Open Meeting Law and Minnesota Government Data Practices Act

MASWCD GOVERNANCE 101
Sept. 17, 2015
The information contained in this document is intended for general information purposes only and does not constitute legal or coverage advice on any specific matter.
Minnesota Government Data Practices Act

FUNDAMENTALS
The Minnesota Government Data Practices Act (MGDPA)

A series of laws that govern:

- The public’s right to access government data
- The government’s obligation to produce such data
Procedural Requirements Under the MGDPA

A government entity must:

- Designate a responsible authority (RA);
- Prepare a public document that names the RA;
- Designate a data practices compliance official;
- Establish an inventory for data on individuals;
- Prepare a written policy on rights of data subject and procedures to access data
- Provide ongoing training to personnel
2014 New Policies and Procedures

• RA must create procedures and appropriate safeguards for all records containing data on individuals that ensures that:
  – Not public data are only accessible to persons whose work assignment reasonably requires the data
  – Data is only being accessed for permitted purposes by appropriate individuals

• Develop a policy incorporating these procedures
  – May include a policy for sharing data with other government entities as authorized by law
    (Minn. Stat. §13.05, subd. 5)
Responsible Authority

SWCDs:

• Individual appointed by the board
• If no individual is appointed, it is the chief clerical officer for filing and record keeping purposes
Duties of Responsible Authority and Compliance Officer

• Responsible authority:
  – Responsible for day-to-day administration of MGDPA
  – Develops and manages policies and procedures to comply with MGDPA
  – Creates security and data safeguard procedures
  – Establishes inventory of not public data

• Compliance Officer:
  – Appointed by RA to respond to public questions or concerns about data access
Source: New York Office of Information Technology
What Is Data?

Definition:

“All data collected, created, received, maintained or disseminated by any government entity regardless of physical form, storage media or conditions of use.”
(Minn. Stat. § 13.02, subd. 7)
Photos by Jim Mims; and phasinphoto, winnond and Stuart Miles for freedigitalphotos.com
Data Is Presumed to Be Public

• Generally, there is a presumption that government data is public data, 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
# Who has Access?

<table>
<thead>
<tr>
<th>DATA ON INDIVIDUALS</th>
<th>DATA NOT ON INDIVIDUALS</th>
<th>WHO HAS ACCESS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public</td>
<td>Public</td>
<td>Anyone</td>
</tr>
<tr>
<td>Private</td>
<td>Non-public</td>
<td>Data subject; government employees and officials whose work assignments reasonably require access; and entities authorized by law</td>
</tr>
<tr>
<td>Confidential</td>
<td>Protected Non-public</td>
<td>Only government employees and officials whose work assignments reasonably require access, and entities authorized by law</td>
</tr>
</tbody>
</table>
Classifying Data: Data on Individuals

- Public Data Examples: subject to a few specific exceptions, employee’s name; employee identification number (may not be SSN); actual gross salary; salary range; contract fees; actual gross pension; the value and nature of employer-paid fringe benefits; basis for and amount of added remuneration, including expense reimbursement in addition to salary (13.43, subd. 2 (a)(1))
- Private Data Examples: personnel evaluations; employee photographs
- Confidential Data Examples: data collected as part of an active investigation undertaken for the purpose of the commencement or defense of a pending civil legal action or which are retained in anticipation of a pending civil legal action (13.39, subd. 2)
Classifying Data: Data Not on Individuals

All government data that is not on individuals. (13.02 subd. 4)
• Public Data Example: job descriptions
• Non-public Data Example: data submitted by a business to a government entity in response to a request for bids as defined in section 16C.02, subdivision 11, are private or nonpublic until the bids are opened. (note: classification changes once bids are open) (13.591, subd. 3)
• Protected Non-public Data Example: data (not on individuals) collected as part of an active investigation undertaken for the purpose of the commencement or defense of a pending civil legal action or which are retained in anticipation of a pending civil legal action (13.39, subd. 2(a))[exception: complainant has access to a statement he/she made to a government entity provided under this subd. (13.39, subd. 2(b))]

