



Essentials of Data Practices for Responsible Authorities

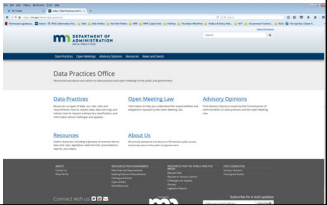
Data Practices Office
Taya Moxley-Goldsmith
Grace Baehren

1

Who we are and what we do

Data Practices Office

- Informal advice/technical assistance
- Commissioner of Administration advisory opinions
- Website and info pages: <https://mn.gov/admin/data-practices/>
- Email list and newsletters
- Legislative assistance
- Training



2

Workshop Agenda

9:00	Data practices basics and best practices in responding to data requests
10:45	Morning break
11:00	Morning scenarios
11:30	Data practices policies, procedures, and training
Noon	Lunch
12:45	Personnel data/redaction exercise
2:00	Afternoon break
2:15	Accuracy and completeness data challenges and appeals
2:30	Data breach requirements – investigation and notification
2:45	Afternoon scenarios
3:15	Final Q&A and evaluations

3

Topics

- Overview of requirements
- Best practices in responding to requests
- Remedies and penalties
- Policies and procedures
- Data breaches
- Data challenges
- Hot topics

4



Data Practices Basics

5

Data practices policy

Maintain proper balance

- Public's right to access public government data
- Privacy rights of individuals
- Government's need to conduct business properly and efficiently



6

Minnesota Government Data Practices Act

- Minnesota Statutes, Chapter 13
 - Presumes government data are public
 - Classifies data that are not public
 - Provides rights for the public and data subjects
 - Requires that data on individuals be accurate, complete, current, and secure
- Minnesota Rules, Chapter 1205
 - Take note: We are updating these rules!

7

Application

- Applies to statewide agencies, statewide systems, or political subdivisions
- Does not apply to the legislative or judicial branches
 - Minn. Stat. §13.02, subd. 7a., Minn. Stat. §13.90
- Does not apply to townships outside the metro area
 - Minn. Stat. §13.02 subd. 11; Minn Stat. §473.121 subd. 2

8

Government data defined

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

(Minn. Stat. § 13.02, subd. 7)



9

Other data practices related laws

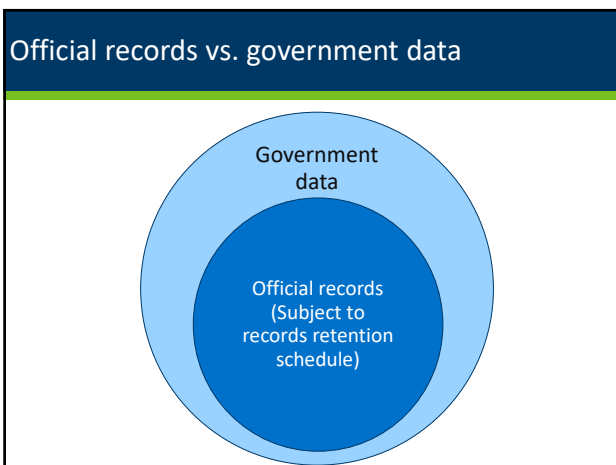
- **Official Records Act**
(Minn. Stat., section 15.17)
 - Make and preserve all records necessary to a full and accurate knowledge of official activities
- **Records Management Statute**
(Minn. Stat., section 138.17)
 - Maintain records according to schedule
 - MNGRIN: <https://sites.google.com/site/mngrin/>
 - MN State Archives website: <https://www.mnhs.org/preservation/state-archives>



10



11



12

Chapter 13 check!

You have three versions of a report from last year including the final report.

- What is the official record?
- Are all the drafts government data?
- Can you destroy the drafts?

13

Chapter 13 check!

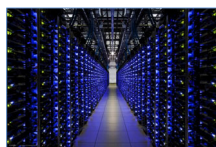
You have three versions of a report from last year including the final report.

