MCIT

Minnesota Counties Intergovernmental Trust

VIRTUAL RISK MANAGEMENT WORKSHOP

The Minnesota Government Data Practices Act (MGDPA): The Basics

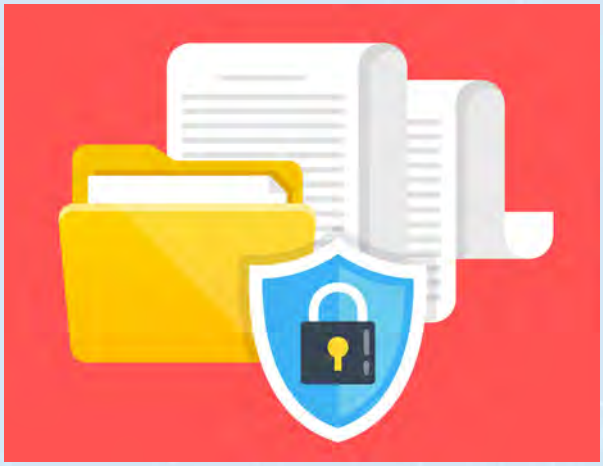
PRESENTED BY:

Karen Clayton Ebert

Senior Staff Counsel for Risk Control

Topics Covered

- Fundamentals of MGDPA
- Data classification and reasons it matters
- Requests for data
- Individual rights
- Data security and breach notification
- Tips for protecting data
- Penalties and coverage



Fundamentals

Minnesota Government Data Practices

Minnesota Government Data Practices Act

A series of laws that govern:

- The public's right to access government data
- The government's obligation to produce such data

Duties of Responsible Authority and Compliance Officer

Responsible Authority

- Responsible for day-to-day administration of MGDPA
- Develops, manages policies and procedures for MGDPA compliance
- Creates security, data safeguard procedures
- Establishes inventory of not public data

Compliance Officer

- Appointed by RA to respond to public questions or concerns about data access

The Responsible Authority

County RA is designated by the board

If none: Administrator or coordinator is default

If neither position: Default is county auditor

Other RAs:

- Noncounty political subdivisions default to chief clerical officer
- Elected officials for own office
- Director of county welfare agency is RA of that agency
- County veteran services officer is RA for all records within that office

What Is Government Data?

"All data collected, created, received, maintained or disseminated by any government entity regardless of physical form, storage media or conditions of use."

Definition from Minnesota Statutes, Section 13.02, Subdivision 7

Examples of Data

- Personnel records and applications for employment
- Policy and procedure manuals
- Notice of meetings and minutes
- Written correspondence, e-mail, voice mail, text messages
- Contracts, memoranda of understanding, joint powers agreements
- Training materials
- Research data/materials
- Resource or reference materials

Employee-owned Devices

- Government data is not defined by where it is stored, its format or how it is used
- Government data may be stored on employee's electronic devices
- If government data is responsive to request, employee's dual use device may need to be produced

General Rule of Thumb

- If the data relates to work *or* employee receives data because he/she is an employee of a public entity:
  - It is government data
- If you have questions, ask!

Data Classification and Why It Matters

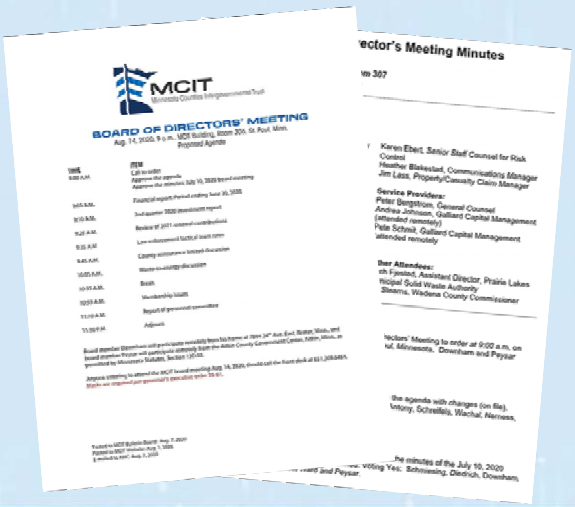
Minnesota Government Data Practices Act

Access to Data

Public Data	Private or Nonpublic Data	Confidential or Protected Nonpublic
Anyone who requests it	Data subject, government employee or official whose job duties reasonably require access, or entities authorized by law	Government employee or official whose job duties reasonably require access, or entities authorized by law

