MINNESOTA Management &Budget

Data Practices for Personnel Records

A guide for human resource staff

12/7/2015

Table of Contents

Introduction

All state agency human resource staff must be aware of the classification (public or not public) of personnel data, and of their obligation to comply with the Minnesota Government Data Practices Act requirements concerning the collection and disclosure of that data.

This document is a reference to help agencies follow data practices requirements for personnel records when:

- Accessing not public personnel data
- Responding to data requests
- Developing policies and procedures related to collection, maintenance, dissemination, and access to personnel data

If you have questions, please consult with your agency Data Practices Compliance Official, or Enterprise Employment Law Counsel or the Research, Policies, and Projects team at Minnesota Management and Budget (MMB).

What is the Minnesota Government Data Practices Act?

The Minnesota Government Data Practices Act (MGDPA) governs access to data that is collected, created, stored, maintained or disseminated by state agencies, including personnel data (M.S. Chapter 13). It balances:

- The individual's concern for privacy
- The public's interest in knowing about their government
- The government's need to have or use data to do its work

Quick Tips: Responding to Data Requests for Personnel Data

1. Before responding to a data request that includes personnel data, carefully consider the classification of the data requested.
2. Consult with your Data Practices Compliance Official or MMB before releasing data.
3. Be cautious. You can always release additional data later, but you can never take back what you have released.
4. Do not provide more data than has actually been requested. For example, if you receive a request for public data contained in the "personnel file," do not include data outside of the personnel file such as settlements, arbitration awards, or disciplinary records that have been removed from the personnel file due to labor contract provisions.
5. If the requestor asks for all public data on an individual under M.S. 13.43, all public data that exists, regardless of where it is maintained, must be released.
6. If the data request is accompanied by a written, informed consent signed by the data subject, the data disseminated to the requestor should include only the items covered in the signed consent form, and nothing else.
7. Before supplying data even in response to a request that includes an informed consent, be sure that the data is not designated as confidential by some other provision, for example, civil investigatory data, and be sure that the data does not include private or confidential data on persons other than the individual who has given informed consent.

What is Personnel Data?

To understand personnel data, it is important to first understand government data.

Government data are all data collected, created, received, maintained, or disseminated by any government entity, regardless of its physical form, storage media, or conditions of use. This includes, but is not limited to, paper records and files, microfilm, electronic documents, or other materials.

Government data include data on individuals. Data on individuals are all government data in which any individual is or can be identified as the subject of the data. This does not include data in which the appearance of a name or other identifying information can be clearly demonstrated to be only incidental to the data, and the data are not accessed by the name or other identifying information of any individual. It also does not include summary data, which are statistical records and reports derived from data on individuals, but in which individuals are not identified and from which neither individual identities nor any other characteristic that could uniquely identify an individual is ascertainable.

Data on individuals may be:

- Public – accessible by anyone
- Private – not accessible to the public; accessible only to the subject of the data, the subject's personal representative, and others authorized by law
- Confidential – not accessible to the public; not accessible to the subject of the data or the subject's personal representative; accessible only to those authorized by law

Personnel data is government data on individuals maintained because the individual is or was an employee, applicant, volunteer, or an independent contractor for a government entity (M.S. 13.43, subd. 1).

In order for data to be personnel data, it must be:

- Data about an individual, and
- The individual must be the subject of the data.

Personnel data is generally presumed to be *private*. Only personnel data that is expressly listed as *public* in statute is accessible by the public. Some data about employees, applicants, volunteers and independent contractors may be confidential (such as active investigative data) and are accessible only to those authorized by law.

Public Personnel Data

Public personnel data is available to the public under statute. There are three categories:

- Public data on applicants for state employment
- Public data on current and former employees, volunteers and independent contractors
- Public data on appointed officials

What personnel data on applicants for state employment are public?

- Veteran status
- Relevant test scores
- Rank on eligible list
- Job history
- Education and training
- Work availability
- ONLY when the applicant is considered a finalist by the appointing authority, the applicant's name is public. A finalist is an individual who is selected to be interviewed by the appointing authority prior to selection. **Prior to an applicant becoming a finalist, the applicant's name is private data**.