- What is the official record?
 - Final report (exceptions)
- Are all the drafts government data?
 - Yes
- Can you destroy the drafts?
 - Yes

14

Maintaining government data

- No requirement to maintain data in a particular format or organization system
- However...
 - Data must be **“easily accessible for convenient use”**



15

Staff with data practices duties

- Responsible authority (RA):
 - A county-level elected official
 - Director of county social services agency
 - County Veterans Services Officer
 - For other County data, individual appointed by the county board –if none, then the RA is the county coordinator or administrator or, if the county does not have a coordinator or administrator, the county auditor.
- Data practices compliance official (DPCO)
- Designees (optional, consider police department)
- All staff have some data practices responsibilities

16

Duties of the RA

- Duties:
 - Create policies and procedures
 - Provide training
 - Coordinate responses to data requests
 - Appoint the data practices compliance official
 - Designate designees

17

DPCO duties § 13.05, subd. 13

The **data practices compliance official** is the designated employee of the government entity to whom persons may direct questions or concerns regarding problems in obtaining access to data or other data practices problems. The responsible authority may be the data practices compliance official.

18

Requests for data

(Minn. Statutes §§13.03 and 13.04)

Members of the public and data subjects can request data – to inspect or get copies

- Written requests
- Accepting requests
 - Designated email address for data requests
 - Forms
 - Use of portal/vendor



19

Resources

- [Developing Data Practices Training](#)
- [Data Practices Basics Webinar](#)
- [What All Responsible Authorities Need to Know](#)
- [What All Employees Need to Know](#)

20

Government data

Data on individuals	Data not on individuals
Data that identify someone • Employee’s telephone number • Name and address of adult arrestee • Athlete of the week photograph	Data that do not identify someone • Makes and models of fleet trucks • Names of companies that are preferred vendors • List of government websites • De-identified data on individuals

21

Classification of government data		
Classification	Meaning of classification	Examples
Public	Available to anyone for any reason	Employee name & salary
Private/ Nonpublic	Available to: • Data subject • Those in the entity whose work assignment requires access • Entities authorized by law • Those authorized by data subject	Employee home address & home phone number
Confidential /Protected nonpublic	Available to: • Those in the entity whose work assignment requires access • Entities authorized by law Not available to the data subject	Data collected as part of an active civil legal action

22

Response time		
	Member of the Public (Section 13.03, subd. 2; Minn. Rules, part 1205.0300)	Data Subject (Section 13.04, subd. 3)
Inspection and/or copies	Appropriate and prompt, a reasonable amount of time	Immediately, if possible, or 10 business days

23

Charging for government data		
	Member of the Public	Data Subject
Inspection	No charge or fee allowed	No charge or fee allowed
Copies	• 25¢ per page 100 or fewer, black and white, legal/letter size paper copies • Actual cost · All other copies · Time for search and retrieval · Time to make and transmit · Materials · No charge to separate public from not public data · Electronic data	• Actual cost · Time to make and transmit · Materials · No charge for search and retrieval · No charge to separate public from not public data · No charge to redact private or confidential data about others

24

Other cost considerations

- Consistent application
 - Charge all requesters OR
 - Have conditions for when charges will apply in policies
 - E.g., If over \$X, copy costs apply/prepayment of 50% applies
- Show your work – how did you arrive at the estimate
- Do you have a process for refunding?
- Requesters can pivot to inspection at any time

25

Responding to data requests Member of the public §13.03

Guidelines for responding to requests

- Clarify if not clear
- Responses:
 - Data do not exist
 - Provide access to public data
 - Data are not public
 - Must give statutory basis for denying access
- If asked, must explain meaning (technical terminology, abbreviations, acronyms, etc.)

26

Responding to data requests Data subject §13.04

Guidelines for responding to requests

- Clarify if not clear
- Data do not exist
- Data exist and are accessible
 - Verify identity
 - Six-month “exception”
- Data are confidential or private about someone else, or otherwise not public
 - Must give statutory basis for denying access
- If asked, must explain (technical terminology, abbreviations, acronyms, etc.)

