



May 2, 2022

Dear Senator Mathews,

Thank you for your time and consideration of clarifying amendments to the current language in S.F. 2307 which will assist with compliance as well as strengthen the privacy protections.

SIIA is the principal trade association for the software information and digital content industry. A number of our member companies partner with schools and the state to provide educational services for in class and online learning, as well as to support general school operations.. Additionally, a number of our member companies have employees based in Minnesota building products that are reflective of the dedication, thoughtfulness, and hard work of your constituents.

We request consideration of the following three changes to the current text. The explanation is followed by suggested language.

#### **Amendment 1**

Lines 3.16-3.23 require a technology provider to establish written procedures to ensure appropriate security safeguards. We support the spirit of this language but are concerned that this would provide a roadmap for bad actors instead of holding technology companies responsible for protecting student data. In addition, it potentially deprives schools of their right and obligation to communicate how they would like their student personal information to be protected, leaving it up to the discretion of the vendor. The amendment below would require a contract between a school and a technology provider to include requirements to ensure appropriate safeguards.

Under the regulations for the federal student privacy law, the Family Educational Rights and Privacy Act (FERPA), the U.S. Department of Education may ban a school from using a company that improperly re-discloses education records for no less than five years (34 CFR § 99.67). Requiring this language to be in a contract between a school and a technology provider would align enforcement under Minnesota's law with federal law and make enforcement more clear cut. This is reflected in the amendment below. In addition, the amendment also deletes the last sentence which is redundant because the contracts are already available for inspection.

Lines 3.16-3.23

(g) The contract between a technology provider and a school must include requirements to A technology provider must establish written procedures to

ensure appropriate security safeguards for educational data. ~~Such a contract must require that:~~ These procedures must require that:

- (1) the technology provider's employees or contractors have access to educational data only if authorized; and
- (2) the technology provider's employees or contractors may be authorized to access educational data only if access is necessary to fulfill the official duties of the employee or contractor.

~~These written procedures are public data.~~

## **Amendment 2**

We also propose to amend lines 3.5-3.8 to remove an ambiguous phrase – “unless renewal of the contract is reasonably anticipated” – and require that contracts outline the timeline for deletion or return of data. We believe this amendment would help to ensure compliance with state and local record retention policies<sup>1</sup>.

Lines 3.5-3.8

~~As outlined in the contract or~~ Unless renewal of the contract is reasonably anticipated, within 30 days of the expiration of the contract, a technology provider must destroy or return to the appropriate public educational agency or institution all educational data created, received, or maintained pursuant or incidental to the contract.

## **Amendment 3**

We propose to amend lines 3.14-3.15 to clarify the term “commercial purpose” in the legislation.

First, we urge a clarification that would allow a business to only use deidentified, aggregate information for analysis of crash reporting and bug fixing and to monitor for activity that may be either an external threat (e.g., a hacker) or may indicate exploitation of a security vulnerability. The language proposed below would enable businesses to use deidentified, aggregate information for this limited purpose.

Second, we are concerned that the provision in 3.14-3.15 placing restrictions on the use of educational data for a “commercial purpose” might prohibit a school from paying a technology provider for a service to carry out school operations or

---

<sup>1</sup> <https://education.mn.gov/mdeprod/groups/educ/documents/basic/mdaw/mdu1/~edisp/055464.pdf>

instruction. For example, a software program for school bus routes may need access to the names and addresses of a student to determine the school bus route. The language outlined below would clarify that a school may contract for such services from a technology provider but those services would need to be outlined in the contract and would ban marketing or advertising to a student or parent.

Lines 3:14-3:15

(f) A technology provider must not use educational data for any commercial purpose beyond the services the technology provider has contracted to provide the public educational agency or institution, including but not limited to marketing or advertising to a student or parent. Nothing in this subdivision prohibits the operator's use of deidentified, aggregate information for maintaining, developing, supporting, improving, or diagnosing the operator's site, service, or application."

Thank you for your time and consideration of this matter. Please contact me with any additional questions at [skloek@siia.net](mailto:skloek@siia.net) or at 651-324-3127.

Thank you,

Sara Kloek, CIPP/US  
Senior Director, Education Policy  
SIIA