MINNESOTA COUNTIES INTERGOVERNMENTAL TRUST
Hypothetical

An SWCD supervisor (who does not serve on the personnel committee) wants access to an employee’s personnel file. May it be released?
Personnel Data Hot Spot

Existence/status of complaints (regardless of disciplinary action)

• Public
• Subject matter underlying complaint—PRIVATE
Personnel Data Hot Spot

• Final disposition of any disciplinary actions—PUBLIC
  – Specific reasons for the action
  – Data documenting the basis of the action
  – Does not include data that would identify confidential sources who are employees of the public body

• Terms of any agreement settling any dispute arising out of an employment relationship—PUBLIC
  – Includes a buyout (123B.143, subd. 2 (a))
  – Must include specific reasons if involve the payment of more than $10,000 of public money
Final Disposition

Occurs when the government entity makes final decision about disciplinary action

• Most future court proceedings do not matter
• Arbitration proceedings under CBA do matter
• Final disposition includes a resignation by an individual when the resignation occurs after the final decision of the government entity or arbitrator
Final Disposition

• Final disposition occurs:
  – Conclusion of arbitration; or
  – Failure to elect arbitration within time outlined in CBA

• A disciplinary action does not become public data if an arbitrator sustains a grievance and reverses all aspects of the disciplinary action
Final Disposition

For the chief administrative officer or the individual acting in an equivalent position, data related to complaint or charge becomes public when:

• The complaint or charge results in disciplinary action or the employee resigns or is terminated from employment while the complaint or charge is pending; or

• Potential legal claims arising out of the conduct that is the subject of the complaint or charge are released as part of a settlement agreement
Final Disposition

• Does not authorize the release of data that are made not public under other law
• Public official includes: managers; chiefs; heads or directors of departments, divisions, bureaus, or boards; and any equivalent position
Hypothetical

• The SWCDs district manager is being investigated for the theft of SWCD funds. The SWCD has hired someone to investigate. The local paper asks if the district manager is under investigation for theft of government funds.

• What, if anything, can you say?
Intergovernmental Access to Data

A responsible authority shall allow another responsible authority access to data classified as “not public” only when the access is authorized or required by statute or federal law.
Hypothetical

An SWCD is having a disciplinary issue with an employee. The SWCD wants to discuss the employee’s interactions with an employee from BWSR.

• Is this allowed?
• How may the SWCD achieve its goals?
Collection of Not Public Data on Individuals

• Tennessen Warning
  – Required when collecting private/confidential data from an individual
  – Purpose: Informed decision regarding whether to provide data

• Generally, a government entity may not collect data on individuals unless the data is necessary to carry out organization’s duties
Informed Consent

A written permission from an individual that allows a government entity to:

• Release the individual’s private data to a third party
• Use the individual’s private data within the entity for a different purpose than originally collected
Hypothetical

A former SWCD employee asks you to be a reference for a job.

• What limitations do you have in being a reference?
• What can you do to address those limitations?
WHEN IN DOUBT, DON’T GIVE IT OUT

- Consult with responsible authority
- Consult with legal counsel
- Obtain opinion from Department of Administration
# Timeline for Responding to Requests

<table>
<thead>
<tr>
<th></th>
<th>MEMBER OF PUBLIC</th>
<th>SUBJECT OF DATA</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>INSPECTION OF DATA</strong></td>
<td>As soon as reasonably possible</td>
<td>Immediately if possible or within 10 business days</td>
</tr>
<tr>
<td></td>
<td>Minn. Stat. 13.03; Minn. R. 1205.0300, subp. 3</td>
<td>Minn. Stat. 13.04, subd. 3</td>
</tr>
<tr>
<td><strong>COPIES OF DATA</strong></td>
<td>As soon as reasonably possible</td>
<td>Immediately if possible or within 10 business days</td>
</tr>
<tr>
<td></td>
<td>Minn. Stat. 13.03; Minn. R. 1205.0300, subp. 3</td>
<td>Minn. Stat. 13.04, subd. 3</td>
</tr>
</tbody>
</table>
## Costs and Fees