Data Is Presumed to Be Public

- Unless otherwise classified by state or federal statute
- Examples of exceptions (presumed private unless otherwise classified):
  - Personnel data
  - Benefit assistance data
  - Health and medical data



What Is Data on Individuals?

"**All government data in which any individual is or can be identified as the subject of that data**, unless the appearance of the name or other identifying data can be clearly demonstrated to be only incidental to the data and the data are not accessed by the name or other identifying data of any individual."

Minnesota Statutes, Section13.02, Subdivision 5

Public Data on Individuals

- For employees subject to the MGDPA:
  - Employee's name
  - Employee's identification number (may not be SSN)
  - Actual gross salary
  - Salary range
  - Contract fees
  - Actual gross pension
  - Value and nature of employer-paid fringe benefits
  - Basis for and amount of added remuneration, including expense reimbursement in addition to salary
  - Others (Minn. Stat. § 13.43)
- Adult jail register logs
- Application to register real property title

Private Data on Individuals

- Most personnel data on employees subject to MGDPA
  - Employee home addresses (§ 13.43)
  - Employee performance evaluations (§ 13.43)
- Most public health data on individuals
- Most welfare (human services) data on individuals
- Workers' compensation data

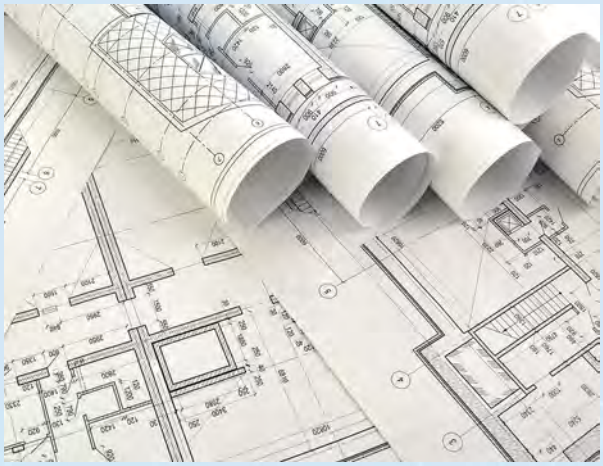
Confidential Data on Individuals

- Civil investigative data:
  - Part of an active investigation for the purpose of commencing or defending a pending civil legal action; or
  - Which are retained in anticipation of a pending civil legal action (§13.39)
- Names of reporters alleging maltreatment of minors or maltreatment of vulnerable adults
- Identities of individuals who register complaints concerning violations of the use of real property
- Attorney-client privileged information

Data Not on Individuals

Anything that is not about an individual

Minnesota Statutes, Section 13.02



Public Data Not on Individuals

- Training materials
- Most land records
- Vendor contracts (redact trade secrets)
- Joint powers agreements/ bylaws
- Maintenance manuals of office equipment
- Board agendas and minutes

Nonpublic Data Not on Individuals

- Security information (§13.37)
  - Computer or database passwords
  - Data on security system that could jeopardize security
  - Data on computer system security (firewalls, etc.)
  - Checking account number
- Trade secrets (as defined by §13.37)

Protected Nonpublic Data Not on Individuals

Civil investigative data not on individuals (§13.39)

Classifying Data

- Data may have different classifications in the hands of different agencies
- What is the classification …
  - … When it is in the hands of your entity
  - … At the time of the request?

Data Classifications May Change with Triggering Events

Examples:

- Sealed bids are nonpublic data, but name of bidder and dollar amount become public once bids are opened (§13.591, subd. 3)
- Names of employment applicants are initially private data but become public data when applicant is certified as eligible for appointment to vacancy or when considered by appointing authority to be finalists for position in public employment (§13.43, subd. 3)

Why Does Classification Matter?