Source: (M.S. 13.43, subd. 3).

What data on current and former employees, volunteers, and independent contractors are public?

- Name
- Employee identification number, which must not be the employee's social security number
- Actual gross salary
- Salary range, including hourly, monthly, and yearly maximums and minimums and steps
- Terms and conditions of employment relationship, including terms and conditions outlined in the job offer, collective bargaining agreement or plan
- Contract fees, including compensation, reimbursement for travel and subsistence expenses, total state obligation for compensation and reimbursement, and terms of payment
- Actual gross pension, which is the benefit amount(s) actually paid after retirement (information which is available only from the applicable retirement system)
- The value and nature of employer paid fringe benefits, including vacation and sick leave, holidays, state-paid premium for health, life, and dental insurance, and state-paid contribution to retirement fund
- The basis for and the amount of any added remuneration, which may include merit increases, overtime pay, work-out-of-class pay, travel expenses, training costs, parking, housing, and achievement awards, in addition to salary
- Job title and bargaining unit, including working title and class title
- Job description
- Education and training background, including location and type
- Previous work experience, including dates, location, and type
- Date of first and last employment by the state agency
- The existence and status ONLY of any complaints or charges against the employee, regardless of whether the complaint or charge resulted in a disciplinary action (more details on page 11)

- The final disposition of any disciplinary action together with the specific reasons for the action and data documenting the basis of the action, excluding data that would identify confidential sources who are employees of the state agency (more details beginning on page 13)
- The complete terms of any agreement settling any dispute arising out of an employment relationship, except that the agreement must include specific reasons for the agreement if it involves the payment of more than $10,000 of public money. This includes grievance settlement agreements and any agreements settling legal claims.
- Work location, including address of work location and state email address (note that if the primary work location is a home address, the home address remains private data)
- Work telephone number (note that if the primary work location is home, the personal telephone number remains private data)
- Badge number
- Work-related continuing education
- Honors and awards received during employment by the state agency, including achievement awards, length of service awards
- Payroll time sheets or other comparable data that are only used to account for the employee's work time for payroll purposes, except data that would reveal the employee's reasons for the use of sick or other medical leave, or other not public data

Source: (M.S. 13.43, subd. 2)

What data regarding applicants for appointment to a public body are public?

The following data on individuals who apply for appointment as a member of a state board, commission, or council are public:

- Name
- City of residence, except when the appointment has a residency requirement that requires the entire address to be public
- Volunteer work
- Awards and honors
- Employment history
- Education and training
- Prior government service
- Veteran status
- Any data required to be provided or that are voluntarily provided in an application for appointment to a state board, commission or council

When the individual is appointed to the state board, commission, or council, additional data becomes public:

- Residential address
- Telephone number or email address where the appointee can be reached, or both at the request of the appointee

- Any telephone number or email address provided by the public body for use of the appointee (this can be the designated telephone number or email address where the appointee can be reached)
- First and last dates of service on the public body
- Existence and status of any complaints or charges against an appointee
- Upon completion of an investigation of a complaint or charge against an appointee, the final investigative report is public, unless access to the data would jeopardize an active investigation

Source: (M.S. 13.601, subd. 3. Additional data are published in a report by the Secretary of State under M.S. 15.0597, subds. 2, 3).

Special Rules For Certain Personnel Data That Is Normally Public

There are some special rules that apply to the public personnel data listed above.

Undercover Law Enforcement Officers (M.S. 13.43, subd. 5)

All personnel data related to an individual employed as or an applicant for employment as an undercover law enforcement officer are private. When the individual is no longer assigned to an undercover position, the relevant personnel data become public unless the law enforcement agency decides that disclosing the data would threaten the officer's personal safety or jeopardize an active investigation.

