INFORMATION MEMO

Data Practices: Analyze, Classify, Respond

Learn your responsibilities under Minnesota's Government Data Practices Act for data your city creates or maintains. Understand how to balance the public's right to know what their government is doing with individuals' right to privacy in government data created and maintained about them, and the city's need to function responsibly and efficiently. Find model resolutions and forms to help you comply with the law.

RELEVANT LINKS:

I. Creation of city data

Government runs on information. Elected and appointed officials make decisions based upon the information they have. Cities rely upon reports, financial projections, and community feedback when establishing:

- License and permit fees.
- Utility rates.
- Employee compensation.
- Budgets.

In turn, cities document their operations. Meeting minutes, ordinances, resolutions, and policies all preserve a record of the decisions made and the basis behind those decisions.

Our reliance on information creates significant responsibilities. Cities and other units of government must:

- Create official records.
- Retain and manage their records.
- Secure and provide access to government data.

This memo focuses on the roles and responsibilities related to the data cities create or maintain.

II. Minnesota's Government Data Practices Act

A. Purpose

Minn. Stat. ch. 13.

The Minnesota Government Data Practices Act (MGDPA) is a series of state laws that attempt to balance the public's right to know what their government is doing, individuals' right to privacy in government data created and maintained about them, and the government's need to function

RELEVANT LINKS:

responsibly and efficiently.

B. Application

Minn. Stat. § 13.01, subd. 3.
Minn. Stat. § 13.02, subds. 7a, 11.

DPO 98-028.
DPO 04-059.
DPO 95-040.

All cities must comply with the MGDPA. The MGDPA also applies to other government units as well as most city-related entities, such as planning commissions, park boards and other advisory boards, Housing and Redevelopment Authorities (HRAs), Economic Development Authorities (EDAs), fire relief associations, city charter commissions, and joint powers entities.

Minn. Stat. § 13.02, subd. 7.

DPO 99-032.

The MGDPA regulates how cities manage government data. Government data is defined as "all data collected, created, received, maintained, or disseminated" by a covered governmental entity "regardless of physical form, storage media, or conditions of use."

DPO 08-024.
DPO 94-026.

The types of data regulated by the MGDPA are not limited to the paper files at city hall, but include computerized files, e-mails, photographs, charts, maps, videotapes, audio tapes - even handwritten notes and working documents.

Navarre v. South Washington County Schools., 652 N.W.2d 9, 25 (Minn. 2002).

The Minnesota Supreme Court has held that even "mental impressions" or spoken comments by governmental officials can be government data if it has derived directly from other government data recorded in physical form.

III. Classifications

The MGDPA divides all government data into three broad classifications: (1) data on individuals, (2) data not on individuals, and (3) data on decedents. These classifications each have three subcategories that determine who can access the data. The following chart sets out the framework for classification and access:

Data On Individuals	**Data Not On Individuals**	**Data On Decedents**	**Who Has Access**
Public	Public	Public	Anyone
Not Public			
Private	Nonpublic	Private	Data subjects and government employees and officials with a business need to know.
Confidential	Protected Nonpublic	Confidential	Only government employees and officials with a business need to know.

RELEVANT LINKS:

Minn. Stat. § 13.02, subd. 8a.

Editorial note: This memo will generally use the term "not public" when addressing one or more of the multiple categories of data classified other than "public" by the MGDPA.

Minn. Stat. § 13.01, subd. 3.

When classifying data, it is important to remember that all government data is presumed to be public unless there is a specific state statute, federal law, or temporary classification that classifies it otherwise. However, with city personnel data the presumption is reversed, and all personnel data is presumed to be private unless a specific state statute or federal law classifies it as public.

Minn. Stat. § 13.43, subds. 2, 4.

See Section VIII-A- *Human resources*.

A. Data on individuals

Minn. Stat. § 13.02, subd. 5.

Minn. R. 1205.0200, subp. 4.

DPO 96-019.

Data on individuals is "all government data in which any individual is or can be identified as the subject of that data, unless the appearance of the name or other identifying data can be clearly demonstrated to be only incidental to the data and the data are not accessed by the name or other identifying data of any individual." An "individual" is defined as a natural person (a living human being). There are three types of data on individuals: public, private, and confidential.

Minn. Stat. § 13.02, subd. 8.

1. Public data

Minn. Stat. § 13.02, subd. 15. Minn. R. 1205.0200, subp. 10.
Minn. Stat. § 13.03, subd. 2.
See Section IV - *City responsibilities*.

"Public data" are anything not classified by state statute, federal law, or temporary classification as either private or confidential. Accessible to anyone for any reason, the city's "responsible authority" is required to establish procedures to facilitate access to public data.

2. Private data

Minn. Stat. § 13.02, subd. 12. Minn. R. 1205.0200, subp. 9.
Minn. R. 1205.0400, subp. 2.

Private data is data on individuals that is expressly classified as private by state statute, federal law, or temporary classification. Private data is not accessible to the public, but may be accessed by:

- The subject of the data.
- Individuals within the city (city officials or employees) whose work assignments reasonably require access.
- Outside entities or agencies that are authorized by state or federal law to access that specific data.
- Entities or individuals given access by the express written direction of the data subject.

Minn. Stat. § 13.05, subd. 4.

Minn. R. 1205.0400, subp. 3.

The responsible authority must establish written procedures that limit access to private data to the appropriate persons.

RELEVANT LINKS:

3. Confidential data

Minn. Stat. § 13.02, subd. 3.
Minn. R. 1205.0200, subp. 3.

Minn. R. 1205.0600, subp. 2.

Confidential data is data on individuals that is expressly classified as confidential by state statute, federal law, or temporary classification. Confidential data is not accessible to the public or the subject of the data. Access is limited to:

- Individuals within the city whose work assignments reasonably require access.
- Outside entities and agencies authorized by state or federal law to access that specific data.

Minn. Stat. § 13.05, subd. 4.

Minn. R. 1205.0600, subp. 3.

Similar to private data, written procedures must be in place to ensure that access to confidential information is limited to the appropriate persons.

B. Data not on individuals

Minn. Stat. § 13.02, subd. 4.
Minn. R. 1205.0200, subp. 8.

Data not on individuals is defined as "all government data that is not data on individuals." This classification includes data on corporations, partnerships, nonprofit organizations or other types of businesses, and other governmental entities. It also includes scientific, studies, or survey data.

DPO 03-014.

There are three types of data not on individuals: public, nonpublic, and protected nonpublic:

Minn. Stat. § 13.02, subd. 14.

Minn. Stat. § 13.02, subd. 9.

Minn. Stat. § 13.02, subd. 13.

- Public data—accessible to anyone for any reason.
- Nonpublic data—accessible to the subject of the data (if there is one, but not accessible to the public).
- Protected nonpublic data—not accessible by either the subject of the data or the public.

C. Data on decedents

Data on decedents is not specifically defined in the MGDPA, but is generally considered to be data related to an individual who is no longer living. There are three types of data on decedents:

Minn. Stat. § 13.02, subd. 15.
Minn. Stat. § 13.10, subd. 1(b).

- Public data—accessible by anyone for any reason.
- Private data—accessible by the representative of the decedent, but not the public.
- Confidential data—not accessible by either the representative of the decedent or by the public.

Minn. Stat. § 13.10, subd. 1(a).

RELEVANT LINKS:

Minn. Stat. § 13.10, subd. 1(c).

The "representative of the decedent" is the personal representative of the estate during the period of administration, or if no personal representative has been appointed (or has been since discharged), the surviving spouse or any child of the decedent. If there is no surviving spouse or child, the parents of the decedent are representatives for purposes of the MGDPA.

Minn. Stat. § 13.10, subd. 2.

Private and confidential data on decedent becomes public 10 years after the actual or presumed death of the individual and 30 years have elapsed from the creation of the data. An individual is presumed dead if 90 years have elapsed since either the creation of the data or the individual's birth, whichever is earlier. Individuals cannot be presumed dead if data indicates they are still alive.

D. Temporary classifications

Minn. Stat. § 13.06, subd. 1.

DPO: Application for Temporary Classification of Government Data.

A city may apply to the commissioner of the Department of Administration to temporarily classify specific data or types of data as not public until a proposed statute can be acted upon by the Legislature. The application for temporary classification is public.

Minn. Stat. § 13.06, subd. 1.

Upon the receipt by the commissioner of an application for temporary classification, the data that is the subject of the application shall be deemed to be classified as set forth in the application for a period of 45 days, or until the application is disapproved, rejected, or granted by the commissioner, whichever is earlier. The commissioner may immediately reject any application inconsistent with the purpose of the temporary classification.

Minn. Stat. § 13.06, subd. 3.

The city bears the burden of proving that there is no other law that prohibits the temporary classification. A city also must prove that other similar data has been classified not public by other government entities, or that public access to the data would render unworkable a program authorized by law. Finally, the city application must clearly establish that a compelling need exists for the immediate temporary classification, which if not granted could adversely affect the health, safety, or welfare of the public, or the data subject's well-being or reputation.

Minn. Stat. § 13.06, subd. 4.

If an application for temporary classification involves data that is reasonably classified in the same manner by all government entities, the commissioner may approve the classification for all similar entities.

E. Changing data classifications

Minn. Stat. § 13.37.

Government data can change classifications in certain circumstances. For example, in the competitive bidding process, sealed bids are nonpublic data but become public once the bids are opened.

RELEVANT LINKS:

Minn. Stat. § 13.03, subd. 4(d).

Minn. Stat. § 13.82, subd. 19.

See Section VIII-C-3-d *Arrest warrant indices.*

Minn. Stat. § 13.03, subd. 9.

Minn. Stat. § 13.591, subd. 3.

Data classifications are also entity specific and may change depending on who is in possession of the data. If one government entity provides data to another, the proper classification for the receiving entity (public or not public data) does not affect the classification for the original entity. For example, an arrest warrant is public when received from the issuing court. But when the warrant is transmitted to and indexed by a local law enforcement agency, the data in the warrant is confidential.

The data remains confidential until the subject of the warrant is taken into custody, served with a warrant, or appears before the court.

Unless expressly provided by a particular statute, the classification of data is determined by the law applicable to the data at the time a request for access is made—regardless of the data's classification at the time it was collected, created, or received. For example, if a city receives a request related to sealed bids before they are opened, the responsible authority must respond to the request and deny access to the data. But, if the same request is made after the bids are opened, the responsible authority could allow access to the data.