- Sharing not public data
  - o May expose government entity to liability
  - o May subject employee to discipline
- Hot button issue in media and political arena

Requests for Data

Minnesota Government Data Practices Act

Data Requests

All requests should be directed to the responsible authority or designee

Requests for Data

- The RA must allow access/copies of the data or provide a reason for the denial, including the statutory cite
- If the information does not exist, the requestor should be informed of that fact
- The entity is not required to create data

Timeline for Responding to Requests

Because of timelines, it is important to route requests for data ASAP!

	Member of Public	Subject of Data
Inspection of Data or Copies of Data	As soon as reasonably possible Minn. Stat. §13.03; Minn. R. 1205.0300, subd. 3	Immediately if possible or within 10 business days Minn. Stat. § 13.04, subd. 3

Costs for Inspection and Copies

	Member of Public	Subject of Data
Inspection of Data	No charge or fee allowed	No charge or fee allowed
Copies of Data	• 100 or fewer, black and white, legal/letter size paper copies: 25 cents per page • All other copies: Actual cost • No charge to separate public and not public data Minn. Stat. § 13.03, subd. 3	Actual cost • No charge to search for and retrieve data • No charge to separate public and not public data • No charge to redact private or confidential data about others Minn. Stat. § 13.04, subd. 3

Individual Rights

Minnesota Government Data Practices Act

Collection of Private or Confidential Data on Individuals

- Generally, public entity may not collect data on individuals unless data is necessary to carry out organization's duties (§13.05, subd. 3)
- Tennessen Warning
  - Required whenever collecting private/confidential data from an individual concerning that individual
  - Allows individual to make an informed decision regarding whether to provide data

Tennessen Warning Requirements

1. The purpose and intended use of the data
2. Whether the individual is legally required to provide the data
3. Known consequences from either providing or refusing to provide the data
4. Identity of other persons and/or entities authorized by federal or state law to receive the data (§13.04, subd. 2.)

If you believe a Tennessen warning may be necessary, discuss with supervisor

Consent to Release Private Data

- *Written permission* from an individual that allows a government entity to:
  1. Release the individual's private data to a third party or different party than originally described in the Tennessen warning
  2. Use the individual's private data within the entity for a different purpose than for what it was originally collected

Consent to Release Private Data

- Written consent should be placed in file with data that was released
- Verbal consent is insufficient

Additional Rights of Data Subjects

- To be informed whether he/she is subject of stored data and its classification
- To challenge the accuracy and/or completeness of data
  - RA has 30 days to respond to the challenge
  - Decision cannot be made by a designee
  - Challenges and appeals resource
    - *MN.gov/admin/data-practices/data/appeals/*

If you receive a challenge, forward to the responsible authority *as soon as possible!*

Data Security and Breach Notification

Minnesota Government Data Practices Act

Data Security

- Individuals have the expectation of the security of their data
- Failure to follow established security safeguards for records containing data on individuals can violate MGDPA
- If a "data breach" occurs, the entity has to:
  - Provide notice
  - Conduct an investigation
  - Compile a report

What Is a Data Breach Under MGDPA?

Person with no reasonable, work-related need to access private or confidential data views or takes the data with the intent to use the data for purposes unrelated to his/her job.

Minn. Stat. §13.055
Per Minn. Dept. of Admin. Data Practices Office: MN.gov/admin/data-practices/data/warnings/breaches/

Notice of Breach

- Must provide written notification to any individual who is the subject of private or confidential data that is reasonably believed to have been breached
- Notice must say:
  - Report will be prepared
  - Individual may obtain a copy of the report via mail or e-mail
- Notice must be sent upon discovery of breach
  - May be delayed if a law enforcement agency determines notification will impede a criminal investigation
- If more than 1,000 individuals, must notify consumer reporting agencies

Written Report About a Breach

If a breach occurred due to an employee, contractor or agent of the government, the report must include:

1. Facts of the breach and type of data accessed
2. Number of individuals whose data was breached
3. Upon final disposition of discipline, if any, the name of each employee and the discipline actions taken against him/her

Tips for Protecting Data

Minnesota Government Data Practices Act

Protecting Not Public Data

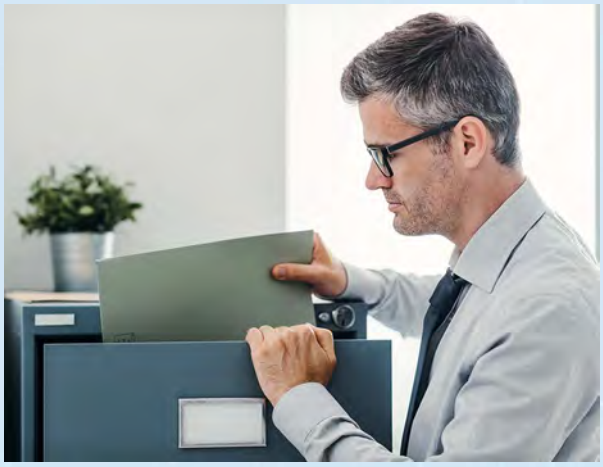
- Be aware of surroundings when discussing not public data
- Care must be taken not to share private or confidential data with anyone not authorized to receive the data
  - Includes co-workers, family, friends and the public

Protecting Not Public Data

- When seeking input from professional peers outside your entity, discuss issues in general terms only
- Omitting the individual's name may not be enough if the other information provided can be used to identify the individual

Protecting Not Public Data

- Ensure not public data in work station is protected
  - Private data should be secured, put under cover and/or removed entirely from view
  - Lock computer screens when leaving computer
- Be aware of what is going in e-mails and to whom
- Be careful about leaving voice mail messages with private data
- Use encryption software when available



Protecting Not Public Data

- Data must be disposed of properly, shredded or minced
  - If you wouldn't give it to the public upon request, then it should be shredded when disposing
- Take care not to leave private or confidential data on printer or copier

Keep in Mind

Posting of not public government data on social media could violate MGDPA or other data privacy laws

- Could be grounds for disciplinary action, even if employee was off duty and using a nonwork computer

Penalties and Coverage

Minnesota Government Data Practices Act

Penalties for Violating the MGDPA

- Civil lawsuit to recover damages sustained, plus costs and reasonable attorney fees
  - If willful, government entity may also be liable for exemplary damages between $1,000 and $15,000 for each violation
- Civil lawsuit to compel compliance
  - May recover costs and reasonable attorney fees
  - Civil penalty of up to $1,000
- Injunctive relief may also be sought

Penalties for Violating the MGDPA

- Administrative remedy: Civil penalty up to $300 and reasonable attorney fees
- Criminal penalty: Intentional violation is a misdemeanor
- Employment penalty: Intentional violation is just cause for suspension without pay or dismissal

MCIT Coverage for MGDPA Claims

MCIT Pays*

- Defense attorney costs
- Damages
- Fees associated with defending the claim

Member Pays:*

- Fines
- Plaintiff's attorney fees

*For covered claims

When in Doubt, Don't Give It Out

- Consult with the responsible authority
- Consult with legal counsel
- Check resources available from
  - Department of Administration, Data Practices Office website
  - *MCIT.org*
- Obtain opinion from Department of Administration (in consultation with legal counsel)

Join Us for More Workshops This Week

Register at *MCIT.org/training-calendar/*

The Devil Is in the Details of the Minnesota Government Data Practices Act
Oct. 21 at 1 p.m.

Essentials of Risk Management for Motor Vehicles
Oct. 22 at 10:30 a.m.

Benefits and Tips for Creating a Positive Safety Culture
Oct. 22 at 1 p.m.

Hot Topics in Risk Management
Oct. 23 at 10:30 a.m.

Trending Topics in Employment
Oct. 23 at 1 p.m.

Discussion

Submit Questions Using the Chat Feature