



# Minnesota Counties Intergovernmental Trust Resource Briefing

Revised June 2010

## Personnel File Maintenance

### Background

The Minnesota Government Data Practices Act (Minnesota Statute – Chapter 13), hereinafter “Act” applies to all state agencies, political subdivisions and statewide systems. The Act regulates the collection, creation, storage, maintenance, dissemination and access to government data. The public policy behind the Act is to provide the public with access to data that is the basis for, and the product of, governmental decisions. Government data is presumed to be accessible by the public for inspection and copying unless it falls within an exception to the Act created by state or federal law. However, “personnel data” is private data on individuals unless classified as public data.

Minn. Stat. §  
13.01

The Act requires that records containing government data must be kept in such an arrangement and condition as to make them easily accessible for convenient use. This Resource Briefing is intended to assist in the identification, classification, storage and dissemination of personnel data for purposes of the Act.

Minn. Stat. §  
13.03, subd. 1

### Data Classifications

The Act defines data on individuals as:

*“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.”*

Minn. Stat. §  
13.02, subd. 5

The Act classifies personnel data as public, private, or confidential, depending upon its characteristics. Personnel data under the Act is defined as:

*“Data on individuals collected because the individual is or was an employee of or an applicant for employment by, performs services on a voluntary basis for, or acts as an independent contractor with a government entity. Personnel data includes data submitted by an employee to a government entity as part of an organized self-evaluation effort by the government entity to request suggestions from all*

Minn. Stat. §  
13.43, subd. 1

*employees on ways to cut costs, make government more efficient, or improve the operation of government. An employee who is identified in a suggestion shall have access to all data in the suggestion except the identity of the employee making the suggestion.*

## Public Personnel Data

Public personnel data is accessible to anyone and includes the following:

### Personal information

- name
- education and training background
- previous work experience

Minn. Stat. §  
13.43, subd. 2

### Compensation-Related Information

- actual gross salary
- salary range – includes salary amounts before deductions
- contract fees, including:
  - compensation
  - reimbursement for travel and subsistence expenses
  - total government unit obligation for compensation and reimbursement
  - terms of payment
- actual gross pension
- value and nature of employer fringe benefits, including:
  - vacation and sick leave
  - holidays
  - government paid portion of insurance premiums
  - government portion of retirement fund contribution
- the basis for and the amount of any added remuneration to salary, to include:
  - travel expenses
  - training costs
  - parking
  - housing and monetary or other awards
  - other expense reimbursement
- payroll time sheets or other comparable data that are only used to account for the employee's work time for payroll purposes. Information on the time sheets that reveal the employee's reasons for use of sick or other medical leave is not public.
- financial disclosure statements of elected or appointed officials

## Work and Performance Information

- job title—including working title and classification title
- employee identification number (must not be social security number)
- job description—including position description and description used for job posting
- bargaining unit
- date of first and last day of employment (with the governmental unit)
- work location, including e-mail address
- work telephone number
- badge number
- honors and awards received (during government employment only)
- long distance telephone billing records of employee
- existence and status of any complaints or charges against the employee, including the employee's name, whether or not the complaint or charge resulted in disciplinary action, exclusive of data describing the nature of the complaint or charge
- the terms of any agreement settling any dispute arising out of the employment relationship, including a buy out agreement as defined in Minn. Stat. §123B.143, subd. 2 paragraph (a). If the agreement includes the payment of more than \$10,000 of public money, the agreement must specify the reason for the agreement
- the final disposition of any disciplinary action together with the specific reasons for the action and data documenting the basis of the action, exclusive of data that would identify confidential sources who are employees of the public entity

Minn. Stat. §  
13.43, subd. 2

Minn. Stat. §  
10.46

## Final Disposition

Final disposition is case specific. Final disposition may depend upon whether or not the employee is covered by a collective bargaining agreement or is a veteran.

*Generally, the following constitutes final disposition when an employee is:*

### Covered by a Collective Bargaining Agreement

Occurs at the conclusion of the arbitration proceedings, or upon failure of the employee to timely elect arbitration when the arbitrator upholds the need for discipline. Final disposition includes a resignation by an individual when the resignation occurs after the final decision of the government entity or arbitrator.

### Not Covered by a Collective Bargaining Agreement

Occurs when the governmental entity makes its final decision about the disciplinary action regardless of the possibility of any later proceedings or court proceedings. It would also occur upon the employee's resignation, but only if that resignation occurs after the final decision of the government agency or body.