Employees of Secure Facilities (M.S. 13.43, subd. 5a)

WHO THE DATA RELATES TO	RESTRICTIONS ON RELEASE OF DATA	WHAT DATA
• Employees of a secure treatment facility • Employees of a state correctional facility, or • Employees of the Department of Corrections directly involved in supervision of offenders in the community	Do not disclose to: • Facility patients or corrections inmates • Other individuals who facility or correction administrators reasonably believe will use the information to harass, intimidate, or assault any of these employees	• Place where previous education or training occurred • Place of prior employment • Payroll timesheets or other comparable data, to the extent that disclosure may reveal future work assignments, home address or telephone number, the location of an employee during non-work hours, or the location of an employee's immediate family members

Statewide Retirement Systems Data (M.S. 13.43, subd. 2a)

Statewide retirement systems that collect and maintain public data on members, survivors, and beneficiaries may only be required to disclose the name, gross pension, and type of benefit awarded, except as required by law.

Private Personnel Data

Personnel data that is not specifically listed in state or federal law as public is considered private. Private personnel data includes, *but is not limited to* (this list is NOT exhaustive):

- Performance reviews
- Performance improvement plans
- Supervisor notes
- Medical documentation
- Home address, personal phone numbers, and personal email addresses
- Data related to an employee's dependents (M.S. 13.43, subd. 4)
- All data created, collected or maintained by a government entity to administer employee assistance programs (M.S. 13.43, subd. 7)
- Data acquired by a peer group member in a public safety peer counseling debriefing (M.S. 13.43, subd. 9)
- The following data gathered as a result of a contractual relationship entered into on or after August 1, 2012: the personal telephone number, home address, and email address of a current or former employee of the contractor or subcontractor. (M.S. 13.43, subd. 19)

Who can access private personnel data?

When accessing personnel data, it is very important to understand the classification of the data. Private personnel data may only be accessed by authorized individuals. Please review HR/LR Policy #1429, Data Protection Policy for Human Resource Systems, for additional information regarding accessing private data.

Private personnel data may be accessed by:

- The subject of the data
- Agency employees with a work assignment that reasonably requires access
- Persons or entities given access by the express written direction of the subject of the data (informed consent)
- Persons or entities authorized by law to receive the data

Without authorization, private personnel data cannot be shared with anyone else! This includes:

- The complainant in an investigation
- Third parties, including the press and references
- Agency employees without a work assignment reasonably requiring access
- Other state agencies without explicit statutory authority

The Subject of the Data

The subject of the private data has access to his or her own data. If the data contain information about multiple subjects, the private or confidential data of other individuals must be redacted (removed) before the data are available to the requestor.

Under M.S. 13.43, subd. 8, an employee does not have access to data that would identify the complainant or other witnesses to allegations of harassment against the employee, if access to the information would threaten the safety of the complainant or witnesses, or subject the complainant or witnesses to harassment. However, the data may be released to the employee if it is necessary for the employee to prepare for a disciplinary proceeding.

Agency Employees

Agency employees may access, acquire, view, or use private data only when the employee is reasonably required to do so in order to accomplish a work assignment or to satisfy the employee's job duties (M.S. 13.05, subd. 5; Minn. Rules 1205.0400). The data may be used only for the purpose of the work assignment and not for personal use or inquiry.

Persons or Entities Authorized by the Data Subject

Private personnel data may be disseminated to persons or entities as expressly authorized by the data subject. The data subject must provide written, informed consent from the data subject allowing the person or entity to access the data (M.S. 13.05, subd. 4(d)).

Informed consent means the subject of private data has agreed, in writing, to disclosure in accordance with the requirements of M.S. 13.05, subd. 4, and appreciates the consequences of allowing the entity to initiate a new purpose or use of the data in question (Minn. Rules 1205.1400, subp. 4).

A valid informed consent must:

- Be voluntary and not coerced
- Be in writing
- Explain why the new use or release is necessary
- Include any known consequences for giving informed consent

Persons or Entities Authorized by Law

Agencies may release private personnel data to individuals or entities authorized by law to access the data. These persons or entities include, but are not limited to:

- Those permitted access by a court order signed by a judge or arbitrator (M.S. 13.03, subd. 6; 13.43, subd. 4) (not a court subpoena (see Minn. R. 1205.0100, subp. 5))
- Department of Employment and Economic Development (DEED), to administer unemployment benefits (M.S. 13.43, subd. 13)
- Department of Administration, to administer the workers' compensation program (M.S. 13.43, subd. 18)