27

Handling large data requests

- No “overly burdensome” exception to deny access
- Practical considerations:
 - Copies or inspection
 - Contact requester to clarify scope of request
 - Give context on length of time it will take to compile responsive data
 - Ask whether to prioritize certain data
 - Consider providing data on a rolling basis
 - Connect with IT to clarify scope of searching
 - Require reasonable prepayment

28

Suspension of response

Minn. Stat. § 13.03, subd. 3(g)

- Suspend further responses if requester has not collected copies or come in to inspect data within 5 business days of notification
 - Include information on this process in your policies
 - Policies can go further and set out when a data request will be considered abandoned (should provide for a reasonable amount of time after suspension of response)
 - Document, document, document

29

Burdensome vs. harassing

- Burdensome requests are not inherently harassing
- Respectful workplace policy extends to how our teams are treated
- Document behavior and consult with HR and legal counsel
- Modifications to process
 - Direct communication to particular employee
 - Communicate in writing
 - Communicate via US Post
 - Limit in-person contact including inspection (free copies)
- Extreme cases – no longer data practices issue
 - Law enforcement
 - HRO

30

Outside of the Data Practices Act

- Creating data
 - Not required to create data to respond
 - Considerations: databases, voluntary creations
 - Exception: summary data (§13.05, subd 7)
- Responding to questions
 - “Why did you cancel the park project?”
 - “Correspondence discussing park project between the Clerk and Parks Director”
 - Exception: DPCO must respond to questions about how to get access to data and if there are issues.

31

Chapter 13 check!

A member of the public asks for your notes taken during a staff meeting.

- Are they public?
- How long do you have to respond?



32

Chapter 13 check!

A member of the public asks for your notes taken during a staff meeting.

- Are they public?
Probably, but depends on the content.
- How long do you have to respond?
Public - within a reasonable amount of time (if requester is the data subject – then within 10 days).



33

Limitation on collection of government data

Minn. Stat. §13.05, subd. 3 and Minn. Rules part 1205.1500, subp. 4

- Collection and storage of data on individuals and
- Use and dissemination of private/confidential data:
 - Limited to data that are “necessary for the administration and management of programs specifically authorized by the Legislature, local governing body, or federal government.”

34

Tennessen warning notice

(Minn. Stat. §13.04, subd. 2)

When collecting private or confidential data from an individual about that individual:

- State the purpose and intended use of data
- Inform the individual whether they may refuse or are legally required to provide the data
- Explain known consequences of supplying or refusing to supply the data
- Identify other persons or entities with statutory authority to access the data
- Examples: SSN, employee home address

35

Informed consent

Minn. Stat. §13.05, subd. 4 & Minn. R. 1205.1400

- Informed consent is necessary when:
 - The individual asks the entity to release private data to another entity or person
 - The entity wants to release private data to another entity or person
 - The data subject received a Tennessen warning notice and the entity now wants to use or release the data in a different way
- Informed consent must be in writing and cannot be coerced

36

Penalties and remedies

- Remedies (Minn. Stat. §13.08)
 - Action for damages, costs, and attorneys fees
 - Action to compel compliance
 - Injunctive relief
- Administrative remedy (Minn. Stat. §13.085)
 - Administrative complaint filed within 2 years of alleged violation
 - Action to compel compliance
- Penalties (Minn. Stat. §13.09)
 - Willful violation or knowing unauthorized acquisition of not public data = misdemeanor
 - Dismissal or suspension

37



Morning break

38



Morning Scenarios

39



Data practices polices and procedures

40

Data policies v. procedures

- Data access policies ≠ Procedures
- Policies + Procedures = compliance
- Data access policies
 - How someone makes a request
- Data procedures
 - How the government entity responds

41

Access policies

Sections 13.025

- Government entities must have access policies
 - Responding to public data requests
 - Data subject rights and responding to data subject requests
- Additional policies & procedures for law enforcement agencies:
 - <https://mn.gov/admin/data-practices/data/types/lawenforcement/policies/>

42

Requirements for data access policies

- Must adopt *written* access policies
 - Cannot simply rely on compliance with Data Practices Act (see [AO 05-003](#); [13-007](#); [22-001](#))
- Must be updated regularly
 - By August 1 of each year *or* “at any other time necessary to reflect changes in personnel, procedures, or other circumstances that impact the public’s ability to access data”

43

Requirements for data access policies, cont.

- Must be *easily available* to the public
 - Distribute free copies to the public
 - Place in conspicuous spot within the entity
 - Post on entity’s website
- Additional requirements for data subject policy
 - Describe rights under 13.04
 - Government entity’s specific procedures to provide data subject with access to public or private data

44

When has a requester made a request?