Minn. Stat. §  
13.43 (b)

## Investigative Data

**Pending Criminal Actions** - Criminal actions and personnel actions must take separate tracks to resolution. Members should consult with the county attorney and/or the county sheriff to determine whether a criminal matter has been concluded. Employee's access to personnel files may be limited since it has the potential to jeopardize an active investigation or reveal confidential sources.

**Inactive Investigative Data** - Civil and criminal investigative data becomes public once the investigation is determined to be inactive (unless it is personnel data and there is no final disposition).

**Civil Investigative Data** - becomes inactive upon the occurrence of any of the following events:

- a decision by the state agency, political subdivision, or statewide system or by the chief attorney acting for the state agency, political subdivision, or statewide system not to pursue the civil action; or
- expiration of the time to file a complaint under the statute of limitations or agreement applicable to the civil action; or
- exhaustion of or expiration of rights of appeal by either party to the civil action.

Minn. Stat. §  
13.39, subd. 3

***Data may become active if government entity's chief attorney decides to renew the civil action.***

**Criminal investigative data** becomes inactive upon the occurrence of any of the following events:

- a decision by the agency or appropriate prosecutorial authority not to pursue the case; or
- expiration of the time to bring a charge or file a complaint under the applicable statute of limitations, or 30 years after the commission of the offense, whichever comes earliest; or
- exhaustion of or expiration of all rights of appeal by a person convicted on the basis of the investigative data.

Minn. Stat. §  
13.82, subd. 7

## Employment Applicant Data

The following information is public:

- veteran status
- relevant test scores
- rank on eligibility list
- job history
- education and training
- work availability

Minn. Stat. §  
13.43, subd. 3

## Public Personnel Data continued

- names of applicants—only the names of “certified applicants” and “finalists” are public

A “certified applicant” has been certified for appointment to a vacancy in the government. A “finalist” is selected to be interviewed by the appointing authority prior to selection.

## Police Excessive Force Complaint Information

Public information includes:

- information identifying complainants in cases of excessive force that are non-pending and noncurrent;
- whether complaints or charges have been filed against individual officers;
- the status of the complaint or charges; and
- the specific reasons for and final disposition of any disciplinary action taken against an officer, together with supporting data.

Actual complaint forms and other data created during an internal investigation regarding use of force by a law enforcement officer are private personnel data unless disciplinary action is taken against the officer.

A complainant has access to his/her statement provided to the government employer in connection with a complaint or charge against an employee.

*Demers v. City of Minneapolis*,  
486 N.W. 2d 828  
(Minn. App.  
1992)

## Licensing Information Maintained by the Licensing Agency

Includes:

- the licensing agency minutes;
- application data on licensees, except non-designated addresses;
- orders for hearing, findings of fact, conclusions of law and specification of the final disciplinary action contained in the record of the disciplinary action;
- the entire record concerning the disciplinary proceeding; where there is a public hearing regarding the disciplinary action;
- if the licensee and the licensing agency agree to resolve a complaint without a hearing, the agreement and the specific reasons; and
- license numbers, license status, continuing education records issued or maintained by the Board of Peace Officer Standards & Training.

Minn. Stat. §  
13.41, subd. 5

If a local government unit has collected this data, it would be private personnel data.

**Summary Data** - Summary data is a report of private or confidential data with all identifiers to the data subject(s) removed. Summary data must be prepared by the public entity upon the written request of any individual if the request is in writing and the cost of preparing the summary data is borne by the requesting person.

Minn. Stat. §  
13.05, subd. 7

## Private Personnel Data

Private personnel data is only accessible to the individual subject of the data and to government officials who are specifically authorized by statute or by the Commissioner of Administration to have access to the data.

Private data should be stored in a location separate from public data. This information must be stored in a secure location preferably in a locked location.