IV. City responsibilities

A. Documents and procedures

Cities are required to prepare documents and related procedures to facilitate public access to data and to inventory the private and confidential data maintained. These are often incorporated into one overall document.

1. Public access procedures

Minn. Stat. §13.03, subd. 2.
Minn. Stat. § 13.025.

See Section IV-B-1 *Responsible authority*.

DPO 04-049.

DPO 05-003.

The responsible authority must establish written procedures to ensure that requests for government data are received and responded to promptly and appropriately. The procedures need to be updated no later than Aug. 1 of each year to reflect changes in personnel or other circumstances that might affect public access to government data. This document must be easily accessible (the city must either provide free copies or post it in a conspicuous place). Failure to establish these procedures is a violation of the MGDPA.

2. Data inventory

Minn. Stat. § 13.025.

The responsible authority is also required to prepare a public document that provides an inventory of all private and confidential data on individuals that is maintained by the city and must include the forms used to collect private and confidential data.

RELEVANT LINKS:

Minn. R. 1205.2000.

The public document must:

- Include the name, job title, and business address of the responsible authority and any designees.
- Identify these people as the persons responsible for responding to inquiries from the public concerning the MGDPA.
- Identify and describe by type all records, files, or processes maintained by the city that contain private or confidential data.
- Specify the files or systems for which each designee is responsible.
- Cite the state statute or federal law that classifies the data as private or confidential.
- Provide descriptions of the records, files, and processes in "easily understandable English," avoiding uncommon or technical words or expressions whenever possible.

Minn. Stat. § 13.025.
DPO 95-006.

The document must also be made available to the public and updated annually to reflect any changes. The commissioner of the Department of Administration may require the responsible authority to provide copies or any additional information relevant to data collection practices, policies, and procedures.

B. Required designations

1. Responsible authority

Minn. R. 1205.1000.
Minn. Stat. § 13.02, subd. 16.
See Section IV-D *Duties of the responsible authority*.

Cities are required to appoint a single employee as the city's "responsible authority." The responsible authority is responsible for the collection, use, and dissemination of government data.

Minn. Stat. § 13.02, subd. 16.

The elected or appointed city clerk is the responsible authority for statutory or home rule charter cities until the city council has made the designation. In home rule charter cities that do not have an office of city clerk, the responsible authority is the chief clerical officer for filing and record keeping purposes.

Minn. R. 1205.2000, subp. 2.

Appointing a Responsible Authority, LMC Model Resolution.
DPO 05-010.

A responsible authority is appointed by resolution, which must include the name of the specific individual who is appointed. It is inadequate to simply have a resolution that designates a job title (such as city clerk or administrator) as the responsible authority. A city will need to adopt a new resolution when the city's responsible authority changes.

2. Designee

Minn. Stat. § 13.02, subd. 6.

Minn. Stat. § 13.03, subd. 2.

A "designee" is any person designated by a responsible authority to be in charge of individual files or systems containing government data and to receive and comply with requests for government data.

RELEVANT LINKS:

Minn. R. 1205.1100, subp. 1.

Minn. R. 1205.1100, subp. 2.

DPO 03-038.
Minn. R. 1205.1100, subp. 3.

A responsible authority may designate one or more designees. Any designee must be a city employee.

The responsible authority must appoint designees by written order. The responsible authority must also instruct any designees in the requirements of the MGDPA and the accompanying rules. If the responsible authority deems it necessary, the instruction must include:

- Written materials describing the requirements of the MGDPA and the accompanying rules.
- Programs that familiarize city personnel with the requirements of the MGDPA and the accompanying rules.
- Mandatory attendance at training programs (within or outside the city).

3. Compliance official

Minn. Stat. § 13.05, subd. 13.

DPO 00-045.

DPO 06-033.

A city employee must also be appointed or designated as the data practices compliance official. Questions or concerns regarding the MGDPA (such as difficulties accessing government data) are directed to the compliance official. The city's responsible authority may also serve as compliance official.

C. Powers of the responsible authority

Minn. R. 1205.0900.

The responsible authority is empowered to:

- Implement the MGDPA and accompanying rules in the city.
- Make good faith attempts to resolve any controversies arising from the city's creation, collection, use, and dissemination of data.
- Change city programs, procedures, and forms to bring them into compliance with the MGDPA and the accompanying rules.
- Take all administrative actions necessary to comply with the general requirements of the MGDPA, particularly the rights of subjects of data.

Minn. Stat. § 13.04.

- Direct designees to perform the detailed requirements of the MGDPA and the accompanying rules (under the general supervision of the responsible authority) as needed.

D. Duties of the responsible authority

When it comes to classifying, maintaining, and disseminating data, accountability begins and ends with the responsible authority. While specific duties are outlined in the MGDPA, a responsible authority must really be aware of all facets of the MGDPA and other applicable state and federal laws in order to ensure the city is in full compliance.

RELEVANT LINKS:

1. Classifying, maintaining, and securing data

Minn. Stat. § 13.05, subd. 5(b).
Minn. R. 1205.1500.

The responsible authority is ultimately in charge of all government data from the time it comes into the city's possession until it is destroyed pursuant to law.

Scott v. Minneapolis Pub. Sch., Special Dist. No. 1, A05-649 (Minn. Ct. App. April 18, 2006) (unpublished decision).
Minn. Stat. § 138.17, subd. 7.

When not public data is being disposed of, it must be destroyed in a way that prevents its contents from being determined. The responsible authority must also keep an inventory whenever records are destroyed.

Minn. R. 1205.0800.

It is the responsible authority's duty to:

- Review and identify all of the types of data maintained by the entity (including data retained as active and inactive).
- Determine what types of data maintained by the entity are classified "not public" (as defined by law).
- Identify either the state statute or provision of federal law supporting any not public classification.
- Administer all city data in accordance with its classification.

Minn. Stat. § 13.02.
Minn. R. 1205.0200.

As a general rule, data should be maintained according to its classification. For example, personnel data is best organized according to the public/private/confidential determinations, with discreet, separable sections for each classification within the individual personnel file. While this can become complicated when different classifications are intertwined, it is still more efficient to maintain data by classification to the greatest extent possible. Moreover, in light of the responsible authority's duty to make data accessible, maintaining it by classification allows the city to respond to requests more quickly and accurately.

See Section VIII-A-1-l *File management*.

As the Legislature frequently changes the MGDPA, it is a good idea to periodically review data classifications and storage measures to ensure the city's data is properly classified, maintained, and readily accessible.

Minn. Stat. § 13.03.

DPO 05-032.

The responsible authority has additional duties when it comes to managing private or confidential data. For records, files, or other data collected prior to Aug. 1, 1975, the responsible authority must:

Minn. R. 1205.1300, subp. 2.

- Review the federal, state, or local authority which required or necessitated the collection of private or confidential data.
- Determine the lawful purpose of the data at the time it was originally collected.
- Direct city staff that private or confidential data collected prior to Aug. 1, 1975, may only be used, stored, or disseminated as authorized at the time the data was originally collected.

RELEVANT LINKS:

Minn. R. 1205.1300, subp. 3.

For private or confidential data collected after Aug. 1, 1975, the responsible authority must:

- Review the relevant law that required or necessitates the collection of data.
- Identify the purposes for the collection of and the intended uses of all private or confidential data that have been (or should have been) communicated to the data subjects at the time of collection.

See Section V-B *Data subjects*.

Minn. R. 1205.1300, subp. 4(A).

After reviewing all data (determining the collection date and relevant law in effect at the time of collection), the responsible authority must prepare lists that identify the uses of and purposes for each type of private or confidential data. Each list must identify all persons, agencies, or entities authorized by state statute or federal law to access the data.

Minn. R. 1205.1300, subp. 4(B).

The responsible authority must do one of the following:

- Attach each list to city forms that collect private or confidential data.
- Communicate, in any reasonable fashion, the contents of each list to data subjects at the time data is collected.

In this context, "reasonable fashion" includes, but is not limited to, communicating orally with data subjects, and providing data subjects with brochures that describe the entity's purposes for collecting private and confidential data and how the entity intends to use the data.

Minn. R. 1205.1300, subp. 5.

The responsible authority must also educate city personnel, prepare administrative procedures, and distribute policy directives requiring compliance with the authorized purposes and uses of private and confidential data.

Minn. Stat. § 13.05, subd. 4.

Minn. R. 1205.1500, subp. 5.

DPO 12-007.

When collecting and maintaining data, the responsible authority must ensure that the city is not collecting data that is not needed, and must ensure that the city uses it only for the purpose for which it was originally collected. There are some exceptions, which include:

Minn. Stat. § 13.05, subd. 4(a).

- Data collected prior to Aug. 1, 1975, which has not been treated as public data, may be used, stored, and disseminated for the purposes for which the data was originally collected, or for purposes that are specifically approved by the commissioner of the Department of Administration as necessary to public health, safety, or welfare.

Minn. Stat. § 13.05, subd. 4(b).

- Private or confidential data may be used and disseminated to individuals or entities specifically authorized access by state, local, or federal law enacted after the collection of the data.

RELEVANT LINKS:

Minn. Stat. § 13.05, subd. 4(c).

- Private or confidential data may be used and disseminated to individuals or entities subsequent to the collection when the responsible authority has requested and has been specifically approved by the commissioner for a new or different use or dissemination that is necessary to carry out a function assigned by law.

Minn. Stat. § 13.05, subd. 4(d).

- Private data may be used by and disseminated to individuals or entities if the data subject has given their informed consent.

Minn. Stat. § 13.05, subd. 5.

DPO 00-043.

The responsible authority must establish procedures to ensure that all data on individuals is accurate, complete, and current for the purposes for which it was collected. It must also establish appropriate security safeguards for all records containing data on individuals, including procedures for ensuring that data that are not public are only accessible to persons whose work assignment reasonably requires access to the data, and are only being accessed by those persons for purposes described in the procedure.

DPO sample policies for government entities.

The responsible authority must also develop a policy incorporating these procedures, which may include a model policy governing access to the data if sharing of the data with other government entities is authorized by law. The Department of Administration has guidance on this requirement.

2. Access to data

Scheffler v. City of Anoka et al., No. A16-0252 (Minn. Ct. App., Feb. 6, 2017).