- Request is submitted under the identified process in data access policies OR
- Request is submitted to responsible authority OR
- Request is submitted to data practices designee

45

When has a requester *not* made a request?

- Request is not submitted according to written policies
 - E.g. over the phone instead of in writing
- Request is submitted to an employee of entity that is *not* the RA or designee
- Requester asks a question instead of requests data

46

Required data procedures

Sections 13.03, subd. 2(a); 13.05; Minn. Rule 1205.0300

- Procedures to ensure data requests are received and complied with in an appropriate and prompt manner
- Procedures to ensure accuracy of data on individuals
- Establish appropriate security safeguards
 - Procedure for ensuring not public data on individuals are only accessed by employees with a work assignment and for purposes stated

47

Required data procedures – minors

Sections 13.02, subd. 8; 13.05; Minn. Rule 1205.0500

- Entities must have a procedure to allow parent access and provide notice to minors of the right to withhold
- Parents may exercise the access rights of their children
- Minors may restrict parental access to data about themselves if it is in the best interest of the child
- Access by parents is presumed

48

Considerations for data procedures

- Will your procedures be written?
 - If not, can your entity demonstrate that requests are processed in appropriate and prompt manner and data are secure?
- How will you delegate responsibilities for response?
 - The entity can determine who responds to the request according to its procedures
 - RA or designee can delegate response BUT
 - RA or designee is still responsible for compliance

49

Considerations for data procedures, cont.

- How do you track request was received, data was compiled, and access provided?
- Do you use a “data request portal”? What accommodations are in place if someone cannot access the portal?
- What steps are taken when receiving data accuracy challenge? (See §13.04, subd. 4)
- How do you ensure internal access to not public data is limited?

50

Developing security procedures

- Are the data “data on individuals”?
 - If no, entity determination about how to protect
- If yes, what is the classification?
 - If public, no security requirements
- If the data are private or confidential:
 - Required procedures on data security (13.05, subd. 5)
 - Listed on the data inventory (13.025, subd. 1)
 - Optional – policy on who may access data outside the entity

51

Model policies/procedures

Model documents:
<https://mn.gov/admin/data-practices/data/rules/policies/>

- Model Data Access Policies
 - Required by section 13.025
 - Model Policy for the Public
 - Model Policy for Data Subjects
- Model Data Inventory
 - Required by section 13.025
 - Identifies and describes private and confidential data maintained by the entity
- Model Policy for Ensuring the Security of Not Public Data
 - Required pursuant to Section 13.05
 - Methods of incorporating access policy into position descriptions

52


DEPARTMENT OF
ADMINISTRATION

Training Employees on Data Practices

53

Responsible authority duties
Minnesota Rules 1205.1100 and 1205.1300

- The RA is required to provide training to designees and to educate entity personnel on private and confidential data.
- The RA may:
 - Distribute written materials
 - Develop a training programs for all staff
 - Require attendance by designees at internal or external training

54

Goals of employee training

- Data protection and security is responsibility of *government entity*
- Create awareness that data employees create may be public
- Helps to avoid or mitigate data breaches under section 13.055
- Entities cannot discipline employees for data practices violations if they are not trained
- [Developing Data Practices Training](#)

55

What all employees should know

- Classifications of data they work with and can access
- Availability of access policies and procedures
- Key staff for data practices questions & requests
- Consequences for not adhering to data practices requirements or causing a breach
- Use DPO YouTube videos
 - [Data Practices Act: What All Employees Need to Know](#)
 - [Data Practices Potpourri series](#)

56



Lunch Break!

57

What is public?

- A. Your payroll timesheet
- B. Your gross salary
- C. Your education background
- D. Your home address
- E. Your employee identification number
- F. Work email address
- G. Your ID badge photo



58



Personnel data, §13.43

59

What do you think: Definition

Personnel data?