Private data includes, but is not limited to the following information:

**Workers' Compensation Data** - A separate file should be maintained for this information. It should contain all information concerning the workers' compensation matter, including medical reports, health data, billing and payment information, claims material and forms, and legal materials relating to the claim. Information in this file includes:

Minn. Stat. §  
13.714

- name, address, phone number, and social security number of the claimant if the claimant is not a public employee;
- claim number, date of claimed injury, employee's social security number, home phone number, home address, date of birth, sex, and marital status;
- whether claimed injury caused loss of time from work;
- whether the employee lost time from work on the day of the claimed injury and the number of hours lost;
- whether the employee has returned to work

## Private Personnel Data continued

- whether full or partial wages were paid for the first day of lost time and the amount paid, time of day, and location where injury occurred;
- whether the injury occurred on the employer's premises;
- the name, address, and phone number of the treating physician or practitioner;
- identification of the hospital where treated;
- nature of the claimed injury or occupational illness;
- part of body affected;
- name or type of object involved in causing the injury;
- nature of injury;
- type of accident;
- description of actions taken to prevent reoccurrence;
- names of coworker witnesses;
- all data collected or created as a result of the investigation of the claim including, but not limited to, physicians' reports;
- other data on the medical condition of the claimant;
- data collected from the claimant's physicians; and
- data collected in interviews of the claimant's employer, coworkers, family members, and neighbors.

Union notification is an additional requirement regarding the handling of workers' compensation data. If a work related injury or death requires a report to the Department of Labor and Industry in accordance with Minn. Stat. §176.231, subd. 1, a copy of the report must be mailed by the employer to the employee's local union. The report must be directed to the union's local office within 48 hours after the public entity receives notice of the occurrence.

Minn. Stat. §  
176.231, subd. 1

**Pre-Employment Testing Data (Non-Physical)** - While test scores and rank on an eligibility list are classified as public data (see above), completed versions of the personnel examinations themselves are classified as private data.

Minn. Stat. §  
13.43, subd. 3

### **Drug and Alcohol Testing Data**

This includes, but is not limited to:

- pre-test acknowledgment forms;
- notices of test results;
- written notices of the right to explain a positive test result; and
- test result information.

Minn. Stat. §  
13.34

Minn. Stat. §  
181.954

Although drug and alcohol testing data must be maintained as private information, the law does provide certain circumstances in which release of the data is permissible. These circumstances are:

Private Personnel Data continued

- disclosure in grievance arbitrations, administrative hearing and judicial proceedings;
- release to the federal government as required by federal law or compliance requirements of a federal government contract; and
- disclosure to a substance abuse treatment facility for purposes of the evaluation or treatment of the employee.

Minn. Stat. §  
181.954, subd. 3

Drug and alcohol testing data may not be used as evidence in a criminal action against an employee or applicant.

Minn. Stat. §  
181.954, subd. 4

**Disciplinary Data** - Prior to a final disposition, the only information that may be released publicly concerning a disciplinary matter is the existence and status of any complaints or charges against the employee.

Minn. Stat. §  
13.43, subd.  
2(a)(4)

The meaning of “existence” and “status” should be interpreted very conservatively. “Existence” and “status” does not permit the release of information regarding the nature of an employee’s misconduct or the type of discipline imposed. It is not until the disciplinary action has reached final disposition that the result of the action, together with the specified reasons for the action and the data documenting the basis of the action, excluding confidential sources, becomes public.

**Health and Medical Data** – This includes but is not limited to data generated by fitness-for-duty testing, information submitted for the purpose of obtaining health insurance, information submitted for purposes of the ADA, FMLA or the Minnesota Human Rights Act (MHRA), and records relating to an employee physical examination, including the results.

**Employee Assistance Data** - This includes but is not limited to any data related to an employee’s participation in an employee assistance program of training, diagnostic, and referral services.

Minn. Stat. §  
13.43, subd. 7

**Peer Counseling Debriefing Data** - This includes but is not limited to data acquired by a peer group member in a group process orientated debriefing session established by any agency providing public safety emergency services that is designed to help a person who has suffered an occupation-related traumatic event begin the process of healing and effectively dealing with posttraumatic stress. Public safety emergency service personnel would include, but not be limited to, peace officers, firefighters, medical emergency persons, and dispatchers.

Minn. Stat. §  
13.43, subd. 9

**Fair Labor Standards Act Complaints** - The identities of individuals who have filed a Fair Labor Standards Act complaint against their employer, as well as the complaint forms themselves are private data.

Minn. Stat. §  
13.79

**Security Information** - Defined as government data, the disclosure of which is likely to substantially jeopardize the security of information, possessions, individuals or property against theft, tampering, improper use, attempted escape, illegal disclosure, trespass, or physical injury. Security information includes but is not limited

Minn. Stat. §  
13.37

to crime prevention, block maps and lists of volunteers who participate in community crime prevention programs and their home addresses and telephone numbers.