A person seeking government data must make a request to the government entity's specified responsible authority or designee before claiming a violation of the MGDPA for failure to provide data or for failure to provide a reason for denial of a request for data. The MGDPA does not recognize responsible authorities or designees by operation of the apparent-authority principles in common law, and city staff who are not the city's responsible authority or designees cannot violate the MGDPA by failing to produce the requested data.

a. Responding to data requests

Minn. Stat. § 13.03, subd. 3(c).

Minn. Stat. § 13.03, subd. 3(f).

It is the responsible authority's duty to respond to requests for data. The responsible authority must allow access to or provide copies of data upon request, and must provide the specific statutory authority when access is denied.

Minn. Stat. § 13.05, subd. 12.

Minn. R. 1205.0300, subp. 2.

DPO 96-043.

The responsible authority or designee generally may not require requestors to identify themselves, state a reason for a request, or otherwise justify a request for public data. It is appropriate, however, to request information to confirm that an individual requesting private data is in fact the subject of the data (or the authorized representative). If the data does not exist, the requestor must be informed of this fact.

RELEVANT LINKS:

DPO 04-063.

DPO 99-046.

When a request is made, it is the duty of the responsible authority or designee to review the request to verify what data, if any, is being requested. It is possible that what appears to be a request for data is not a request, or the request might be ambiguous.

Before responding, the responsible authority must determine what data is requested, what data exists, if the requestor is the subject of the data, and how the data is classified.

Minn. Stat. § 13.03, subd. 3(a).

DPO 95-030.

A person must be permitted to inspect and copy public government data at reasonable times and places and, upon request, must be informed of the data's meaning. Data requests need not be made in person, but a city may require requests to be in writing as part of its access procedures.

b. Inspection, copies, and copy costs

Minn. Stat. § 13.03, subd. 3(a).

Minn. Stat. § 13.04, subd. 3.

DPO 00-074.
DPO 03-037.

Although the MGDPA requires that the responsible authority inform the requestor of the data's meaning, the responsible authority is not required to interpret the data for the requestor. It simply means that any abbreviations, acronyms, "lingo," or other words that are not commonly used or understood must be explained.

Minn. Stat. § 13.03, subd. 3(b).

An "inspection" is typically (but is not limited to) a visual inspection of paper or similar types of government data. Inspections do not require printing copies, unless printing a copy is the only way to provide access. When a person requests access for the purpose of inspection, the responsible authority may not impose a charge or otherwise require the payment of a fee to inspect data.

Minn. Stat. § 13.03, subd. 3(a).
DPO 04-058.

Minn. Stat. § 13.03, subd. 3(c).
Minn. R. 1205.0300.

See Section VIII-B-1 *Requestor is not the subject of the data*.

See DPO, Copy Costs for the Public.

The responsible authority or designee must provide copies of public data upon request. If a requestor wants copies (including data transmitted electronically), he or she may be required to pay the actual costs of searching for and retrieving government data, including the cost of employee time, and for making, certifying, compiling, copying, and/or electronically transmitting the data. An individual may not be charged for costs related to separating public from not public data.

Minn. Stat. § 13.03, subd. 3(c).

DPO 07-002.
DPO 07-008.

However, if the request is for 100 or fewer pages of black and white, letter or legal size paper, and the requestor is not the subject of the data, the maximum allowable charge is 25 cents for each page copied (or 50 cents for two-sided copies). Actual costs may not be charged for requests of this size.

RELEVANT LINKS:

Minn. Stat. § 13.03, subd. 3(d).

DPO 01-030.
DPO 02-011.
DPO 03-025.
DPO 08-012.

A responsible authority may charge a reasonable fee, in addition to the costs of making and certifying copies, when the public government data has commercial value and is a substantial and discrete portion of an entire formula, pattern, compilation, program, device, method, technique, process, database, or system developed with a significant expenditure of public funds by the city. Any fee charged must be clearly demonstrated by the city to relate to the actual development costs of the information. Upon request, the responsible authority must provide sufficient documentation to explain and justify the fee being charged.

Minn. Stat. § 13.03, subd. 3(d).

DPO 96-032.

An electronic copy of any public data maintained in a computer storage medium must be provided if the government entity can reasonably make the copy or have a copy made.

A city is not, however, required to provide the data in an electronic format or program different than it is maintained. The requesting person may be required to pay the actual cost of providing the copy.

c. Time limits

Minn. Stat. § 13.03, subd. 2(a).
Minn. Stat. § 13.03, subd. 3(c).
DPO 03-025.
DPO 95-006.
Northwest Publications, Inc. v. City of Bloomington, 499 N.W.2d 509 (Minn. Ct. App. 1993).

Requests for government data must be responded to in an "appropriate and prompt manner." If the responsible authority or designee is unable to provide copies at the time a request is made, they must be supplied as "soon as reasonably possible." Because there is no specific number of days for responding to all requests for public data, the responsible authority has some discretion, based on the scope of the request and the time it will take to respond.

Minn. Stat. § 13.04, subd. 3.

DPO 04-032.

There is a specific time limit when the request comes from the data subject. If an immediate response is not possible, the responsible authority must respond within 10 business days of the request.

d. Denying access

Minn. Stat. § 13.03, subd. 3(f).

DPO 01-074.
DPO 02-016.
DPO 04-062.

If a request for data is denied or redacted based on the data classification, the responsible authority or designee must inform the requesting person of the determination either orally at the time of the request, or in writing as soon as possible, providing the specific statutory section, temporary classification, or specific provision of federal law on which the determination is based.

Upon the request of the person denied access, the responsible authority or designee must certify the denial (citing the basis for the denial) in writing.

RELEVANT LINKS:

e. Unreasonable or harassing requests

While there is no limit on the volume of government data that may be requested or provided, a responsible authority has no duty to provide information if a request is unreasonable or made for the purpose of harassing city staff.

DPO 01-031.
DPO 01-034.
DPO 03-046.

Minn. Stat. § 645.17.

Unfortunately, the MGDPA does not provide any specific guidance on what is an unreasonable request. In advisory opinions, the commissioner of the Department of Administration has indicated that a request must be extremely burdensome or harassing before a government entity may decline a request to access public data.

Large requests take up significant staff time and other city resources. It is particularly frustrating when the requestor never comes in to inspect the requested data, or only wants a few pages copied out of a larger compilation of materials.

Webster v. Hennepin County et al., A16-0736 (Minn. Ct. App., April 10, 2017).

The Minnesota Court of Appeals has determined that the MGDPA does not allow government entities to require a requestor to narrow their search because the amount of responsive data is too large, or too time consuming to produce. However, the court did note the MGDPA does not prevent a government entity from working with a requestor to better understand or narrow the scope of a request. But if the requestor refuses to narrow their search, this would not allow the government entity to refuse access to public government data.

While city officials may feel that many such requests are unreasonable or harassing, a request will need to be extremely unreasonable before the obligation to respond is relieved.

f. Summary data

Occasionally, a city is asked for data that is generally understood to be data on individuals (e.g., city employees), but does not specifically identify any one person.

Minn. Stat. § 13.02, subd. 19.

"Summary data" is defined as statistical records and reports derived from data on individuals, but in which individuals are not identified and from which neither their identities nor any other characteristic that could uniquely identify an individual is ascertainable. Unless it is classified differently under a temporary classification, another state statute, or federal law, summary data is public.

Minn. Stat. § 13.05, subd. 7.
Minn. R. 1205.0700.

RELEVANT LINKS:

Minn. Stat. § 13.05, subd. 7.
Minn. R. 1205.0700, subp. 4.

Upon written request, the responsible authority must prepare summary data from private or confidential data. Within 10 days of the request, the responsible authority must inform the requestor of the estimated cost to prepare the summary data. The requestor is responsible for the cost of preparing the summary data.

Minn. R. 1205.0700, subp. 4.
DPO 98-019.

Minn. Stat. § 13.05, subd. 7.

The responsible authority may delegate the preparation of summary data to:

- An administrative officer responsible for any central repository of summary data.
- A person outside the city if the purpose is set forth in writing, the person agrees not to disclose information, and the entity reasonably determines that the access will not compromise private or confidential data.

Minn. R. 1205.0700, subp. 5.

DPO 01-053.

When providing summary data in response to a request, the city should provide as much detailed information as possible without revealing the identity of the data subjects.

g. Redacting and separating data

Minn. Stat. § 13.03, subd. 1.

DPO 95-025.

As a general rule, a city is not required to create data in response to requests. However, in instances where documents, files, records, or the like contain both public data and not public data, an individual may typically request and obtain access to the public data within. The responsible authority must remove any not public data prior to release.

DPO 02-028.

One way to accomplish this is to redact any not public data. Redaction involves removing or blocking out protected data.

Rather than altering any original records, the responsible authority provides a redacted copy of the requested data. If the requestor only wants to inspect data, the city may not charge for any copies made responding to the request.

Minn. Stat. § 13.03, subd. 3(a).

DPO 94-056.
DPO 95-006.

Another way is to separate the public and not public data. Separating data is distinguishable from creating new data. When separating data, the responsible authority or designee must remove data that is not accessible. As with redacting, the city may not charge for any costs incurred separating the data.

Minn. Stat. § 13.03, subd. 3(c). Minn. Stat. § 13.04, subd. 3.

Northwest Publications, Inc. v. City of Bloomington, 499 N.W.2d 509 (Minn. Ct. App. 1993).
DPO 96-002.
DPO 11-013.

In some instances, public data and not public data may be so intertwined that it is impossible to separate the data by classification. In rare situations, cities may decline access if the public data is rendered useless after it is separated out. This type of denial should be used a last resort in extreme situations.

RELEVANT LINKS:

h. Standing requests

Minn. Stat. § 13.03, subd. 3.

A "standing request" is a blanket request for newly created or updated data as it becomes available.

Minn. Stat. § 13.04, subd. 3.

DPO 04-007.

DPO 96-047.

For example, a resident might make a standing request for copies of city council meeting minutes upon adoption by the council. While the MGDPA does not specifically address standing requests, the commissioner of Administration has concluded that the broad language of the law creates an obligation to respond.

i. Access by other government agencies

Minn. Stat. § 13.05, subd. 9.

DPO 98-034.

A responsible authority must allow other responsible authorities to access not public data as authorized or required by state statute or federal law. An entity supplying government data may require the requesting entity to pay the actual cost of supplying the data.

j. Security assessment

Minn. Stat. § 13.055, subd. 6.
Minn. Stat. § 325E.61, subd. 1.