- A. Job posting for an administrative assistant
- B. Email from Data Practices Office staff to you about a copy cost question
- C. Applicant resume
- D. Report on website design vendors with a staff member's name on it



60

Personnel data

Government data *on individuals* maintained because an individual is or was an employee of a government entity, applicant for employment, volunteer, or independent contractor

General public presumption is reversed:

- All personnel data are private except data specifically classified as public

61

Not everything we create is personnel data

- Employee must be the identifiable subject of the data
- Consider:
 - Meeting notes
 - Reports
 - Correspondence about an official activity
- Some “personal” data

62

Personal data

- Data on an employee’s personal matters, unrelated to job duties or operation of government.
 - Government data?
 - Policy for incidental use
- Advisory opinions 01-075, 02-049

63

What do you think: Contracts

The County has signed a contract with the county administrator.

A member of the public would like a copy of the contract.

Can the requester have it?



64

Public personnel data includes §13.43, subd. 2

- Name
- Actual gross salary
- Terms and conditions of employment
- Value and nature of employer paid fringe benefits
- Basis amount of added remuneration, including expense reimbursement
- Education and training background and previous work experience

65

Public personnel data, cont.

- Work location and a work telephone number
- Work-related continuing education
- Payroll time sheets *or* other comparable data that are *only used* to account for employee's work time for payroll purposes
 - Except if disclosure would reveal the employee's *reasons* for the use of sick or other medical leave or other not public data

66

Public complaint and disciplinary data

- Existence and status of complaints or charges, regardless of disciplinary action
- Final disposition of any disciplinary action plus the specific reasons for and data documenting the basis of the action
- Complete terms of any agreement settling any dispute arising out of an employment relationship, including a buyout agreement
 - The agreement must include specific reasons for the agreement if more than \$10,000

67

Public disciplinary data – local public officials

- Chief administrative office, three highest paid employees, managers; chiefs; heads or directors of departments, divisions, bureaus, or boards
- “All data” become public if they
 - Resign while complaint is pending
 - Are terminated while complaint is pending
 - Are disciplined
 - Settle and releases employer for liability related to the complaint or charge
- Employee witness IDs remain private

68

What is disciplinary action?

- Some entity discretion: entity HR policies and review collective bargaining agreements.
- *Minnesota Coalition on Government Information vs. City of Minneapolis, et al.*, No A25-0919 (Minn. App. May 18, 2026), nonprecedential.
 - An action imposed by the MPD to punish, penalize, or correct behavior in response to a complaint or charge against the employee, consistent with the rights and obligations as established by PELRA.
 - Minneapolis has petitioned the Supreme Court for review

69

Advisory opinions – personnel data

- 97-049: Employee work email address is public as part of work location.
- 04-017: Dollar value of employee's health insurance benefit is public as "fringe benefit."
- 08-029: Added remuneration, outside income unrelated to employment are private personnel data.
- 13-002: Requester entitled to redacted application and supplement.
- 21-005: Work-sponsored training that offers continuing education credits and other benefits is "work-related continuing education."

70

Data on applicants

§13.43, subd. 3

- Everything is private except:
 - Veteran status
 - Relevant test scores
 - Rank on eligible list
 - Job history
 - Education and training
 - Work availability
- Names are private until a finalist
 - Finalist = selected for interview by appointing authority



71

Elected officials

- Entity determines whether they are employees
 - *Krout v. City of Greenfield*, A11-1200, (Minn. App. April 16, 2012), nonprecedential
 - Advisory Opinions 26-003 (citing 5 other opinions)
 - Document decision – resolution, bylaw, memo
- If no determination, data about them data are presumptively public
- Exception in Minn. Stat. §13.601
 - Correspondence with individual constituents is private
 - Required financial disclosures are public

72

What do you think: Personal devices

A Government employee sends a work-related email from their personal email address on their phone.

- Are the data on their personal email account and/or phone government data?



73

What do you think: Personal devices - answer

- Employees can create government data on personal devices
- Employers might consider:
 - Policy on compliance with records retention and data requests
 - Policy on usage



74

4-Part webinar series on personnel data

- [Webinar series](#)
 1. Introduction to personnel data
 2. Sharing personnel data
 3. Complaints and discipline
 4. Recap

75



Redaction exercise

Small group discussion
Handouts

76

Redaction

- Separate responsive data from those data not accessible
- At the data element level
- Identity can be more than a name
- Provide specific citation in support of redaction
 - At data element level or at document level?