**Certain P.O.S.T. Data** - The home addresses of licensees and applicants for licenses and data that identify the state agency, statewide system, or political subdivision that employs a licensed peace officer are private data.

Minn. Stat. §  
13.41, subd. 3

### License Data

This includes:

Minn. Stat. §  
13.41

- data, other than names and designated addresses, submitted by applicants for licenses;
- the identity of complainants who have made reports concerning licensees or applicants which appear in inactive complaint data unless the complainant consents to the disclosure;
- the nature or content of unsubstantiated complaints when the information is not maintained in anticipation of legal action;
- the identity of patients whose medical records are received by any health licensing agency for purposes of review or in anticipation of a contested matter;
- inactive investigative data relating to violations of statutes or rules; and
- the record of any disciplinary proceeding, except as authorized by statute.

**Undercover Law Enforcement Information** - All personnel data relating to an individual employed as or an applicant for employment as an undercover law enforcement officer are private data on the individual. If the individual is no longer assigned to an undercover position, data which would ordinarily be classified as public personnel data, would become publicly available, unless the law enforcement agency determines that revealing the data would threaten the personal safety of the officer or jeopardize an active investigation.

Minn. Stat. §  
13.43, subd. 5

**Excessive Force Complaints Leading to No Disciplinary Action** - Complaint forms and other investigative documents created by a police department's internal affairs division in investigating allegations of use of excessive force or criminal violations by police officers, which allegations were not sustained and did not result in disciplinary action.

**Employment and Training Data** - Data on individuals collected, maintained, used, or disseminated because an individual applies for, is currently enrolled in, or has been enrolled in employment and training programs funded with federal, state, or local resources.

Minn. Stat. §  
13.47

**Social Security Numbers** - This information is private except to the extent that access is specifically authorized by law.

**Department of Administration Data** - A government entity may submit not public data to the commissioner for the purpose of requesting or responding to a person's request for an opinion. Government data submitted to the commissioner by a government entity or copies of government data submitted by other persons have the same classification as the data have when held by the government entity. If the nature

of the opinion is such that the release of the opinion would reveal not public data, the commissioner may issue an opinion using pseudonyms for individuals. Data maintained by the commissioner, in the record of an opinion issued using pseudonyms that would reveal the identities of individuals protected by the use of the pseudonyms, are private data on individuals.

Minn. Stat. §  
13.072, subd. 4

**Public Employees Retirement Association Data** - The following data on individual beneficiaries and survivors of PERA members:

Minn. Stat. §  
13.63, subd. 3

- address;
- birth date;
- direct deposit account number; and
- tax withholding data.

### **Data Regarding Any Complaints, Grievances, or Comments of Which an Employee Is or Was the Subject**

#### **Performance Evaluations**

**Harassment Complaint Data** - Generally speaking, during an investigation, the employee (who is the subject of the investigation) is entitled to all data concerning the allegation including the identity of the complainant(s). When the allegation is of a sexual or harassing nature, however, the employee against whom the allegation is being made may be denied access to this information if the employer determines that access to that data would threaten the personal safety or result in the harassment of the complainant(s). Whenever information is released, the employee must be reminded that any action of retaliation against the complainant(s) is strictly forbidden.

Minn. Stat. §  
13.43, subd. 8

When a disciplinary proceeding is commenced, the employee is entitled to the data as may be necessary for the employee to prepare for the proceeding.

The employer cannot guarantee confidentiality to individuals making a complaint of harassment. The employer is obligated to investigate complaints of harassment.

**Supervisor Files Containing Data Concerning an Individual Employee** - This would include supervisory notes, unofficial files, and personal notes, whether kept on the work premises or not, concerning employees, applicants, volunteers, independent contractors, board or commission members or applicants.

Personnel data specifically not identified as public data by statute are private data.

## **Confidential Personnel Data**

Confidential personnel data is defined as nonpublic data. This data is inaccessible to the public AND to the subject of the data. This type of data is accessible only to

government officials specifically authorized by statute or the Commissioner of Administration to access the data. This data would include:

**Civil Investigative Data** - Comprised of any 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. A civil legal action includes judicial, administrative or arbitration proceedings. Only data affirmatively collected and not passively received is confidential. The chief attorney acting for the state agency, political subdivision or statewide system determines whether a legal action is pending. A complainant has access to a statement provided by the complainant to a government entity.