At least annually, cities must conduct a comprehensive security assessment of any personal information maintained by the government entity. The term "personal information" is defined as an individual's first name or first initial and last name in combination with a social security number, driver's license or Minnesota ID card number or an account or credit/debit card number.

k. Disclosure of data breach

Minn. Stat. § 13.055.

A relatively recent addition to the responsible authority's duties is the city's obligation to take certain actions in the event of a breach or unauthorized acquisition of private or confidential data on individuals. If the security and classification of the data are compromised by such a breach by the city or its contractor, the city must notify the subject of the data upon discovery or notification of the breach.

The city must also inform the individual of and prepare a report detailing the facts and results of an investigation into the breach. The notice and report are carefully described by the law.

RELEVANT LINKS:

V. Rights regarding government data

A. General public

Minn. Stat. § 13.03, subd. 3.

See Section III *Classifications*.

Every person has the right to inspect and copy public government data at reasonable times and places, as well as be informed of the data's meaning (an explanation of abbreviations or other words that are not commonly used or understood) upon request. Because one of the primary purposes of the MGDPA is to ensure public access to government data, it is imperative to properly classify data in order to facilitate access by the public.

B. Data subjects

Minn. Stat. § 13.04, subd. 3.

Providing for the rights of the subjects of data can be far more complicated. Individuals have the right to know whether:

- They are the subject of any government data.
- The data is classified as public, private, or confidential.

Minn. Stat. § 13.04, subd. 3.

The responsible authority must provide a data subject with access to any public or private data about that individual and must inform the individual of the content and meaning of the data if requested. When possible, the data subject must be provided access immediately. When immediate compliance is not possible, the responsible authority must comply within 10 business days of the request.

Minn. Stat. § 13.04, subd. 3.

See DPO, Copy Costs for Data Subjects.

In contrast, see Minn. Stat. § 13.03, subd. 3(c).

Upon request, the responsible authority must provide copies of any private or public data to the data subject. The responsible authority may require the requesting person to pay the actual costs of making, certifying, and compiling the copies. The data subject may not be charged for staff time to search for and retrieve the data.

Minn. Stat. § 13.04, subd. 3.

DPO 04-068.

Once an individual has been shown the private data and informed of its meaning, the city is not required to allow access to the data by the data subject for six months, unless:

- A dispute or legal action pursuant to the MGDPA is pending.
- Additional data on the individual has been collected or created.

DPO 95-014.

The data subject's use of the data is not regulated by the MGDPA. Even if the data subject makes private data public (e.g., an employee tells someone what is in his or her own personnel file), the city is still bound by the MGDPA and must act in accordance with the data's classification.

RELEVANT LINKS:

1. Tennessen warning

Minn. Stat. § 13.04, subd. 2.

In addition to the right to access private data, individuals who are asked to supply private or confidential data concerning themselves must be informed, before the data is collected, of:

DPO 98-003.

- The purpose and intended use of the requested data within the collecting government entity.
- Whether the individual may refuse or is legally required to supply the requested data.
- Any known consequence arising from supplying or refusing to supply private or confidential data.
- The identity of other persons or entities authorized by state or federal law to receive the data.

DPO 03-047.

See DPO, Tennessen Warning Notice.

This notice is commonly referred to as a "Tennessen warning," named after Sen. Robert Tennessen, the author of the original data privacy law in Minnesota. A Tennessen warning should be in writing and in easily understandable language. If the data subject is asked to provide information on a pre-printed form, it is a good idea to include a Tennessen warning on the form itself, or to have the warning on a sheet or card that the data subject may keep.

See, for example, *Employment Application*, LMC Model Form (see the "Data Practices Advisory" at the end), and *Recreational Registration with Tennessen Warning*, LMC Model Form.

DPO 96-062.
DPO 11-003.

In situations where a Tennessen warning was necessary, but not provided, the city is prohibited from using the data collected.

A city should not collect any information that is not needed, or use private or confidential information for any purpose other than what was explained to the data subject upon collection.

2. Informed consent

Minn. R. 1205.1400.
See DPO, Informed Consent.

Before the city may use an individual's private or confidential data differently than was indicated at the time of collection (with the Tennessen warning), it must obtain the individual's written permission.

Informed Consent for Release of Information, LMC Model Form.

A city must obtain an individual's "informed consent":

- When the individual asks the entity to release not public data to an entity or person that wasn't listed in the Tennessen warning.
- If it wants to use not public data in a way that is different than was explained in the Tennessen warning.
- When the data subject wants his or her private data released to another entity or person (e.g., a prospective employer).

RELEVANT LINKS:

Minn. R. 1205.1400.

An individual must have sufficient mental capacity to understand the consequences of his or her decision. To be valid, an informed consent must:

- Be voluntary (not coerced).
- Be in writing.
- Explain why the new use (or release) is necessary.
- Include any known consequence for giving informed consent.

VI. Disputes, procedures, and penalties

Because of the significant rights and numerous responsibilities involved with the MGDPA, there are situations where:

- A data subject questions the accuracy of data.
- An individual believes the responsible authority is improperly restricting access to information.
- The responsible authority isn't sure what the proper classification is.
- Not public data is accessed improperly.

The MGDPA provides several mechanisms for resolving these types of disputes, as well as penalties for noncompliance.

A. Challenging the accuracy or completeness of data

Minn. Stat. § 13.04, subd. 4.
DPO, Challenges and Appeals.

DPO 01-062.
DPO 04-052.

Individuals have the right to challenge the accuracy or completeness of data of which they are the subject. An individual must notify the responsible authority in writing, describing the nature of the disagreement. The responsible authority then has 30 days to do one of the following:

- Correct data found to be inaccurate or incomplete and attempt to notify past recipients of inaccurate or incomplete data, including recipients named by the individual.
- Notify the individual that the authority believes the data to be correct.

Minn. Stat. § 13.04, subd. 4(a).

The city must include a copy of the statement of disagreement every time it discloses the disputed data until the time the responsible authority makes a determination.

Minn. Stat. § 13.04, subd. 4(a).

Minn. Stat. §§ 14.48-.69.

If the data subject disagrees with the determination, he or she may appeal pursuant to the provisions of the Administrative Procedure Act for contested cases. Before issuing the notice and order of a contested case hearing, the commissioner of the Department of Administration will try to resolve the dispute informally, such as through conferences or conciliation.

RELEVANT LINKS:

With both parties' consent, the matter may be referred to mediation. If the parties are unable to come to an agreement, the commissioner will order a contested case hearing.

Minn. Stat. § 13.04, subd. 4(b).

Minn. Stat. § 138.17.

If the challenge is successful, the responsible authority must complete, correct, or destroy the data without regard to the requirements of the records retention law. The city may retain a copy of the commissioner's order or, if no order was issued, a summary of the dispute that does not contain any particulars of the successfully challenged data.

B. Commissioner opinions

Minn. Stat. § 13.072.

Minn. Stat. ch. 13D.

The commissioner of Administration has the authority to issue advisory opinions on the MGDPA and the Minnesota Open Meeting Law (OML). These opinions may be requested:

See DPO, Requesting a Data Practices Advisory Opinion.

- By a city, when the responsible authority is unsure how to classify data or respond to a data request.
- By a person, when that individual disagrees with a data practices determination.

Minn. Stat. § 13.072, subd. 1.
See DPO, Requesting an Open Meeting Law Advisory Opinion.

No fee is required to request a data practices advisory opinion (there is a $200 fee for requesting an OML advisory opinion). The commissioner may decide that no opinion is necessary (perhaps previous advisory opinions have already addressed a similar situation).

Minn. Stat. § 13.072, subd. 1(c).

Minn. Stat. § 13.072, subd. 1(d).

The person requesting the opinion must be notified of the decision not to issue an opinion within five business days of receipt of the request. Opinions may be issued within 20 days of receiving the request, but may be extended for an additional 30-day period upon written notice and for "good cause."

Minn. Stat. § 13.072, subd. 2.
Minn. Stat. § 13.072, subd. 1(f).
Billigmeier v. Hennepin County, 428 N.W.2d. 79, 81-82 (Minn. 1988).

Opinions of the commissioner can be helpful, but they are not binding (as are court decisions). In addition, an opinion issued by the attorney general takes precedence over a commissioner's opinion (but are also not legally binding like court decisions).

Minn. Stat. § 13.072, subd. 2.

However, when deciding MGDPA disputes, a court or other tribunal must give deference to an opinion of the commissioner. City staff or city officials who act in conformance with the commissioner's opinion will not be liable for damages or attorney fees if a court later determines that a violation of the MGDPA has occurred.

Minn. Stat. § 13.09.

In addition, city officials or other staff who rely on a commissioner's opinion will not be subject to forfeiture of their office for MGDPA violations.

RELEVANT LINKS:

Minn. Stat. § 13.072, subd. 2.

A person who requests an advisory opinion is not prevented from bringing another lawful action regarding access, classification, accuracy, or completeness of government data.

C. Civil remedies

1. Venue

Minn. Stat. § 13.08, subd. 3.

A civil action to recover damages, obtain an injunction, or compel compliance may be commenced:

- In the county in which the individual alleging damages or seeking relief resides.
- In the county wherein the political subdivision exists.
- When the dispute concerns the state of Minnesota, any county.

2. Damages

Minn. Stat. § 13.08, subd. 1.

Walker v. Scott County, 518 N.W.2d 76 (Minn. Ct. App. 1994).

A responsible authority or government entity is liable for violations of the MGDPA. The person damaged (or a representative of a decedent) may bring an action against the responsible authority or city to cover any damages sustained, as well as costs and reasonable attorney fees. In the case of a willful violation, the government entity will also be liable for exemplary damages (intended to reform or deter similar conduct) of not less than $1,000 and not more than $10,000 for each violation.

3. Injunction

Minn. Stat. § 13.08, subd. 2.

A court also has the authority to impose an injunction on a city or responsible authority that has or proposes to violate the MGDPA. The court may make any order or judgment as may be necessary to prevent any practices that violate the MGDPA.

4. Compel compliance

Minn. Stat. § 13.08, subd. 4(a).
Wiegel v. City of St. Paul, 639 N.W.2d 378 (Minn. 2002).

Any aggrieved person seeking to enforce their rights or obtain access to data may bring an action in district court to compel compliance with the MGDPA and may recover costs and disbursements, including reasonable attorney fees, as determined by the court.

See Section VI-D *Administrative remedies.*

Minn. Stat. § 13.08, subd. 4(c).