<table>
<thead>
<tr>
<th>INSPECTION OF DATA</th>
<th>MEMBER OF PUBLIC</th>
<th>SUBJECT OF DATA</th>
</tr>
</thead>
<tbody>
<tr>
<td>No charge or fee allowed</td>
<td>No charge or fee allowed</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>COPIES OF DATA</th>
<th>MEMBER OF PUBLIC</th>
<th>SUBJECT OF DATA</th>
</tr>
</thead>
<tbody>
<tr>
<td>25 cents per page (100 or fewer, black &amp; white, legal/letter size paper copies)</td>
<td>Actual cost</td>
<td></td>
</tr>
<tr>
<td>Actual cost (all other copies, no charge to separate public and not public data)</td>
<td>no charge to search for and retrieve data</td>
<td></td>
</tr>
<tr>
<td>Minn. Stat. 13.03, subd. 3</td>
<td>no charge to separate public and not public data</td>
<td></td>
</tr>
<tr>
<td></td>
<td>no charge to redact private or confidential data about others</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Minn. Stat. 13.04, subd. 3</td>
<td></td>
</tr>
</tbody>
</table>
Challenging Accuracy of Data

• Data subject has a right to challenge the completeness or accuracy of data
• RA has 30 days to respond
MGDPA

EMERGING ISSUES: PERSONAL DEVICES AND SOCIAL MEDIA
Complex Issue

• Risks to bring your own device (BYOD) apply to both employer and employee

• No one-size-fits-all solution
  – Depends on the needs and resources of government entity and employees
  – May differ among departments and positions

• Multidisciplinary approach may yield best results
The Problem

• Government entity is legally responsible for data privacy and security
• Employee is responsible for physically securing device and data
Inadvertent Release of Data

• Lost or stolen device
• Access by friends and family
• Malware or computer viruses
• Employee upgrades device
• End of employment relationship
• Remote backup and storage
Employee-owned Devices

• Government data includes all data collected, created, received, maintained or disseminated by a government entity
  – It is not defined by where it is stored, in what format or how it is used

• Government data on an employee’s personal device is subject to the MGDPA and may need to be produced
Conduct a Risk Assessment of Current BYOD Use

- Who is using a personal mobile device for work purposes?
  - Exempt vs. nonexempt employees
- How often is the device used for work purposes?
- Why is the employee using his or her personal device?

- How is government data being accessed or stored on the device?
- What data or information is being accessed or stored?
- How is the data or information classified under the MGDPA?
- What security measures are in place on device?
Mitigating the Risks

- Consider a BYOD policy
- Password/passcode to protect personal devices
- Encrypt any work-related data to the extent possible
- Use the device’s screen lock function
- Do not download or store private government data on the device unless necessary
- Keep work and personal information separate to the extent possible
- Comply with data privacy policies and any other retention requirements
MGDPA

NOTIFICATION OF BREACHES
New in 2014: 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 that a report will be prepared and that the 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
What Is a Data Breach?

• Defined as any unauthorized acquisition of data by an unauthorized person
  – “Unauthorized acquisition”: A person obtained, accessed or viewed government data without informed consent of the subject of the data
  – With intent to use the data for a nongovernmental purpose

• An unauthorized person is anyone accessing data:
  – Without a work assignment that reasonably requires access
  – Regardless of assignment, if an individual accesses for a purpose not described in an entity’s access policies

• (Minn. Stat. §13.055)
Investigating a Breach

• All data breaches must be investigated
• Upon completion of the investigation, entities are required to prepare a report
• New in Minnesota Statutes, Section 13.055
Written Report About a Breach

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

• Facts of the breach and type of data accessed
• Number of individuals whose data was breached
• Upon final disposition of discipline, if any, the name of each employee and the discipline actions taken against him or her
Minnesota Government Data Practices Act

PENALTIES AND COVERAGE
Penalties for Violating the MGDPA

• Civil liability: damages, costs, compliance, injunctive relief and attorney fees
  – If a willful violation, liable for exemplary damages of not less than $1,000 and not more than $15,000 for each violation