Minn. Stat. §  
13.39

**Criminal Investigative Data** - This includes data collected or created by a law enforcement agency in order to prepare a case against a person, whether known or unknown, for the commission of a crime or other offense for which the agency has primary investigative responsibility, while the investigation is active.

Minn. Stat. §  
13.82, subd. 7

### **Internal Affairs Investigatory Data**

**Harassment Complaint Data Which Identifies the Complainant or Other Witnesses of the Harassment**

Minn. Stat. §  
13.43, subd. 8

**Active Investigative Data Relating to the Investigation of Complaints Against Any Licensee**

Minn. Stat. §  
13.41, subd. 4

**Attorney-Client Privileged Data and Attorney Work Product**

Minn. Stat. §  
13.393

**Inter-agency dissemination of data** - Data disseminated to other government agencies or subdivisions retains its initial classification unless the government agency is required to reclassify the data pursuant to statute, judicial order or administrative ruling. Should the recipient agency or subdivision re-classify the data upon receipt, that reclassification does not affect the initial classification given the data.

Minn. Stat. §  
13.03, subd. 4

**Data That Is Classified Both Private and Confidential** - Whenever information contains two classifications of data, the requirements for the more restrictive classification applies.

Minn. Stat. §  
13.03, subd. 4(b)

**Protection of the Employee or Others** - If it is determined that the release of personnel data is necessary to protect an employee from harm to self or to protect another person who may be harmed by the employee, private data that are relevant to the concerns for safety may be released.

Minn. Stat. §  
13.43, subd. 11

## **Open Meeting Law**

Public data may be discussed at an open meeting. Non-public (private) data about employees may be discussed at an open meeting if the disclosure relates to a matter within the scope of the public body's authority and is reasonably necessary to conduct the business or agenda item before the public body.

Minn. Stat. §  
13.05, subd. 1

## Open Meeting Law continued

Data discussed at an open meeting retains its original classification. A record of the meeting must be made available to the public. For more detailed information regarding the Open Meeting Law, please see the MCIT Resource Briefing on this matter.

Meetings that **must** be closed when non-public (private or confidential) data are discussed or disclosed, such as:

Minn. Stat. §  
13.05, subd. 2

- active “investigative data” as defined by Minn. Stat. § 13.82, subd. 7
- internal affairs data relating to allegations of law enforcement personnel misconduct
- “preliminary consideration” of disciplinary charges, unless the subject of the charge requests an open meeting
- data identifying alleged victims or reporters of criminal sexual conduct, domestic abuse, or maltreatment of minors or vulnerable adults
- educational data, health data, medical data, welfare data, or mental health data that are not public data under the Data Practices Act

The closed meeting must be taped (except for meetings closed pursuant to the attorney client privilege).

Meetings **may** be closed when non-public (private) data are discussed or disclosed such as:

- personnel evaluations, unless the subject of the evaluation requests the meeting to be open. The subject to be evaluated must be identified by the public body prior to closing the meeting. A summary of the evaluation must then be made available at the next meeting of the public body
- data subject to the attorney-client privilege or which consists of attorney work product
- labor negotiations
- preliminary consideration of charges against an employee
- preliminary considerations of purchase or sale of real or personal property; to review confidential or nonpublic appraisal data
- to receive security briefings and reports; to discuss issues related to security and emergency response procedures

If it is concluded that discipline of any nature may be warranted as a result of those specific charges or allegations, further meetings or hearings relating to those specific charges or allegations held after that conclusion is reached must be open.

## Collection of Government Data

Once recorded, data becomes government data regardless of its physical form, storage media or the conditions of its use. "Data" must be "recorded" in some format for it to become government data.

Minn. Stat. §  
13.02, subd. 7

### Tennessee Warning

Private or confidential data on individual may not be collected, stored, used or disseminated by political subdivisions for any purpose except those stated to the individual at the time of collection, in accordance with statute, with certain limited exceptions.

Minn. Rules  
1205.0200,  
subp. 4

A "Tennessee Warning" or "Right to Know" statement must be administered to the subject of the data at the time of or prior to the collection of private or confidential data of which they are the subject. Such a warning must inform the subject of:

Minn. Stat. §  
13.04, subd. 2

- the purpose and intended use of the data requested;
- whether the individual may refuse to supply or is legally obligated to supply the data;
- any known consequences of supplying or not supplying the data; and
- the identity of other persons authorized to receive the data.