However, if the court determines that the action is frivolous, it may award reasonable costs and attorney fees to the responsible authority. The court must award reasonable attorney fees to a prevailing plaintiff if the court finds all of the following:

RELEVANT LINKS:

- The city was subject to a written advisory opinion.
- The opinion was directly related to the cause of action.
- The city did not act in conformity with the opinion.

Minn. Stat. § 13.08, subd. 4(a).

An action to compel compliance must be heard as soon as possible.

The court may inspect the disputed data in camera (off the record—perhaps in chambers), but the hearing must be conducted in public, in a manner that protects the security of any not public data.

If the court issues an order to compel compliance, a copy of the order is forwarded to the commissioner of the Department of Administration.

Minn. Stat. § 13.08, subd. 4(a).

Minn. Stat. § 13.08, subd. 4(b).

If the court issues an order to compel compliance, the court may impose a civil penalty of up to $1,000 against the city, payable to the state general fund. In determining whether to assess a civil penalty, the court must consider whether the government entity has substantially complied with the MGDPA, including but not limited to whether the entity has:

Minn. Stat. § 13.02, subd. 16.
Minn. Stat. § 13.05, subd. 13.
Minn. Stat. § 13.025, subd. 1.

- Designated a responsible authority.
- Designated a data practices compliance official.
- Prepared a data inventory that names the responsible authority and describes the records and data on individuals that are maintained.
- Developed public access procedures.
- Developed procedures to guarantee the rights of data subjects.

Minn. Stat. § 13.03, subd. 2.
Minn. Stat. § 13.025, subd. 3.
Minn. Stat. § 13.05, subd. 5.

- Developed procedures to ensure that data on individuals is accurate, complete, and safe.
- Acted in conformity with an advisory opinion.

Minn. Stat. § 13.072.

- Provided ongoing training to city personnel who respond to data requests.

It is important for cities and their responsible authorities to keep current in all of these areas to avoid additional penalties for MGDPA violations.

D. Administrative remedies

Minn. Stat. § 13.085.

For an expedited alternative to court actions, persons with data practices disputes may file a complaint with the state Office of Administrative Hearings (OAH). In contrast to the advisory opinion process, OAH administrative law judges (ALJs) have the authority to:

- Dismiss filed complaints.
- Determine whether violations of the MGDPA occurred.
- Impose civil penalties of up to $300 for violations.
- Issue an order compelling compliance with the MGDPA.
- Establish deadlines for production of data.

RELEVANT LINKS:

See Section VI-E *Criminal penalties*.

Minn. Stat. § 13.085, subd. 2.

OAH Complaint Form.

MN OAH.

Minn. Stat. § 13.085, subd. 6.

Minn. Stat. § 13.085, subd. 5(f).

Minn. Stat. § 13.09.

- Refer complaints to the appropriate prosecuting attorneys for possible criminal charges.

A complaint must be filed with the OAH within two years of the alleged violation (in cases involving concealment or misrepresentation by a government entity that could not be discovered during the two-year period, a complaint must be filed within one year after the concealment or misrepresentation is discovered). The complaint must:

- Be in writing.
- Be submitted under oath.
- Detail the factual basis for the alleged violation.
- Be accompanied by a filing fee of $1,000 or bond to guarantee payment.

Upon receipt of a filed complaint, the OAH notifies the government entity (the "respondent") and provides a copy of the complaint. The OAH must also try to notify the subject of the data in dispute (for example, a city employee, if the dispute concerns access to information within his or her personnel file). Upon notice, the respondent has 15 business days to submit a response. If the ALJ determines that the complaint presents sufficient facts (or "probable cause") that a MGDPA violation occurred, a public hearing will be conducted, and the ALJ will rule on the alleged violation. OAH decisions are enforceable in state district court; the losing party may appeal directly to the state Court of Appeals.

Unless there was a "mere technical" violation of the MGDPA or genuine uncertainty about the appropriate action, a successful complainant will be refunded the filing fee (minus $50) and awarded reasonable attorney fees, not to exceed $5,000.

If the government entity was the subject of an advisory opinion directly related to the matter in dispute, but did not comply with the opinion, attorney fees (up to $5,000) must be awarded. If the complaint was frivolous or brought for the purpose of harassment, the respondent may be awarded attorney fees, up to $5,000.

A government entity, city official, or city staff member who acts in conformity with an OAH order is generally immune from civil or criminal liability for that action.

E. Criminal penalties

In addition to the civil consequences of a violation of the MGDPA, there are criminal penalties.

RELEVANT LINKS:

A person who intentionally violates the MGDPA or the accompanying rules or whose conduct constitutes the knowing unauthorized acquisition of "not public" data is guilty of a misdemeanor crime.

F. Employment consequences

HR Reference Manual, Chapter 3.

Some employees have, by virtue of city policy or contractual agreement, a "property interest," or expectation of continued city employment.

Minn. Stat. § 13.09.

Willful violation of the MGDPA or its rules or conduct constituting knowing unauthorized acquisition of data that isn't public is considered just cause for suspension without pay or dismissal from employment.

VII. Other laws to consider

A. Minnesota statutes

In addition to the MGDPA, there are other Minnesota statutes that impose obligations on a city related to data management. For example, the MGDPA includes several sections that refer to "data coded elsewhere." As the provisions are spread throughout the statutes, it is always a good idea to verify that all applicable laws have been taken into account when classifying and managing data, or when making determinations as to access.

B. Federal law

1. Freedom of Information Act

5 U.S.C. § 552.

DPO 98-028.

The federal Freedom of Information Act (FOIA) addresses public access to records of the federal government and does not apply to state or local governments. If responsible authorities receive a request for data under the guise of the FOIA, prior to any disclosure, they may (and probably should) request clarification and inform the requestor that the FOIA does not apply.

2. HIPAA

45 C.F.R. § 160.

45 C.F.R. § 162.

45 C.F.R. § 164.

Cities that offer employer-sponsored health benefits, or operate a municipal hospital or ambulance service that transmits health information in electronic form, must comply with the data security and privacy provisions of the Health Insurance Portability and Accountability Act (HIPAA).

U.S. Department of Health and Human Services.

This federal law is intended to streamline industry inefficiencies, reduce paperwork, and make it possible for a worker to continue receiving health insurance benefits when switching jobs, even if the worker or a family member has a pre-existing condition.

RELEVANT LINKS:

HIPAA also created a starting point for protecting an individual's medical information.

HIPAA Administrative Simplification Statute and Rules.

HIPAA's administrative simplification regulations affect health care providers, clearinghouses, and health plans, including insurance companies, HMOs, and employer-sponsored health plans. These regulations require standardized electronic transactions, improved privacy and security methods, and greater access to and rights for individuals regarding their health information.

HIPAA Privacy Rule.

HIPAA Security Rule.

HIPAA privacy and security rules mandate the implementation of policies, procedures, and security measures with respect to protected health information (PHI).

These policies and procedures must be reasonably designed, taking into account the size and type of activities that relate to PHI, to ensure compliance.

45 C.F.R § 160.103.

PHI is any information that identifies an individual that is created, modified, received, or maintained and that relates to an individual's past, present, or future physical or mental condition, treatment, or payment for care. Information that may be considered (or may contain) PHI includes:

- Medical records.
- Diagnosis of a certain condition.
- Procedure codes on claim forms.
- Claims data.
- Pre-authorization forms.
- Explanation of Benefits (EOB).
- Crime reports.
- Coordination of benefit forms.
- Enrollment information and forms.
- Election forms.
- Reimbursement request forms.
- Records indicating payment.
- Claims denial and appeal information.

Contact the LMC HR & Benefits Staff for more information.

Information does not necessarily need to include an individual's name, address, or Social Security number to be considered "individually identifiable." For example, a claim report that contains only diagnoses, procedures and amounts paid during a specific period may contain individually identifiable information if the city has a relatively small number of participants in the health plan. Therefore, small cities may need to take extra precautions to ensure that they are protecting employee health information.

RELEVANT LINKS:

DPO 04-017.

DPO The Minnesota Consent Form to Release Health Information.

Except where specifically pre-empted, HIPAA regulations do not replace or supersede the MGDPA or any other applicable state law. As a consequence, there are many issues for cities to consider when it comes to individual health information.

The responsible authority must decide how to apply HIPAA, the MGDPA, and any other applicable laws together to ensure compliance with all of them.

VIII. Areas of interest

Minn. Stat. § 13.01.

While the MGDPA applies to all government data, city officials find that most requests concern a select number of subjects. Despite the frequency of requests, it can still be quite difficult to apply the MGDPA to the data in question and respond accordingly.

DPO
201 Administration Building
50 Sherburne Avenue
St. Paul, MN 55155.
(651) 296-6733.
(800) 657-3721.

A responsible authority or designee should consider consulting the city attorney for advice on data classifications, or before responding to any request for data that is not routine. The Data Practices Office (DPO) of the Department of Administration is an additional resource.

A. Human resources

Cities maintain a tremendous amount of data on their employees, elected and appointed officials, volunteers, and independent contractors.

1. Personnel data (employees, volunteers, and contractors)

Minn. Stat. § 13.43, subd. 1.

DPO 08-008.

Personnel data is defined as government data on individuals maintained because the individual is or was:

- A city employee.
- An applicant for city employment.
- A city volunteer.
- An independent contractor working with or for a city.

See Section VIII-A-1-i *Volunteers*.
See Section VIII-A-1-j *Independent contractors.*

Minn. Stat. § 13.43.

Personnel data includes data submitted by an employee as part of an organized self-evaluation effort by the city to request suggestions from all employees on ways to cut costs, improve efficiency, or improve the operation of government. An employee identified in a suggestion must be allowed to access the suggestion, but cannot be provided the identity of the person who made the suggestion.

RELEVANT LINKS:

DPO 03-002.

Minn. Stat. § 13.43, subd. 4.

Minn. Stat. § 13.43, subd. 2.

DPO 03-048.

DPO 03-008.

DPO 08-023.

DPO 08-004.
DPO 02-030.

DPO 95-001.

DPO 95-036.

DPO 01-063.
DPO 03-045.

DPO 96-045.
DPO 02-051.

DPO 96-020.
Minn. Stat. § 13.43, subd.1.
DPO 12-006.

DPO 04-030.

a. Public personnel data

The "presumption of openness" that generally applies to government data does not specifically apply to personnel data. Personnel data—including data pertaining to an employee's dependents—is presumed to be private and may only be released pursuant to court order.