• Administrative remedy: civil penalty up to $300 and reasonable attorney fees

• Criminal penalty: an intentional violation of the MGDPA is a misdemeanor
Penalties for Violating MGDPA (Continued)

• Employment consequences: an intentional violation of the MGDPA may subject the employee to suspension without pay or dismissal
MCIT Coverage for MGDPA Claims

• MCIT will pay:*  
  – Defense attorney costs
  – Damages
  – Fees associated with defending the claim

• Entities will pay:*  
  – Fines
  – Plaintiff’s attorney fees

*For covered claims
OPEN MEETING LAW
The Minnesota Open Meeting Law

- Found in Minnesota Statutes Chapter 13D
- Presumes all meetings of a public entity’s governing body are open to the public unless the governing body has the statutory authority to close the meeting
Purpose of the Open Meeting Law

1. Prohibit actions from being taken at a secret meeting where it is impossible for the public to become fully informed about a public body’s decision or to detect improper influences

2. To assure the public’s right to be informed

3. To afford the public an opportunity to present its views to the public body
Open Meeting Law

APPLICATION
Applies to Meetings of the Governing Body of:

- School district however organized
- Unorganized territory
- County
- Statutory or home rule charter city
- Town
- Other public body
Which Meetings?

• All meetings of the public body as a whole
• Committees or subcommittees if:
  – Public body members comprise a quorum of the committee or subcommittee; or
  – Public body delegated authority to the committee or subcommittee
Informational Gatherings

• OML applies to informational gatherings, such as:
  – Retreats
  – Executive sessions
  – Public hearings
  – Work sessions on matters currently facing or that might come before the body

• Minnesota Attorney General: Attendance at training programs designed for board members or officials in general does not violate the law if the members do not discuss specific municipal business
Social Gatherings

• OML does not apply to a quorum that comes together by chance or at a social gathering
• The quorum may not discuss or receive information about official business
Serial Meetings

• Serial meetings must not be used to build a consensus outside of a public meeting
• Includes telephone conversations, e-mails, texting and social media
Use of social media: The use of social media by members of a public body does not violate this chapter so long as the social media use is limited to exchanges with all members of the general public. For purposes of this section, e-mail is not considered a type of social media.
Open Meeting Law

MEETING TYPES
Meeting Types

• Regular meetings
• Special meetings
• Emergency meetings
• Recessed and continued meetings
Regular Meetings

• Conducted routinely or on a prescribed schedule

• Schedule of the board’s regular meetings must be kept on file at its primary office and include times and locations

• If a meeting is at a time or location inconsistent with the schedule, must give notice of the changes in the same manner as a special meeting
Special Meetings

Meetings not conducted as part of the normal routine but planned far enough in advance to be scheduled
Special Meeting Notice

- Posted with the date, time, place and purpose of the meeting on the principal bulletin board or door of its usual meeting room, and

- Mailed or delivered to people who have filed a written request for special meeting notices

- Posted and mailed/delivered at least three days before the meeting

- Alternative to mailing: may publish notice in the official newspaper three days prior to the special meeting
Emergency Meetings

Meetings called because of circumstances that require immediate attention in the public body’s judgment
Emergency Meeting Notice

- Must make good faith effort to provide notice to news media that have filed a written request with telephone number
- Notice must include date, time, place and explanation of subject of the meeting

- Must also give notice by telephone or other reasonable method to members of the public body
Recessed and Continued Meetings

No published or mailed notice is necessary if:

• The time and place of the meeting was established during the previous meeting and
• It was recorded in the minutes of that meeting
4 Conditions for Meeting via Interactive Television

1. All members of the body participating in the meeting, wherever their physical location, can hear and see one another as well as hear and see all discussion occurring at any location at which at least one member is present;

2. Members of the public present at the regular meeting location can hear and see all discussions, testimony and votes of the public body;

3. At least one member of the public body is physically present at the regular meeting location; and

4. Each location at which a member of the public body is present is open and accessible to the public.
Other Requirements for Meeting via Interactive Television

• Must give notice of meeting location and any site where a board member will be participating in the meeting by interactive television

• To the extent practical, a public body shall allow a person to monitor the meeting electronically from a remote location
Meeting by Telephone or Other Electronic Means