See MCIT March 2010 Bulletin article, "Collecting Performance Evaluation Data from Employees."

## Release and Responses to Requests for Government Data

Requests for information should be made in writing and specifically identify the type of information sought.

**Public Personnel Data** - Members of the public are entitled to inspect and copy public personnel data at reasonable times and places, upon request. A member of the public also has the right to be informed of the meaning of public data.

Minn. Stat. §  
13.03, subd. 3

A request for public personnel data must be complied with as soon as reasonably practicable. Accordingly, the Data Practices Act mandates that the records must be kept in such an arrangement and conditions as to make them easily accessible for convenient use.

Minn. Stat. §  
13.03, subd. 1

**Private Personnel Data** - The subject of the data has the right to inspect and receive copies of the data upon request. The subject of the data also has the right to be informed whether they are the subject of any government personnel data and whether the data is classified as public, private or confidential. Within the public entity, persons whose job duties reasonably require such access may access private personnel data. Access is limited to that which is necessary for the administration and

Minn. Stat. §  
13.02

management of programs specifically authorized by the legislature, the federal government or the local governing body.

**A request for private personnel data by the subject of the data must be complied with within 10 business days of the request** - If the requested data is determined to be classified so as to deny the requesting party access, the requesting party must be informed of the denial and the reasons therefore.

Minn. Stat. §  
13.04, subd. 3

**Confidential Personnel Data** - Confidential data is accessible only to government officials specifically authorized by statute or the Commissioner of Administration to access the data. This data is not accessible to the public or the individual who is the subject of the data.

Minn. Stat. §  
13.02

If the requested data is determined to be classified so as to deny the requesting party access, the requesting party must be informed of that determination orally at the time of the request or in writing as soon after that time as possible and the reason for the denial.

**Data Which Contains Both Public and Nonpublic Data** - An entire document may be withheld under the Act only when public and nonpublic data is so inextricably intertwined that segregation of the material would impose a significant financial burden and leave the remaining part of the document with little information of value. The data must be separated, either by redacting the nonpublic portions or by separating the portions that are not accessible to the public.

*Northwest  
Publishing Inc. v.  
City of  
Bloomington,  
499 N.W. 2d 509  
(Minn. App.  
1988)*

**Denying Access to Data** - If a public entity determines that data is classified such that access must be denied, the public entity must inform the requester of that fact and cite the applicable law classifying the data as private or confidential. Upon request, the public entity must certify in writing that a request for data has been denied with a cite to the applicable law requiring denial of access to the data.

**Reproduction and Fees for Copies of Records** - To a limited extent counties and other public entities have some opportunity to recover their costs for filling data requests. No charge or fee is permitted, if an individual is merely requesting an inspection of data. If copies or electronic transmittals are requested, the responsible authority may charge a fee.

- If the individual requesting copies of the data is the subject of the data, the government entity may only charge the actual cost of copies. **The government entity may not charge to search for and retrieve the data; to separate public and not-public data; to redact private or confidential data about others.**
- If the individual requesting copies of the data is anyone other than the subject of the data, the government entity may charge \$.25 per page if the request is for 100 or fewer, black & white, legal/letter size paper copies. In all other circumstances, the government entity may only charge the actual cost of copies. The entity may require the requesting person to pay the actual costs of searching for and retrieving government data, including the cost of employee time, and for making, certifying, compiling, and electronically transmitting the

copies of the data or the data, but may not charge for separating public from not public data.

When calculating costs for employee time, the cost must be calculated based on the wage/salary (may include benefits) of the lowest-paid entity employee who could have completed the task.

## Maintaining Personnel Government Data

**Central Location** - Personnel data should be kept in a single office. In order to keep convenient and readily accessible records, all data of any kind with respect to an employee should be directed to the employee's general personnel file or special confidential personnel file and medical sub-file. An individual in the public entity should be designated as the record's custodian, whose responsibility it is to see that personnel data gets promptly and accurately placed in the proper personnel file.

**Public Data** - Data which is classified as public is subject to release to anyone who requests the data, therefore, it should be maintained in such a way that it is made readily accessible to any member of the public who requests it.

**Most Private Data** - The vast majority of personnel data is private data, which is inaccessible to the public or to people within the organization who have no legitimate reason to have access to it. Such data is readily accessible by the employee who is the subject of the data. Personnel data, other than health data or confidential data should be placed in a general personnel file that is inaccessible to co-workers and the public, but is accessible to supervisors and others who have a legitimate business reason to review the materials.