The following personnel data on current and former employees, volunteers, and independent contractors is public:

- Name.
- Employee identification number (must not be Social Security number).
- Actual gross salary.
- Salary range.
- Terms and conditions of employment relationship.
- Contract fees.
- Actual gross pension.
- The value and nature of employer-paid fringe benefits.
- The basis for and the amount of any added compensation (including expense reimbursement) in addition to salary.
- Job title and bargaining unit.
- Job description.
- Education and training background.
- Previous work experience.
- Date of first and last day of employment.
- The existence and status of any complaints or charges against an employee (regardless of whether the complaint or charge resulted in disciplinary action).
- The final disposition of any disciplinary action against the employee, together with the specific reasons for the action and any data documenting the basis for the action (excluding data that would identify city employees who were confidential sources).
- The "complete" terms of any settlement agreement (including buyout agreements) except that the agreement must include specific reasons for the agreement if it involves the payment of more than $10,000 of public money. Best practice suggests working with the city attorney on settlement agreements.
- Work location and work telephone number.
- Badge number.
- Work-related continuing education.
- Honors and awards received.

RELEVANT LINKS:

DPO 04-032.
DPO 01-006.
DPO 17-001.

- Payroll time sheets or other comparable data that are only used to account for an employee's work time for payroll purposes (excluding any timesheet data that would reveal the employee's reasons for the use of sick or other medical leave, or any other not public data).

b. Access to personnel files

Minn. Stat. § 13.03.

Minn. R. 1205.0300, subp. 3.

DPO 95-029.

When an individual requests access to data, the government entity must respond promptly, appropriately, and within a reasonable time. While anyone may access public data contained within a personnel file, the level of access may change if the request comes from the employee, a supervisor, or even a councilmember.

(i) Employees

Minn. Stat. § 13.04, subd. 3.

DPO 98-038.

Cities must allow employees to access the public and private data within their own personnel files. After an employee has been provided access to private data, the city is not required to disclose the information again for a six-month period, unless a dispute or action (perhaps concerning accuracy or completeness) is pending or additional data on the employee has since been collected or created.

Minn. Stat. § 13.04, subd. 3.

DPO 01-005.

The city must respond to a request for access to a personnel file immediately, if possible, or within 10 days of the date of the request (excluding weekends and legal holidays) if immediate compliance is not possible.

(ii) Elected or appointed officials

Minn. R. 1205.0400, subp. 2.

Minn. R. 1205.0600, subp. 2.
DPO 99-019.
Handbook, *Local Government in Minnesota*.

Handbook, *The Statutory City*.

Responsible authorities often struggle determining whether, or to what extent, elected or appointed city officials and staff may access employee-related data. While private and confidential data may be accessed by individuals whose work assignments reasonably require access, determining who those individuals actually are can be difficult in practice. When it comes to members of the city council, the answer may depend in part on the type of city and its form of city government.

In Standard Plan and Plan A statutory cities, city employees are subject to the authority of the city council, so councilmembers would generally be allowed to access personnel data classified "not public." But, because this authority is exercised by the whole council (or a quorum thereof) together, independent or "unauthorized" requests from one councilmember may need to be handled in the same manner as if it came from a member of the public. In a Plan B statutory city, the council has delegated supervisory authority to a city manager and potentially limited the circumstances where council work would require access.

Handbook, *City Administrative Staff*.

RELEVANT LINKS:

Handbook, *The Home Rule Charter City*.

In Home Rule Charter cities, access to personnel files will depend on who has supervisory authority over city employees, be it the council or an executive officer (such as the city manager, administrator, or—in extremely limited circumstances—the mayor).

It can be very difficult for city staff to say "no" to a city councilmember's request to access not public data, but that may be required. It is always a good idea to seek the advice of the city attorney if one doubts an individual's ability to access private or confidential data.

c. Applicants for employment

Minn. Stat. § 13.43, subd. 1.

Personnel data includes government data maintained on individuals who are or were applicants for city employment. The following types of application data are classified as public:

Minn. Stat. § 13.43, subd. 3.

DPO 00-050.

DPO 94-022.

- Veteran status.
- Relevant test scores.
- Rank on eligibility list.
- Job history.
- Education and training.
- Work availability.

Minn. Stat. § 13.43, subd. 3.

Star Tribune Co. v. Univ. of Minn. Bd. of Regents, 683 N.W.2d 274 (Minn. 2004).

The applicants' names are private, unless or until they are either:

- Certified as eligible for appointment to a vacancy.
- Considered by the appointing authority to be finalists for a public employment position.

Minn. Stat. § 13.43, subd. 3.

Mankato Free Press Co. v. City of N. Mankato, 563 N.W.2d 291 (Minn. Ct. App. 1997).

An individual becomes a finalist when selected to be interviewed by the appointing authority (city council) prior to selection. Finalists become public when the council decides who they want to interview, regardless of whether a candidate agrees to be interviewed for the position.

(i) Background checks

HR Reference Manual, Chapter 2.

"Criminal Background Check Statutes: An Overview", House Research Department, Feb. 2014.

Minn. Stat. § 626.87.
Minn. Stat. § 13.43, subd. 12.

Minn. Stat. § 13.43, subd. 4.

Many cities conduct pre-employment background checks on potential employees. For certain government positions, criminal background checks are mandatory. As an example, cities are required to conduct a thorough background investigation before hiring a peace officer and must share that information with the Minnesota Board of Peace Officers Standards and Training (POST) or any other law enforcement agencies performing background investigations. Because the MGDPA does not specifically address background checks or related data for other city applicants, it is presumptively private data.

RELEVANT LINKS:

(ii) Pre-employment examinations

Minn. Stat. § 13.43, subd. 3.

Some cities require prospective employees to perform pre-employment evaluations, such as civil service exams. The MGDPA classifies "relevant test scores" as public data, but does not expand on the term's meaning. In an opinion, the commissioner of Administration advised that a reasonable interpretation of the term covered a quantifiable, objective score from an evaluation or test that is a requirement for the position and would not include for subjective evaluations (such as psychological or personality tests) that are considered highly sensitive.

DPO 05-035.

Minn. Stat. § 13.34.

DPO 05-040.

Testing or examination materials, such as scoring keys, are classified as nonpublic data if disclosure would compromise the objectivity or fairness of the testing or examination process. Examinees should be able to access their completed exams, unless such access would also compromise the examination process.

d. Complaints

Minn. Stat. § 13.43, subd. 2.

Navarre v. South Washington County Schools, 652 N.W.2d 9, 22 (Minn. 2002).

The existence and status of any complaints or charges against an employee—regardless of whether the complaint or charge results in disciplinary action—is public data. However, the nature of the complaint and the specific allegations against an employee are private.

See Section VIII-A-1-e *Discipline*.

DPO 11-013.

That information becomes public after a "final" disposition of the complaint or charge is reached by the city council or other arbitrator. Informal complaints made by council members among each other or to the city administrator regarding employee performance are considered private data

(i) Harassment

Minn. Stat. § 13.43, subd. 8.

DPO 99-014.

An employee generally has the right to access private data within his or her personnel file. However, when allegations of sexual or other types of harassment are made against an employee, that employee does not have the right to access data that would identify the complainant or any other witness, if the responsible authority concludes that access would threaten the personal safety of the complainant or other witness, or lead to harassment. If a disciplinary proceeding is initiated, data on the complainant (or other witness) must be made available to the employee as may be necessary for the employee to prepare for the proceeding.

(ii) Complainant identity

Demers v. City of Minneapolis, 468 N.W.2d 71 (Minn. 1991).

The MGDPA is often interpreted literally when it comes to who is allowed access to data that identifies a complainant.

RELEVANT LINKS:

DPO 97-018.
DPO 11-013.

If the complainant is another city employee, the identity of the complainant has been considered personnel data on the complainant and, therefore, private. At the same time, if the complainant is a member of the public (and not "protected" by Minn. Stat. § 13.43), the complainant's identity is presumed to be public.

Minn. Stat. § 13.43, subd. 8.

DPO 96-002.

This literal interpretation could lead to conflicting, perhaps questionable, results. For example, where a city employee may be prevented from knowing the identity of the individual alleging some form of harassment by the employee, the public wouldn't necessarily be precluded. While the commissioner acknowledged the absurdity of such a result, the MGDPA has not been amended to prevent it.

e. Discipline

Minn. Stat. § 13.43, subd. 2(a)(5).

The final disposition of any disciplinary action, as well as the specific reasons for the action and any data documenting the basis of the action (excluding data that would identify confidential sources who are city employees), is public data.

Minn. Stat. § 13.43, subd. 2(b).

A "final disposition" occurs when the city makes its final decision about the disciplinary action, regardless of the possibility of later proceedings.

City of Duluth v. Duluth Police Local, 690 N.W.2d 357 (Minn. Ct. App. 2004).

In the case of arbitration proceedings arising under collective bargaining agreements (CBAs), a final disposition occurs at the conclusion of the arbitration proceedings, or upon the failure of the employee to elect arbitration within the time provided by the CBA.

Final disposition includes resignations that occur after the final decision of the city or an arbitrator. However, if an arbitrator sustains an employee's grievance and reverses all aspects of any disciplinary action, the disciplinary action does not become public data.

State v. Renneke, 563 N.W.2d 335 (Minn. Ct. App. 1997).
DPO 03-045.

Sometimes an investigation or related matter concludes without any discipline occurring. For example, a city may investigate a citizen's complaint about an employee, but in the end take no action (perhaps the allegations were found to be without merit). If no disciplinary action is taken, then there is no final disposition for purposes of the MGDPA, and only limited data about the existence of a complaint or charges against an employee is public.

DPO 05-025.

Minn. Stat. § 13.43, subd.1.

For certain employees, upon completion of an investigation of a complaint or charge against them, or if they resign or are terminated while the complaint or charge is pending, all data relating to the complaint or charge are public.

These employees largely include employees within state government. However, sometimes it can also apply to certain city employees.

RELEVANT LINKS:

Minn. Stat. § 13.43, subd.1.

The same data is public for certain city employees if the complaint or charge results in disciplinary action, the employee resigns or is terminated while the complaint or charge is pending, or particular legal claims related to the complaint or charge are released as part of a settlement agreement. This applies to the following city employees.

- The chief administrative officer for the city.
- The top three highest paid employees in the city, and
- Managers; chiefs; heads or directors of departments, divisions, bureaus, or boards; and any equivalent position in a city with a population greater than 7,500.