77



Afternoon break

78

Data Challenges and Appeals

Minnesota Statutes, section 13.04, subd. 4 & Minnesota Rule 1205.1600

79

Challenging the accuracy and completeness of data

- Data subjects have the right to challenge the accuracy and completeness of data about themselves.
- Data being challenged must be:
 - Public or private
 - About the person submitting the challenge (or minor child)
- The data challenge itself must be:
 - In writing
 - Addressed to the Responsible Authority

80

What do you need to do when you receive a data challenge?

- RA must respond within 30 days by:
 - Correcting data that are inaccurate/incomplete and notify past recipients of the inaccurate/incomplete data OR
 - Notifying the data subject that the data are accurate and complete, and their right to appeal
 - Disputed data can only be disclosed if a statement of disagreement is included with the data

81

Data challenge appeals

- Data subject can appeal to the Commissioner of Administration
- A complete appeal that is not resolved through informal resolution is set for a contested case hearing
 - Entity pays for hearing
- Commissioner may dismiss appeal if it is not timely, data was presented as evidence in court, or appellant is not the data subject.

82



Data Breaches

83

Data Breaches

(Minn. Stat. § 13.055)

- Statute defines “breach of the security of the data”
 - Unauthorized acquisition by an unauthorized person that compromises security and classification of data
 - Unauthorized acquisition = obtained, accessed, or viewed data with **intent** to use data for nongovernmental purposes
 - Unauthorized person = any person who accesses data without a work assignment



84

When has there been a data breach?

- There has been a breach that generally triggers a notice under section 13.055 when ALL of the following apply:
 - A person,
 - Views or takes private or confidential data,
 - Without permission or statutory authority, and
 - With the intent to use the private or confidential data for nongovernmental purposes

85

What should a breach notice look like?

- In writing
- Inform the individual that a report will be prepared about the breach investigation
- State that an individual may request a copy of the report by mail or email
- Sent without unreasonable delay

86

How must an entity provide notice?

- First class mail or electronic notice
- Substitute notice is an option if:
 - Cost of written notice exceeds \$250,000 or the group exceeds 500,000, or
 - Entity does not have sufficient contact information
- Substitute notice must include:
 - Email notice if the entity has an email address for affected individuals
 - Post the notice on the website of the entity, if the entity maintains a website
 - Provide notification to major media outlets within the entity's jurisdiction
- Entity must notify consumer reporting agencies if a breach requires notification to more than 1,000 individuals

87

What type of report is required following a breach investigation?

- Entity must complete an investigation and prepare a report, including facts and the results of the investigation
- If the breach involved unauthorized access by an employee, the report must include:
 - Description of the data that were accessed or acquired
 - Number of individuals affected
- If there is a final disposition of disciplinary action against an employee, the report must include:
 - Name of each responsible employee
 - Final disposition of discipline taken in response

88

Data breach annual security assessment

- Yearly security assessment of any personal information entity maintains
- “Personal information” is an individual's first name or first initial and last name in combination with one or more of these elements when unencrypted:
 - Social security number
 - Driver's license number or Minnesota ID card number
 - Account number or credit/debit card number in combination with the security code, access code, or password
- Security assessment will vary depending on personal information maintained

89

Data breaches?

	Corrective Action	13.055 Notice
Accidentally accesses not public database	Yes	No
Incorrectly types email address and sends not public data to wrong government employee	Yes	No
Inadvertently reads report with not public data without appropriate work assignment	Yes	No
Looks up driver’s license data about new neighbor without appropriate work assignment	Yes	Yes

90

Cybersecurity incidents

(Minn. Stat. §16E.36)

<https://mn.gov/mnit/about-mnit/security/cir/>

- Requires notification of any cybersecurity incidents to MNIT. New requirement beginning Dec. 1, 2024
- Applies to all public agencies
- Cybersecurity incident
 - An action taken through the use of an information system or network
 - That results in an actual or potentially adverse effect on an information system, network, or information residing therein

91



Scenarios

Small group discussion

92



Contact DPO

651-296-6733
info.dpo@state.mn.us
<https://mn.gov/admin/data-practices/>
YouTube training videos: user/infoipad

93
