Recent Updates to the Minnesota Government Data Practices Act

Stephen M. Knutson & Katharine M. Saphner
Knutson, Flynn & Deans, P.A.

Craig Oftedahl
Independent School District No. 2184 (Luverne Public Schools)

Overview of MGDPA

- Government data is defined as: “all data collected, created, received, maintained or disseminated by any government entity regardless of its physical form, storage media or conditions of use.”
- Members of the public are able to access public data by making a data request to a government entity’s responsible authority.
- Government data is presumed public unless there is a statutory provision that states it is private, not public, or confidential.
- Two of the most common protected categories that come up in the school setting are personnel data (Minnesota Statutes 13.43) and educational data (Minnesota Statutes 13.32), which are generally private, with enumerated exceptions.
  - Accordingly, there is essentially a presumption that personnel and educational data are NOT public.

Outline of New Provisions Applicable to School Districts

- Educational Data (Minn. Stat. 13.32):
  - New Definitions of Parent, Technology Provider, and School-Issued Device
  - New restrictions and responsibilities for Technology Providers
  - New restrictions on searches of School-Issued Devices
- New Provision on Educational Support Services Data
  - Minn. Stat. 13.463
- New Advisory Opinion on timing of data responses
  - Advisory Opinion 22-001

Educational Data: New Definitions

- Parent:
  - “Parent” means a parent of a student and includes a natural parent, a guardian, or an individual acting as a parent in the absence of a parent or a guardian.
- School-issued device:
  - “School-issued device” means hardware or software that a public educational agency or institution, acting independently or with a technology provider, provides to an individual student for that student's dedicated personal use. A school-issued device includes a device issued through a one-to-one program.
- Technology provider: means a person who
  - (1) contracts with a public educational agency or institution, as part of a one-to-one program or otherwise, to provide a school-issued device for student use; and
  - (2) creates, receives, or maintains educational data pursuant or incidental to a contract with a public educational agency or institution.

Educational Data: Restrictions on Technology Providers

Subdivision 13 (a):

A technology provider is subject to the provisions of section 13.05, subdivision 11.

- This provision states that if a government entity enters into a contract with a private person to perform any of its functions, all of the data created, collected, received, stored, used, maintained or disseminated by the private person while performing those functions are subject to the Data Practices Act.
- Contracts entered into under this provision must include a notice that the requirements of this subdivision apply.
  - If the contract does not contain the provision, the data is nevertheless subject to the Data Practices Act.

This is a mutual responsibility of the School and the Technology Provider.

Educational Data:
Restrictions on Technology Providers

Subdivision 13 (b):

All educational data created, received, maintained, or disseminated by a technology provider pursuant or incidental to a contract with a public educational agency or institution are not the technology provider's property.

This is a limitation on the Technology Provider.

Educational Data: Restrictions on Technology Providers

Subdivision 13 (c):

If educational data maintained by the technology provider are subject to a breach of the security of the data, the technology provider must, following discovery of the breach, disclose to the public educational agency or institution all information necessary to fulfill the requirements of section 13.055.

- Section 13.055 requires government entities to:
  - Provide notice to individuals of breaches of data regarding those individuals
  - Prepare a report describing the facts and results of the investigation

This is a responsibility of the Technology Provider.

Educational Data:
Restrictions on Technology Providers

Subdivision 13 (d):

Unless renewal of the contract is reasonably anticipated, within 90 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.

This is a responsibility of the Technology Provider.

Educational Data:
Restrictions on Technology Providers

Subdivision 13 (e):

A technology provider must not sell, share, or disseminate educational data, except as provided by this section or as part of a valid delegation or assignment of its contract with a public educational agency or institution. An assignee or delegee that creates, receives, or maintains educational data is subject to the same restrictions and obligations under this section as the technology provider.

This is a responsibility of the Technology Provider.

Educational Data:
Restrictions on Technology Providers

Subdivision 13 (f):

A technology provider must not use educational data for any commercial purpose, including but not limited to marketing or advertising to a student or parent. For purposes of this paragraph, a commercial purpose does not include providing the specific services contracted for by a public educational agency or institution. Nothing in this subdivision prohibits the operator's use of deidentified, aggregate information for improving, maintaining, developing, supporting, or diagnosing the operator's site, service, or operation.

This is a responsibility of the Technology Provider.

Educational Data: Restrictions on Technology Providers

Subdivision 13(g):

A contract between a technology provider and a public educational agency or institution must include requirements to ensure appropriate security safeguards for educational data. The contract 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.

This is a mutual responsibility of the School and the Technology Provider.

Educational Data: Restrictions on Technology Providers

(h) Within 30 days of the start of each school year, a public educational agency or institution must give parents and students direct and timely notice, by United States mail, email, or other direct form of communication, of any curriculum, testing, or assessment technology provider contract affecting a student's educational data. The notice must:

- (1) identify each curriculum, testing, or assessment technology provider with access to educational data;
- (2) identify the educational data affected by the curriculum, testing, or assessment technology provider contract; and
- (3) include information about the contract inspection and provide contact information for a school department to which a parent or student may direct questions or concerns regarding any program or activity that allows a curriculum, testing, or assessment technology provider to access a student's educational data.