- Labor unions, to the extent the agency determines that the release is necessary to enable the union to conduct elections, notify employees of fair share fee assessments, or to implement Chapter 179A (M.S. 13.43, subd. 6) (more details on page 12)
- Law enforcement, to report a crime or aid in the investigation of a crime (M.S. 13.43, subd. 15)
- Licensing authorities, for example, mandatory reporting of discipline to the Board of Nursing (M.S. 148.263)
- Minnesota Management and Budget has access to all public and private personnel data kept by appointing authorities that will aid in the discharge of the MMB commissioner's duties (M.S. 43A.04, subd. 1(b))
- Office of the Legislative Auditor, when the agency obtains information indicating that public funds or resources may have been used unlawfully, or that private or confidential data may have been accessed or used unlawfully (M.S. 3.971)

Emergencies may also necessitate the release of private personnel data. Personal home contact information may be used or shared with other government entities to contact an employee in the event of an emergency or disruption affecting the continuity of operations (M.S. 13.43, subd. 17). Additionally, an agency may release private personnel data if the agency determines that doing so is necessary to protect the employee from harm to self or to protect another person who may be harmed by the employee (M.S. 13.43, subd. 11). Only data that are relevant to the safety concerns may be released. The data may only be released to the person who may be harmed or to his or her attorney, to a prepetition team conducting an investigation, or to a court, law enforcement agency, or prosecuting authority.

Other entities may have access to private personnel data, including licensing authorities and enforcement agencies. If you have questions regarding who may have access to private personnel data, please contact your Data Practices Compliance Official or MMB.

Confidential Data

Some data about employees, applicants, volunteers and independent contractors may be confidential data. Confidential data have the most protection. This data is not available to the public or to the subject of the data. It is only accessible to agency employees who have a work assignment that reasonably requires access, or to those permitted access under law or court order.

Civil Investigations

Under M.S. 13.39, data collected as part of an active investigation related to a pending civil legal action are confidential. Only the chief attorney acting for the government entity can determine whether a civil legal action is pending. A pending civil legal action includes, but is not limited to, judicial, administrative or arbitration proceedings.

Civil investigative data may be released to the following individuals or entities:

- Any person, agency, or the public if the applicable government entity determines that the access will aid the law enforcement process, promote public health or safety, or dispel widespread rumor or unrest (M.S. 13.39, subd. 2(a))
- A complainant has access to the statement provided by the complainant to a government entity as part of the active investigation (M.S. 13.39, subd. 2(b)); this does not include an investigator's notes or interview summary
- Under a court order authorizing the release of the data (M.S. 13.39, subd. 2a) (not a court subpoena (see Minn. R. 1205.0100, subp. 5))

Any civil investigative data presented as evidence in court or made part of a court record are public.

Inactive civil investigative data are public, unless the release of the data would jeopardize another pending civil legal action, and except for those portions of a civil investigative file that continue to be classified as not public under law.

Civil investigative data become inactive upon the occurrence of any of the following events:

- A decision by the government entity or by the chief attorney acting for the government entity not to pursue the civil action
- Expiration of the time to file a complaint under the statute of limitations or agreement applicable to the civil action
- Exhaustion of or expiration of rights of appeal by either party to the civil action

Data determined to be inactive may become active again if the government entity or its chief attorney decides to renew the civil action. Data which become active again are reclassified as confidential.

Additional data classified as confidential include:

- Data on a decedent which was private or confidential prior to death remains private or confidential, respectively, following death (M.S. 13.10)
- Licensing agency data which relate to the investigation of complaints against any licensee (M.S. 13.41, subd. 4)

- Data that is protected by the attorney-client privilege and/or attorney work-product doctrine, are not government data subject to the MGDPA. As a result, disclosure is governed by statutes, rules, and professional standards applicable to such privilege and doctrine.

Please note that this list is not exhaustive and other data may be classified as confidential or private under statute. If you have any questions about whether data is confidential or private, please contact your Data Practices Compliance Official or MMB.

Data Breaches

A data breach, as defined in M.S. 13.055, is the acquisition of private or confidential data without informed consent or statutory authority, with the intent to use the data for a nongovernmental purpose. This compromises the security of the data. There is an exception for the good faith acquisition of private or confidential data for state agency purposes, as long as the data is not provided to or viewable by an unauthorized person.

