December 2023

Office of General Counsel

Advanced MGDPA Overview

Daniel McCabe
Assistant General Counsel

Part One: The Responsible Authority

Responsible Authorities

- The individual on campus responsible for MGDPA compliance.
- By default, this person is the President.
- The President may further delegate the duties of the Responsible Authority as they see fit.

Duties of the Responsible Authority

- Set forth in various sections of the Minnesota Government Data Practices Act, Minnesota Statutes Chapter 13.
- The next slides summarize some examples of these responsibilities, but this list is not exhaustive.

Data Protection

- Establish procedures to assure that all data on individuals is accurate, complete, and current for the purposes for which it was collected;
- Establish appropriate security safeguards for all records containing data on individuals, including procedures for ensuring that data that are not public are only accessible to persons whose work assignment reasonably requires access to the data, and is only being accessed by those persons for purposes described in the procedure; and
- Develop a policy incorporating these procedures, which may include a model policy governing access to the data if sharing of the data with other government entities is authorized by law.
- When not public data is being disposed of, the data must be destroyed in a way that prevents its contents from being determined.

Data Inventory

- The responsible authority shall prepare an inventory containing the authority's name, title, address, and a description of each category of record, file, or process relating to private or confidential data on individuals maintained by the authority's government entity. Forms used to collect private and confidential data may be included in the inventory. The responsible authority shall update the inventory annually and make any changes necessary to maintain the accuracy of the inventory. The inventory must be available from the responsible authority to the public.

Data Access Policies

- Responsible Authority must create a written data access policy available to members of the public.
- The policy must detail how data subjects and members of the public can access government data.
- The policy must be readily available. The best practice is to post it on your campus' website.

Part Two: The DPCO

Delegations of Authority

- Presidents may delegate duties to a DPCO.
- By default, only responsible for responding to data requests and answering question from the public about data requests.
- The DPCO role does not carry over with position description. It must be delegated by the President.
- Our Office has delegation forms available on our website: (https://www.minnstate.edu/system/ogc/dataprivacy/index.html).

Who is My DPCO?

- Our office maintains a list.
- We rely on the campuses to keep this list up to date.
- If the list is inaccurate for the campus, please contact our office.

Who Should be DPCO?

- The President makes this determination.
- Often, Registrar for student data, CHRO for other data (including personnel data).
- The “main” DPCO should be a person high in the College or University’s reporting structure. Preferably a cabinet member.

Additional DCPO Duties

- Some campuses may choose to delegate other duties besides answering data requests and answering questions about access to data.
- Presidents can delegate any Responsible Authority duties to the DPCO.
- If you are have questions about delegations, reach out to OGC.

Response Time and Multiple Requests

- Keep in mind that only Data Practices Compliance Officials are responsible for fulfilling data requests.
- If someone is asking for their own data – 10 business days.
- Otherwise, we have a “reasonable” time to respond.
- A data subject cannot ask for the same data twice in a six month period.
- A member of the public who is not the data subject can ask for data as many times as they want.
- These restrictions still exist despite the status of our operations.

Asking for More Information

- We cannot:
  - Ask for data requestor why they are asking for data
  - Ask data requestor to identify themselves, unless they are asking for data on themselves
- We can:
  - Ask to clarify a request
  - Ask for requests to be in writing
  - Ask a data requestor for identification if they are asking for data on themselves
  - Ask if a data requestor is a credit card issuer

Identity Verification

- Persons are entitled to government data on themselves in most circumstances.
- However, we have to verify that someone is who they say they are when they ask for “data on themselves.”
- Reasonable procedures include making the person come to an office and present photo identification or using a verifiable portal such as “Move-It Securely” or D2L.
- In person verification is not currently an option, so we should consider how we remote verify.

Valid Releases

- Must be signed and dated by data subject.
  - Must sufficiently describe the information to be released and to whom it is to be released to.
  - May be a category such as “future employers” but specific names preferred.
  - Fax copy ok but e-mail alone is not.
  - Requests for data authorized by the data subject must be fulfilled within ten (10) business days. This is the same timeline as if the request came from the data subject themselves.

Part Three: Miscellaneous Advanced Topics

Data Classification (System Office IT Policy)

- Public Data – Low security
- Private Data
  - Restricted: Most private data
  - Highly Restricted: Sensitive data such as financial data and social security numbers

Record Retention and Storage

- Government data must be kept in a manner that is readily accessible for convenient use.
- Follow record retention policies. HR, Finance, and Facilities records fall under Statewide General Schedules, and campuses typically have their own retention schedules for other documents.
- In addition, there is a requirement to maintain a “data inventory.” This is separate from System Office IT’s data classification project.

MGDPA and Contracts

Once the college or university signs a contract, state law classifies data related to that contract as public data.

- Exceptions include:
  - Trade Secrets
    - Examples of trade secrets include the Coca-Cola Recipe and some software source code.
    - We do not typically accept requests from contractors to define pricing data as trade secret data.
  - Security Data
    - The law defines security data as data that, if revealed, can jeopardize the safety of persons or property, including IT systems.
  - Contracts occasionally contain other non-public data.

Data Breaches

The MGDPA requires notice to affected individuals of a breach of security (unauthorized access) for

- any private or confidential data (not just SSN or financial information)
- in any medium (not just computerized).

E.g., lost or stolen laptop containing student program data.

Contact your supervisor or campus DPCO if you believe you have a possible security breach situation.

- OGC will assist in determining whether notice is required, how it must be done and other details.

THE FEDERAL DEPARTMENT OF EDUCATION NOW REQUIRES SAME-DAY NOTIFICATION OF DATA BREACHES.

Consequences of Violations

- A violation of the Data Practices Act could result in:
  - Court order for corrective action
  - Damages to data subject
  - A violation of Section 13.32 (FERPA) could result in sanctions by the Department of Education

Minnesota State Contact Information

Dan McCabe
Assistant General Counsel
daniel.mccabe@minnstate.edu
651-201-1833

Office of General Counsel
https://www.minnstate.edu/system/ogc/index.html

How to Access Today's Materials

- The PowerPoint can be found on the Office of General Counsel's webpage.
- If you would like a link to the recording please send an email to Amanda Bohnhoff Amanda.Bohnhoff@minnstate.edu