request to delete personal data;

(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 laws, rules, or regulations;

(4) investigate, establish, exercise, prepare for, or defend legal claims;

(5) provide a product or service specifically 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 the consumer prior to entering into a contract;

(6) take immediate steps to protect an interest that is essential for the life or physical safety of the consumer or of another natural person, and where the processing cannot be manifestly based on another legal basis;

(7) 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 such action;

(8) assist another controller, processor, or third party with any of the obligations under this paragraph;

(9) engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws and is approved, monitored, and governed by an institutional review board, human subjects research ethics review board, or a similar independent oversight entity that has determined:

(i) the research is likely to provide substantial benefits that do not exclusively accrue to the controller;

(ii) the expected benefits of the research outweigh the privacy risks; and

(iii) the controller has implemented reasonable safeguards to mitigate privacy risks associated with research, including any risks associated with reidentification; or

(10) process personal data for the benefit of the public in the areas of public health, community health, or population health, but only to the extent that the processing is:

(i) subject to suitable and specific measures to safeguard the rights of the consumer whose personal data is being processed; and

(ii) under the responsibility of a professional individual who is subject to confidentiality obligations under federal, state, or local law.

(b) The obligations imposed on controllers or processors under sections 325M.10 to 325M.21 do not restrict a controller's or processor's ability to collect, use, or retain data to:

(1) effectuate a product recall or identify and repair technical errors that impair existing or intended functionality;

(2) perform internal operations that are reasonably aligned with the expectations of the consumer based on the consumer's existing relationship with the controller, or are otherwise compatible with processing in furtherance of the provision of a product or service specifically requested by a consumer or the performance of a contract to which the consumer is a party; or

(3) conduct internal research to develop, improve, or repair products, services, or technology.

(c) The obligations imposed on controllers or processors under sections 325M.10 to 325M.21 do not apply where compliance by the controller or processor with sections 325M.10 to 325M.21 would violate an evidentiary privilege under Minnesota law and do not prevent a controller or processor from providing personal data concerning a consumer to a person covered by an evidentiary privilege under Minnesota law as part of a privileged communication.

(d) A controller or processor that discloses personal data to a third-party controller or processor in compliance with the requirements of sections 325M.10 to 325M.21 is not in violation of sections 325M.10 to 325M.21 if the recipient processes the personal data in violation of sections 325M.10 to 325M.21, provided that at the time of disclosing the personal data, the disclosing controller or processor did not have actual knowledge that the recipient intended to commit a violation. A third-party controller or processor receiving personal data from a controller or processor in compliance with the requirements of sections 325M.10 to 325M.21 is not in violation of sections 325M.10 to 325M.21 for the obligations of the controller or processor from which the third-party controller or processor receives the personal data.

(e) Obligations imposed on controllers and processors under sections 325M.10 to 325M.21 shall not:

(1) adversely affect the rights or freedoms of any persons, including exercising the right of free speech pursuant to the First Amendment of the United States Constitution; or

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

(f) Personal data that are processed by a controller pursuant to this section may be processed solely to the extent that the processing is:

(1) necessary, reasonable, and proportionate to the purposes listed in this section;

(2) adequate, relevant, and limited to what is necessary in relation to the specific purpose or purposes listed in this section; and

(3) insofar as possible, taking into account the nature and purpose of processing the personal data, subjected to reasonable administrative, technical, and physical measures to protect the confidentiality, integrity, and accessibility of the personal data, and to reduce reasonably foreseeable risks of harm to consumers.

(g) If a controller processes personal data pursuant to an exemption in this section, the controller bears the burden of demonstrating that the processing qualifies for the exemption and complies with the requirements in paragraph (f).

(h) Processing personal data solely for the purposes expressly identified in paragraph (a), clauses (1) to (7), does not, by itself, make an entity a controller with respect to the processing.

History: *2024 c 121 art 5 s 11*

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.