Under M.S. 13.055, if a data breach occurs, the agency must:

- Provide timely written notice to the subject of the data whose private or confidential data was, or is reasonably believed to have been, acquired by an unauthorized person (see M.S. 13.055 for specific notice requirements)
- Notify consumer reporting agencies if the data of more than 1,000 individuals at one time is breached

Under M.S. 3.971, subd. 9, the agency must notify the Office of the Legislative Auditor when it obtains information indicating that private or confidential data may have been accessed or used unlawfully.

Complaint and Disciplinary Data, Grievance Settlements, and Arbitration Awards

This section will discuss the public or private nature of personnel data related to complaints of employee misconduct, employee misconduct investigations, discipline, grievance settlements, and arbitration awards.

Data Related to Complaints

When complaints or charges of misconduct are made against a state employee, during the time the appointing authority is investigating the allegations, **ONLY** the following information is publicly available:

- Existence of a complaint: a government entity can disclose that a complaint
  - *Exists*; or
  - *Does not exist*
- Status of a complaint: If a complaint exists, a government entity can disclose the status as:
  - Complaint received
  - Pending
  - Under investigation
  - Resolved/completed/closed

All other information related to the complaint is private, including the nature, type, or character of the complaint, and whether investigatory leave was imposed.

A complainant has access to the statement that he or she provided to the agency in connection with a complaint or charge against an employee (M.S. 13.43, subd. 2(d)). Please note that an investigator's notes or interview summaries do not constitute the complainant's statement and should not be released to the complainant.

At the close of the investigation, if no discipline is imposed, no additional data will become public; only the existence and status of the complaint (as described above) will be public data. All other data related to the complaint and the investigation remain private data.

If discipline is imposed, please review the information below regarding "disciplinary data".

If sending a letter to the complainant following the investigation, remember that the letter may not include any private data on the subject of the complaint. This means that if there is no final disposition of disciplinary action (discussed further below), the letter may only contain information about the existence and status of the complaint.

Tennessen Notices During Investigations (M.S. 13.04, subd. 2)

A Tennessen notice is required whenever an individual is asked to supply private or confidential data about themselves. The subject of a complaint must receive a Tennessen notice at the beginning of any investigatory interview.

Agencies are encouraged to provide a Tennessen notice to witnesses at the beginning of an investigatory interview, since the witness may volunteer private or confidential data about himself or herself during the interview (including, but not limited to, personnel data on the witness or medical data about the witness).

Sample investigation notices are available on the MMB website.

Disciplinary Data

Access by Labor Unions (M.S. 13.43, subd. 6)

An agency may disseminate private personnel data to a labor organization representing the subject of discipline if the agency determines that the data is necessary for the union to process a grievance and/or arbitration resulting from the discipline. M.S. 13.43, subd. 6. Disclosure of data to the union usually takes place after the union has filed the grievance at Step 2 at the agency level or has filed for arbitration of the grievance. Agencies may agree to disclose data to the union earlier in the grievance process, but should first consult with the MMB Labor Relations Office.

Depending on the seriousness of the case and the amount and type of data involved, the agency may request the union to agree to a stipulation describing who has access to the data and the penalties if the data are released contrary to the provisions of the stipulation.

If the agency withholds information on the basis of a provision in the MGDPA or other statute, the agency must provide to the labor representative, in writing, the specific statutory section upon which the denial is based.

Final Disposition of Disciplinary Action

The final disposition of disciplinary action is public personnel data.

The definition of "final disposition" will vary depending on whether the employee is a member of a union.

- If the employee is a member of a labor union, the final disposition of a disciplinary action occurs at the end of an arbitration sustaining the discipline, or, upon the employee's failure to elect arbitration within the time provided by the collective bargaining agreement.
- If the employee is not a member of a labor union, the final disposition occurs when the employer makes its final decision about disciplinary action, regardless of the possibility of later proceedings.

If no discipline is imposed following an investigation, then **no additional data** become public. This means that **only** the existence and status of the complaint are public data.

If discipline is imposed, **before** there is final disposition of disciplinary action, **only** the existence and status of the complaint are public data.