This is a responsibility of the School.

Educational Data:
Restrictions on Technology Providers

Subdivision 13(i):

A public educational agency or institution must provide parents and students an opportunity to inspect a complete copy of any contract with a technology provider.

This is a responsibility of the School.

Practical takeaway: Locate, save, and print a copy of all contracts with technology provider as soon as they are entered into and keep a physical copy on hand.

Educational Data:
Restrictions on School-Issued Devices

Subdivision 14 (a):

Except as provided in paragraph (b), a government entity or technology provider must not electronically access or monitor:

(1) any location-tracking feature of a school-issued device;

(2) any audio or visual receiving, transmitting, or recording feature of a school-issued device; or

(3) student interactions with a school-issued device, including but not limited to keystrokes and web-browsing activity.

Educational Data:
Restrictions on School-Issued Devices

Subdivision 14 (b):

A government entity or technology provider may only engage in activities prohibited by paragraph (a) if:

- (1) the activity is limited to a noncommercial educational purpose for instruction, technical support, or exam-proctoring by district employees, student teachers, staff contracted by a district, a vendor, or the Department of Education, and notice is provided in advance;
- (2) the activity is permitted under a judicial warrant;
- (3) the public educational agency or institution is notified or becomes aware that the device is missing or stolen;
- (4) the activity is necessary to respond to an imminent threat to life or safety and the access is limited to that purpose;
- (5) the activity is necessary to comply with federal or state law, including but not limited to section 121A.031 (bullying); or
- (6) the activity is necessary to participate in federal or state funding programs, including but not limited to the E-Rate program.

Educational Data:
Restrictions on School-Issued Devices

Subdivision 14 (c):

- If a government entity or technology provider interacts with a school-issued device as provided in paragraph (b), clause (4) (imminent threat to life or safety), it must, within 72 hours of the access, notify the student to whom the school-issued device was issued or that student's parent and provide a written description of the interaction, including which features of the device were accessed and a description of the threat. This notice is not required at any time when the notice itself would pose an imminent threat to life or safety, but must instead be given within 72 hours after that imminent threat has ceased.

Other Issues with Cloud-Based Storage

- Some School Districts use cloud-based storage (e.g. Google Drive)
- If sensitive material that could violate child pornography laws is located in the cloud, there is an open question as to whether that constitutes “possession”
  - Out of an abundance of caution, we recommend contacting law enforcement and notifying this if this issues arise
  - Make sure the School District knows how to remove sensitive material from the cloud, but do so only after contacting law enforcement

Education Support Services Data

- New Statute: Section 13.463
- “Education support services data” means data on individuals collected, created, maintained, used, or disseminated relating to programs administered by a government entity or entity under contract with a government entity designed to eliminate disparities and advance equities in educational achievement for youth by coordinating services available to participants, regardless of the youth's involvement with other government services.
  - Education support services data does not include welfare data under section 13.46.
- Unless otherwise provided by law, all education support services data are private data on individuals and must not be disclosed except according to section 13.05 or a court order.

Advisory Opinion 22-001

- On November 5, 2021, a data requester requested all data on himself in the possession of a specific government entity “from the beginning of time.”
- The government entity responded on November 22, the tenth non-weekend day since the request, and offered future dates at which he could view the data. The data requester noted that he was entitled to view it on November 22, as it was the tenth day.
- At 3pm on November 22, the entity offered to allow him to access the data at 4pm on that date. He refused to do so and eventually reviewed the data in December 2021.
- The Commissioner determined this response violated the Data Practices Act’s requirement to allow access to data on oneself within 10 days.

Advisory Opinion 22-001

“Based on the plain language of the law, the 10-day deadline is strict and does not provide exceptions for mitigating circumstances despite the challenges it may pose for small government entities that must search through a substantial amount of electronic and digital data.”

“Although it may have been possible for [the requester] to inspect data on November 22, a meaningful opportunity to inspect data by the expiration of the 10-day deadline was extremely limited. The Commissioner does not believe that [the government entity’s] same-day offer that [the requester] could inspect responsive data from 4 p.m. to 5 p.m. on November 22 reasonably met the requirements of section 13.04, subdivision 3 when considering the totality of the facts and the strict requirements of the law.”

Advisory Opinion 22-001

The entity asserted that some of the delay was due to safety concerns with respect to the requester. (The entity wanted law enforcement present during the inspection of the data.) The Commissioner noted that the entity had discretion to approach the access of data by the requester in that manner, but nevertheless violated the Data Practices Act due to the timing of the access.

Takeaway: Schools should provide advance notice as to times that data can be reviewed within the 10-day period.

Questions?

Stephen M. Knutson

651-225-0626

sknutson@kfdmn.com

Katharine Saphner

651-225-0645

ksaphner@kfdmn.com