• Used only when an in-person meeting or a meeting conducted under the interactive television provision is not practical or prudent because of:
  – A health pandemic
  – An emergency declared under Minnesota Statutes Chapter 12

• Board must comply with statutory conditions when holding a meeting by telephone (Minn. Stat. § 13D.21)
Criteria For

CLOSING MEETINGS
Must Be Closed

Preliminary consideration of allegations or charges against an individual subject to the board’s authority:

- Must be open if the individual who is the subject of the allegations/charges requests it to be
- If body concludes that discipline may be warranted as a result, further meetings relating to the specific allegations/charges held after that conclusion is reached must be open
Must Be Closed

Data identifying alleged victims or reporters of:

- Criminal sexual conduct
- Domestic abuse
- Maltreatment of minors or vulnerable adults
**Must Be Closed**

- Active criminal investigation data as defined in Minnesota Statutes, Section 13.82, Subdivision 7 or
- Internal affairs data relating to allegations of law enforcement personnel
**Must Be Closed**

- Certain not public data under MGDPA for:
  - Education (Minn. Stat. § 13.32)
  - Health (Minn. Stat. § 13.3805, subd. 1)
  - Medical (Minn. Stat. § 13.384)
  - Welfare (Minn. Stat. § 13.46, subd. 7)
  - Mental health (Minn. Stat. § 13.46, subd. 2)

- Medical records governed by Minnesota Statutes, Sections 144.291 to 144.298

- Expressly required by other law
May Be Closed

• Labor negotiations
• Performance evaluations: Must be open upon request of employee being evaluated
• Attorney-client privilege
May Be Closed

• To determine the asking price for real or personal property to be sold by the entity
• To review confidential or protected nonpublic appraisal data under Minnesota Statutes, Section 13.44, Subdivision 3
• To develop or consider offers or counteroffers for the purchase or sale of property
May Be Closed

• Security briefings and reports
• Issues related to security systems
• Security deficiencies in or recommendations regarding public services, infrastructure and facilities
• Emergency response procedures
Open Meeting and Not Public Data

• Unless required to be closed, not public data may be discussed at an open meeting if the disclosure:
  – Relates to a matter within the scope of the public body’s authority
  – Is reasonably necessary to conduct the business or agenda item before the public body

• Any data discussed retains its original classification
Procedures For

CLOSING A MEETING
Closing a Meeting

• A motion to close the meeting must be made in open session:
  – Reference applicable statutory provision
  – Describe subject to be discussed
• Discussion in the closed meeting should be limited to the subject of the closing
• Withhold any materials discussed in closed session from public
Recording Closed Meetings

• Closed meetings must be recorded
• Does not apply to meetings closed under attorney-client privilege
• Recordings must be preserved for at least three years, unless another period is provided by an existing law
Hypothetical

The SWCD would like to conduct interviews for a new district manager. May the SWCD close the meeting?
Hypothetical

The SWCD Board is going to conduct a personnel evaluation of the district manager:

• Does the district manager have to know about the evaluation?
• May the board close the meeting? How?
• What if the district manager objects to closing the meeting?
ENFORCEMENT, PENALTIES AND COVERAGE
Penalties

- Board member(s) may be personally fined up to $300 for each violation if a court finds intentional violation of the OML.
- Fines may not be paid by the public body.
- If a board member is found to have intentionally violated the law three or more separate and unrelated times, the court may remove the board member(s) from office.
Penalties

• Board member(s) may be ordered to pay costs, disbursements and attorney fees up to $13,000 to claimant

• Public body may choose to indemnify the board member(s) for these expenses

• Monetary penalties and attorney fees awarded only if intent to violate is found
MCIT Coverage

Pays defense attorney fees and defense costs associated with defending an OML claim:

• Excludes fines imposed under the OML
• Excludes costs, disbursements and attorney fees awarded to a claimant
What to Do

WHEN YOU’RE UNSURE
When in Doubt

Notice the meeting and comply with other Open Meeting Law requirements
Ask Questions and Share Experiences

DISCUSSION