ONLY upon the final disposition of a disciplinary action, the following data become public:

- Nature of discipline
- Specific reasons for the discipline
- Data documenting the basis for the discipline (excluding data that would identify confidential sources who are employees of the agency)

For both unionized and non-unionized employees, final disposition can include a resignation *under specific circumstances*: If the resignation occurs **after** the final decision of the arbitrator sustaining the discipline (for unionized employees) or **after** the final decision of the employer (for non-unionized employees), then the final disposition includes the resignation, and the data discussed above are public. If the resignation occurs **before** a final decision, however, then there is no final disposition of disciplinary action, and the above data are not public.

If a grievance settlement or arbitration award results in all aspects of the disciplinary action being reversed, then data about the disciplinary action does not become public.

When sending a disciplinary letter to the subject of the investigation, remember that the letter cannot contain any private or confidential data about the complainant, witnesses, or anyone other than the subject of the investigation.

What if a complaint or charge is made against a public official?

The release of data related to complaints or charges against public officials is treated differently.

A state public official is defined under M.S. 13.43, subd. 2(e) as:

- The head of a state agency and deputy and assistant state agency heads
- Members of boards or commissions required by law to be appointed by the governor or other elective officers
- Executive or administrative heads of state departments, bureaus, divisions, or institutions

All data relating to a complaint or charge against a state public official are public in the following circumstances:

- **Upon completion** of the investigation (*but not before*), regardless of whether or not the complaint is substantiated or the public official receives discipline
- If the public official resigns or is terminated while the complaint or charge is pending

The agency may decide not to disclose data if it determines that disclosure of that data would jeopardize an active investigation or reveal confidential sources. In addition, this provision does not authorize release of data that is made not public under other law (*e.g.*, civil investigative data or attorney-client privileged data).

How should I store data related to employee discipline?

Grievance settlements, arbitration awards, and employment-related lawsuit documentation are to be retained in a location other than the employee's personnel file; for example, a grievance file.

Disciplinary data is often recorded in the employee's personnel file. If necessary, personnel records must be revised to accurately reflect the terms of a grievance settlement or an arbitration award whenever the grievance settlement or arbitration award rescinds or reverses all, or a part of, disciplinary action.

If discipline is reversed pursuant to an arbitration award, records of the reversed disciplinary action (such as the discipline letter) must be removed from:

- The SEMA4 record
- The personnel file
- Any other file containing a record of the reversed disciplinary action, such as the supervisory file or disciplinary log. This does not apply to grievance files.

No comments should be added to the personnel record or SEMA4 record that would indicate why the record was revised or what the previous record contained.

State agencies are responsible for making such revisions to an employee's personnel records, including the SEMA4 record.

If discipline is rescinded pursuant to a grievance settlement, agencies must revise records according to the terms of the grievance settlement. Agencies may retain records of discipline rescinded pursuant to a grievance settlement in their grievance files. If you have questions

regarding the terms of a grievance settlement, please contact your Labor Relations Representative.

Disciplinary Records and Labor Contracts

Several labor contracts contain provisions about removal of disciplinary records from employee personnel files after a certain time period. For example, the MAPE agreement provides for the removal of a written reprimand after one year, when requested by the employee. When such records are removed, they shall be retained in a location separate from the personnel file, for example, a grievance file.

No change to SEMA4 records is made when disciplinary records are removed from a personnel file due to the successful completion of the timelines as described in labor contract provisions.

Disciplinary records classified as public data under M.S. 13.43 and removed from personnel files due to labor contract provisions, and which are not classified as private or confidential under any other provision, continue to be public data regardless of where they are kept. This data must be released if a request is received for "all public data on an individual."

Are logs or records tracking agency disciplinary actions personnel data?

Agencies may maintain a tracking or log of all disciplinary action taken within the agency.

When such logs contain only summary data and do not contain employee names or other information by which the employee can be identified, the log does not constitute a personnel record or a personnel file, nor is it data on individuals. Therefore, it is not governed by the requirements of M.S. 13.43.

If the log does contain employee names, the log is considered data on individuals and must be treated in accordance with the provisions of M.S. 13.43.