Cities are encouraged to consult their attorney as needed in interpreting the applicability of this relatively new provision of law.

f. Health and medical (injury and accident reports)

Minn. Stat. § 13.43, subd. 2.

Any health or medical data a city has on its employees is not public, under both the MGDPA and other applicable state and federal law.

See Section VII-B-2 *HIPAA*.

Editorial note: While this memo (and common practice) uses the term "medical data" to describe the various types of medical or health-related information collected or maintained on city employees, the MGDPA defines this term to describe "data collected because an individual was or is a patient or client of a hospital, nursing home, medical center, clinic, health, or nursing agency operated by a government entity, including business and financial records, data provided by private health care facilities, and data provided by or about relatives of the individual."

Minn. Stat. § 13.384, subd. 1.

See Section VIII-T *Medical data (municipal hospitals).*

City officials understandably will continue to consider these types of records "medical data," but for purposes of applying the MGDPA, they will generally fall under the "personnel" data definition.

DPO 97-017.

If an employee is injured on the job, any data that the city might have related to the incident is also most likely not public personnel data. The employment status of the employee (for example, "on medical leave") is likely public, but data created as a result of the incident is not. If the incident is investigated and might result in a disciplinary action (against the injured individual or another employee), MGDPA provisions related to discipline would apply.

See Section VIII-1-e *Discipline*.

Minn. R. 1205.0400.

DPO 99-019.

See Section VIII-2 *Elected and appointed officials.*

If the responsible authority receives a request for data related to the incident from the mayor or a councilmember, access to information should be limited to the extent necessary for those elected officials to perform their official capacities.

RELEVANT LINKS:

See Section VIII-D-1 *Open Meeting Law*.

If the council considers a changing city policy as a result of an injury (perhaps to try and prevent similar accidents in the future), government data—in one form or another—would most likely be created. With the exception of any personnel data related to the specific employee involved in the original incident that might be included, data on the incident considered or created during a policy discussion would be public.

g. Employment reference checks

Minn. Stat. § 181.967, subd. 4.
Minn. Stat. § 13.05, subd. 4(d).

Cities will often receive requests for information from prospective employers about former or current city employees. Public employers, including cities, are generally immune from liability for dissemination of personnel data that is classified as public.

See Section V-B-2 *Informed consent.*

If a former or current city employee gives a written consent to the release of the following private data, the city would be immune from liability for disclosure of:

- Written employee evaluations of the former employee conducted while the employee worked for the city.
- The employee's written response to the evaluation contained in the employee's personnel record.
- The written reasons for the employee's separation from city employment.

Minn. Stat. § 181.967, subd. 2.

However, a city could be held liable for the dissemination of any data if the employee (or former employee) can demonstrate by clear and convincing evidence both of the following:

- The data was false and defamatory.
- The city knew or should have known the data was false and acted with malicious intent to injure the current or former employee.

See HR Reference Manual, Chapter 2.

A city must obtain a written release before giving out any private data. As many employment-related documents contain a mixture of public and private information, cities need to be careful to remove any private data if no release has been signed.

h. Emergency exception

Minn. Stat. § 13.43, subd. 11.

If the responsible authority or designee reasonably determines that the release of personnel data is necessary to protect an employee from self-harm, or to protect another person who may be harmed by the employee, data (relevant to such safety concerns) may be released to:

RELEVANT LINKS:

- The person who may be harmed and to an attorney representing the person when the data is relevant to obtaining a restraining order.
- A pre-petition screening team conducting an investigation of the employee for judicial commitment.
- A court, law enforcement agency, or prosecuting authority.

Minn. Stat. § 253B.07, subd. 1.

Data released under this emergency exception may change to a more restrictive classification when in the possession of the agency or authority that receives the data. If released to the person who may be harmed (or the person's attorney), the data may only be used or released further to the extent necessary to protect the person from harm.

Minn. Stat. § 13.43, subd. 11(c).
Minn. Stat. § 13.03, subd. 4(c).

i. Volunteers

Minn. Stat. § 13.43, subd. 1.

DPO 95-026.

As the MGDPA defines personnel data to include data on individuals maintained because the individual performs services on a voluntary basis for the city, the classifications and rules that apply to employees and applicants also apply to city volunteers, such as firefighters or recreation program volunteers.

j. Independent contractors

Minn. Stat. § 13.43, subd. 1.

Minn. Stat. § 13.02, subd. 8.

IBEW, Local No. 292 v. City of St. Cloud, 765 N.W.2d 64 (Minn. 2009).

Minn. Stat. § 13.02, subds. 8, 10.
DPO 11-002.

The MGDPA definition of personnel data also includes data on individuals maintained because the individual acts as an independent contractor with a government entity. An "individual" is defined as a natural person, a living human being.

The Minnesota Supreme Court has determined that data collected by a government entity on the employees of a corporation hired to perform services as an independent contractor cannot be considered personnel data, because a corporation is a "person" (and not an "individual") for the purpose of the MGDPA. Therefore, personnel data collected on the employees of private companies is presumed public and must be disclosed upon request unless there is a specific legal exception to the data's public nature.

As a result, similar data (such as home addresses) will have different classifications, depending on whether it concerns a city employee (private), an individual who is an independent contractor (private), or an employee of a corporation, partnership, or similar association that is the independent contractor (public).

RELEVANT LINKS:

Minn. Stat. ch. 13D.

LMC information memo, *Meetings of City Councils*. See Section VIII-D *Meetings*.

Minn. Stat. § 13.03, subd. 11.

Minn. Stat. § 13D.05, subd. 1.

DPO 09-012.

Minn. Stat. § 13D.05, subd. 1(c).

DPO 02-013.

See LMC information memo, *Management of Personnel Files*.

DPO 01-039.

k. Open Meeting Law

The relationship between the Minnesota Open Meeting Law (OML) and the protections afforded personnel data under the MGDPA can be confusing. Some assume that because private personnel data needs to be discussed, the meeting must be closed.

In reality, it is often necessary for city councils to discuss personnel data at open, public meetings—sometimes at the request of the city employees themselves.

However, the MGDPA provides that most not public data may be discussed at an open meeting. Except under specific circumstances, meetings may not be closed simply because not public data will be discussed. Not public data may be discussed at a meeting without liability or penalty 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.

Data discussed at an open meeting retains its original classification. For example, even if private personnel data is discussed at an open meeting, the data is still private (although a record of the meeting, regardless of form, is public).

l. File management

There are many issues to consider when it comes to managing city files, personnel files specifically. But, for the purposes of data practices, a personnel file management system must balance accessibility and security. The responsible authority should see to it that public, private, and confidential personnel data are kept separately, in order to allow appropriate access to the data as required.

2. Elected and appointed officials

Cities often struggle classifying the data related to their elected and appointed city officials. While the MGDPA provides some guidance, many questions remain.

a. Personnel data

One such question concerns whether (or to what extent) data on elected or appointed city officials can be considered personnel data.

Unfortunately, the MGDPA does not specifically address the employment status of city officials. However, the commissioner of the Department of Administration has suggested that this depends on how the city treats its elected officials.

RELEVANT LINKS:

DPO 03-011.

If elected and/or appointed officials are considered city employees, data related to their employment is treated as any other personnel data; if elected and/or appointed officials are not considered city employees, any data collected would fall under the general "public" presumption.

Krout v. City of Greenfield, No. A11-1200 (Minn. Ct. App. Apr. 16, 2012) (unpublished decision).

The Courts recently reviewed this issue when elected officials were asked to turn over their personal cell phone records after the city received a data request. The city released the data after determining which calls were related to city business. Elected officials were not considered employees, therefore, the data was public.

While cities have some discretion in designating their officials as employees, it is a good idea to include this determination within their written personnel policies.

b. Candidates for elected office

A.G. Op. 852, Oct. 6, 2006.

Minn. Stat. § 205.13, subd. 1.
Minn. Stat. § 204B.06, subd. 1.

The attorney general has advised that candidates seeking election to public office cannot be considered "applicants for employment" and as a result, "candidate" data is presumptively public. For example, individuals running for elected office must file an affidavit of candidacy with the city clerk; information provided in the affidavit is public data.

c. Applicants for office

Minn. Stat. § 13.601, subd. 3.
See Section VIII-A-2-e *Advisory boards and commissions.*

The MGDPA specifically provides that certain information about individuals who have applied for positions as elected or appointed officials is public:

- Name.
- City of residence, except when the appointment has a residency requirement that requires the entire address to be public.
- Education and training.
- Employment history.
- Volunteer work.
- Awards and honors.
- Prior government service or experience.
- Veteran status.
- Any data required to be provided or that are voluntarily provided in an application to a multimember agency pursuant to Minn. Stat. § 15.0597.

Minn. Stat. § 13.601, subd. 3.

Once an individual is appoint to a public body, the following additional items of data are public:

RELEVANT LINKS:

- Residential address.
- Telephone number or e-mail address, or both at the request of the appointee.
- First and last dates of service on the public body.
- Existence or status of complaints or charges against an appointee.
- Final investigation report about a compliant or charge against an appointee, unless access to the data would jeopardize an active investigation.

Some cities that treat their elected and appointed officials as employees have taken the position that this list represents the only information about applicants for elected or appointed office that would be public (and that anything not on this list would be presumed to be private). However, the commissioner has taken the position that this list merely reinforces the MGDPA's general presumption that all government data is public. The commissioner reasoned that, unlike personnel data, which is specifically presumed private except as enumerated public, this amendment does not begin with the same specific presumption. It simply reflects the Legislature's apparent intent to remove data on applicants for elected and appointed positions from the provisions related to personnel data. However, the commissioner did not explain why such a reinforcement of the general presumption was necessary.

DPO 05-036.

The attorney general has reached a different conclusion, reasoning that the enactment of Minn. Stat. § 13.601 does not preclude other data from being classified as private under another statute (such as Minn. Stat. § 13.43). Under this reasoning, in a city that considers elected and appointed officials to be employees, data submitted by applicants for these positions could be treated as private personnel data, notwithstanding any data expressly made public by any other provision of the MGDPA.

Informal A.G. Op., July 14, 2006.

Minn. Stat. § 13.43, subd. 3.
Minn. Stat. § 13.601, subd. 3.

d. Correspondence

Correspondence between individuals and elected officials is private data on individuals, but may be made public by either the sender or the recipient.

Minn. Stat. § 13.601, subd. 2.