**Medical and Health Data** - Employers are required by the ADA and FMLA to keep this data in a file separate from all other personnel data and in a secure location.

**Confidential Data** - This data should be kept in a separate file in a separate locked cabinet from the employee's regular personnel data.

**Segregation of Data by Specific Program or Event** - Data concerning an individual's eligibility for a specific employment related program or benefit should be maintained separately from other personnel data concerning that individual. This would include data concerning eligibility for benefits or preference programs, such as those provided by the Americans with Disabilities Act and the Family Medical Leave Act. Further, data related to or generated by any ongoing investigation or litigation of which the individual is the subject, should be maintained separately in a litigation or investigation file devoted exclusively to the matter.

**Treatment of Data After Employee Death** - Upon the death of an individual, personnel data which had been classified as either private or confidential at the time of death, remains so classified until either 10 years following the individual's death or 30 years following the creation of the material, when it will become public personnel data.

## Challenging Data

The Minnesota Government Data Practices Act provides a specific mechanism to allow an employee to challenge data placed in their personnel file.

Minn. Stat. §  
13.04, subd. 4

The Act provides that an individual who is the subject of public or private data may contest the accuracy or completeness of the data. To exercise this right, the individual employee must notify the public entity in writing of the objection to the data. The public entity then has 30 days to take action. The public entity may:

1. correct the data found to be inaccurate or incomplete and attempt to notify past recipients of inaccurate or incomplete data, including recipients named by the individual; or
2. notify the individual that the public entity believes the data to be correct. Thereafter, data that is a subject of dispute may only be disclosed if the individual subject's statement of disagreement is included with the disclosed data.

The decision of the public entity with respect to allegedly inaccurate or incomplete data may be appealed to the Commissioner of the Department of Administration. Upon receiving such an appeal, the Commissioner must first attempt to resolve the dispute. If the parties consent, the Commissioner may also refer the matter to mediation. Following these efforts, the Commissioner must either dismiss the appeal if resolved or issue an order and notice of hearing.

Data on individuals that is successfully challenged under Minnesota Statutes § 13.04, subd. 4 must be completed, corrected or destroyed by the public entity without regard to the requirements of Minnesota Statutes § 138.17 (Records Retention Law).

After completing, correcting or destroying successfully challenged data, the public entity may retain a copy of the Department of Administration's' order issued under Chapter 14. If no order is issued, the public entity may maintain a summary of the dispute. The summary must not contain any of the particulars of the successfully challenged data.

## Data Security

The Data Practices Act requires the establishment of procedures to assure that all data on individuals is accurate, complete, and current for the purposes for which it was collected and that appropriate safeguards be established to maintain the security of the data.

Minn. Stat. §  
13.05, subd. 5

## Other Records Retention Issues

The maintenance of public records is also regulated by the requirements of the Minnesota Records Retention Act. It provides for the creation of a records management program and a records retention schedule. Public entities are required to treat personnel records in a manner consistent with its individual records management system and schedule.

Minn. Stat. §  
138.17

The Data Practices Act requires the preparation of a public document containing the authority's name, title and address, and a description of each category of record, file, or process relating to private or confidential data on individuals maintained by the authority's state agency, statewide system, or political subdivision. This document is to be updated yearly and may need to be submitted annually (August 1 of each year) to the Commissioner of Administration, along with any forms used to collect private and confidential data.

A county or other public entity that has adopted the Minnesota General Records Retention Schedule or developed its own retention schedule may use this to develop its annual report, thereby eliminating duplicative efforts of identifying and classifying data. In addition, it promotes labeling of nonpublic and protected nonpublic data.

## Conclusion

Personnel data represent a small portion of the information placed in the trust of public entities. Inappropriate or uninformed decisions to release or deny access to information expose the organization to risk. The public entity can mitigate risks associated with the handling of data by identifying a responsible authority to oversee data management, developing policies and procedures for the handling of data, training staff and enforcing established protocols relative to data management. The cost of defending a lawsuit, the erosion of public confidence, poor employee morale and disruption in workflow can accompany a poor decision. The entire entity must be committed to data management. Individuals responsible for the maintenance of personnel files must be offered the opportunity and the tools to perform their jobs in order to safeguard the organization from the consequences of improperly handling information about employees. Contact MCIT for more information on the topic of personnel file management.