However, in certain circumstances, such as correspondences related to public personnel data, between city employees and city officials (or any combination of employees or officials), or written on behalf of a corporation, the data is presumed public. Since such correspondence is necessarily related to their official work—to the extent that public data is included in the correspondence—and because the data does not fall within the parameters of the intended private designation, such correspondence is considered public data.

DPO 02-013.
DPO 10-023.
DPO 11-006.
DPO 11-019.

RELEVANT LINKS:

e. Advisory boards and commissions

Minn. Stat. § 13.601, subd. 3.

DPO 05-036.

Many cities use advisory boards and commissions, such as a planning commission or parks and recreation commission, to foster more community involvement in city decisions. The people serving in these positions are appointed and volunteer their time (although some cities do compensate those serving).

See Section VIII-A-2-c *Applicants for office.*

The same considerations discussed earlier about elected or appointed officials would apply to members of advisory boards and commissions.

3. Personal data

A city official or employee's personal data is sometimes intermingled with government data. For example, many employees make note of personal appointments on work or e-mail calendars that also contain data on appointments related to their official city business. This personal data is not government data and is not subject to the classifications and other requirements of the MGDPA.

DPO 96-055.

Data on an employee's calendar, even government data collected and created because the person is or was a city employee, if not personal data (and outside the MGDPA), will most likely be considered private personnel data.

DPO 02-003.

However, if a calendar serves another purpose, such as a telephone register, then any government data included in it would be public, subject to redaction of any not public data.

DPO 01-075.

DPO 05-017.

Many cities allow employees limited use of city computers for personal reasons. The public would not have access to any data stored on the computer that is strictly personal. Not all data on a city-owned computer is automatically government data.

DPO 97-049.

Minn. Stat. § 13.43, subd. 2(a)(7).

A frequent question raised by city staff and officials concerns the status of an employee's work e-mail address. Although this is personnel data, the data is likely public because it is considered by the commissioner to be an indicator of an employee's work location, which is specified as public data.

B. Copies

Minn. Stat. § 13.03, subd. 3(a).

See Section IV-D-2 *Access to data*.

When a person requests to inspect government data, the responsible authority must provide access (pursuant to the applicable classifications of the MGDPA) at no cost to the requestor. If a person requests copies of the data, the responsible authority must provide copies, but may charge for the copies provided. The amount the responsible authority may charge for copies of data will vary, depending on the nature of the request, as well as who is requesting the data.

RELEVANT LINKS:

1. Requestor is not the subject of the data

a. 100 or fewer pages

Minn. Stat. § 13.03, subd. 3(c).

DPO 07-002.
DPO 07-008.

DPO 09-018.

If 100 or fewer pages of black and white, letter or legal size paper copies are requested, the responsible authority may charge no more than 25 cents for each page copied, or 50 cents for each two-sided copy.

A city may not charge any more than this amount for black and white copies, regardless of the actual cost to respond to the request.

b. Actual costs

See DPO, Copy Costs for the Public.

Minn. Stat. § 13.03, subd. 3(c).

Minn. R. 1205.0300.

DPO 04-072.

DPO 04-055.
DPO 04-056.

DPO 05-016.

For any other request for copies of data (such as for more than 100 black and white paper copies, color copies, photographs, or audio/video cassettes or discs), the responsible authority may require the requestor to pay the actual costs of searching for and retrieving government data, including the cost of employee time, and for making, certifying, compiling, or electronically transmitting the copies of the data. The city may not charge for costs related to separating public from not public data.

Actual costs may include staff time required to retrieve, sort, and label documents (if necessary to identify what is to be copied), to remove staples or paper clips, to take documents to the copier for copying, and to copy documents. Staff time must be calculated at the wages or salary (and benefits) level of the lowest-paid employee who could have prepared the documents or made the copies.

Minn. R. 1205.0300, subp. 4.

DPO 97-013.

Actual costs can include materials, such as paper, ink/toner, staples, audio or videotapes, CDs, etc., as well as any special costs that could occur when copying computerized data, such as creating or modifying a computer program when necessary to format the data. Actual costs may also include mailing costs and vehicle costs that occur if the city has to transport the data to another facility in order to provide copies.

DPO 04-038.

DPO 09-018.

When someone inspects data, but only requests copies of some of that data, the city may only charge for the number of pages actually copied. Under these circumstances, if the request is for 100 or fewer pages, the city may charge no more than 25 cents per page actually copied. If more than 100 pages are copied, then the city may charge actual costs, but only for the portion of the inspected documents that were copied, not the total amount incurred responding to the initial request to inspect.

Actual costs may not include:

RELEVANT LINKS:

DPO 04-038.
DPO 04-072.

- Costs related to inspection.
- Costs related to verifying the accuracy of data.
- Staff time separating public from not public data.

DPO 04-072.
DPO 94-059.

- Purchase or rental of a copier.
- Maintenance or depreciation of a copier.

DPO 01-066.

- Normal operating expenses (such as electricity).
- Administrative costs not related to copying.

DPO 04-040.
DPO 04-055.

- Records storage (obtaining and returning data to off-site storage facility).

DPO 95-044.
DPO 99-024.

- Sales tax.

DPO 05-016.

The MGDPA does not allow cities to charge a minimum copying fee.

c. Commercial value

Minn. Stat. § 13.03, subd. 3(d).
DPO 03-025.

A responsible authority may impose an additional "reasonable" fee for copies of public government data that:

- Has commercial value.
- Is a substantial and discrete portion of—or an entire—formula, pattern, compilation, program, device, method, technique, process, database, or system developed with a significant expenditure of city funds.

DPO 08-012.

Any such fee charged must be clearly demonstrated by the city to relate to the actual development costs of the information. The responsible authority, upon the request of any person, must provide sufficient documentation to explain and justify the fee being charged.

d. Electronic format

Minn. Stat. § 13.03, subd. 3(e).

DPO 96-032.

If the city maintains data in a computer storage medium, the responsible authority must provide copies of any public data contained in that medium, in electronic form, if the city can reasonably make copies or have the copies made. This does not require a city to provide the data in an electronic format or program that is different from the format or program in which the data is maintained by the city. The city may require the requesting person to pay the actual cost of providing the copy.

e. Response time

Minn. Stat. § 13.03, subd. 3(c).
See Section IV-D-2-c *Time limits*.

When possible, copies should be provided at the time a request is made. If the responsible authority or designee is not able to provide copies at that time, copies shall be supplied as soon as reasonably possible.

RELEVANT LINKS:

2. Requestor is the subject of the data

Minn. Stat. § 13.04, subd. 3.

When the data subject makes the request, somewhat different rules apply. The requestor must be allowed to inspect data (public or private) without any charge.

DPO 96-051.
See Section VIII-B-1-b *Actual costs*.

If the requestor wants copies, then the responsible authority may require the requestor to pay the actual costs of making, certifying, and compiling the copies.

Unlike for requests made by the public, actual costs also apply to requests for 100 or fewer pages of black and white, legal or letter size copies.

Minn. Stat. § 13.04, subd. 3.

DPO 04-032.

The responsible authority must respond to a request from the data subject immediately, if possible, or within 10 days of the request (excluding Saturdays, Sundays, and legal holidays) when an immediate response is not possible.

3. Copies made by the requestor

DPO 01-086.

DPO 02-036.

DPO 04-059.

The commissioner of Administration has suggested that the MGDPA would allow someone to bring in and use his or her own personal electronic device, such as a tape recorder, scanner, portable copier, or digital camera, to make copies of data the requestor has requested or inspected.

4. Prepayment

DPO 04-068.

The commissioner has also suggested that a government entity is within its right to establish a policy that requires data requestors to pay all or part of any copy costs before providing copies.

A policy requiring advance payment will address situations where an individual will not pay copy fees (or perhaps subsequently reduces the size of the request based on cost) after copies have been prepared.

C. Law enforcement data

Minn. Stat. § 13.82, subd. 1

Cities with "agencies that carry on a law enforcement function," such as police departments, fire departments, or ambulance services, are creating and maintaining comprehensive law enforcement data subject to the MGDPA. Unfortunately, it can be difficult to determine law enforcement data's proper classification and often needs to be decided on a case-by-case basis.

1. Public law enforcement data

Certain law enforcement data is classified as public.

RELEVANT LINKS:

a. Arrest data

Minn. Stat. § 13.82, subd. 2.

DPO 94-010.

The following data created or collected by law enforcement agencies to document any actions taken by them to cite, arrest, incarcerate, or otherwise substantially deprive an adult individual of liberty is public at all times in the originating agency:

DPO 04-028.

- Time, date, and place of the action.
- Any resistance encountered by the agency.
- Any pursuit engaged in by the agency.
- Whether any weapons were used by the agency or by another individual.
- The charge, arrest or search warrants, or other legal basis for the action.
- Identities of the agencies, units within the agencies, and individual persons taking the action.
- Whether and where the individual is being held in custody or is being incarcerated by the agency.

DPO 08-006.

- Date, time, and legal basis for any transfer of custody and date, time, and legal basis for any release from custody or incarceration.

DPO 94-054.

- Name, age, sex, and last known address of an adult person cited, arrested, incarcerated or otherwise substantially deprived of liberty.
- Age and sex of any juvenile person, cited, arrested, incarcerated or otherwise substantially deprived of liberty.

DPO 12-010.
Minn. Stat. § 13.82, sub. 2.

- Whether the agency employed a portable recording system, automated license plate reader, wiretaps or other eavesdropping techniques (unless the release of this specific data would jeopardize an ongoing investigation).
- Squad car video footage, regardless of the existence of an active internal investigation stemming from the same incident.
- Manner in which the agencies received the information that led to the arrest.

Minn. Stat. § 13.82, subd. 17.
See Section VIII-C-5 *Protection of identities*.

- The names of individuals who supplied the information (unless the identities of those individuals qualify for protection, including an undercover law enforcement officer, a victim of or witness to a crime, a paid or unpaid informant, a witness or a juvenile witness, a 911 caller, or a mandated reporter).
- Response or incident report number.

DPO 00-025.

Arrest data includes situations where a law enforcement agency issues a citation (such as a parking ticket), rather than making an arrest. Citations are public, unless classified not public by another provision of the MGDPA.

RELEVANT LINKS:

b. Request for service data

Minn. Stat. § 13.82, subd. 3.

DPO 98-008.

DPO 00-078.

The following data created or collected by law enforcement agencies, which document requests by the public for law enforcement services, is public government data:

- The nature of the request or the activity complained of.
- The time and date of the request or complaint.
- The response initiated and the response or incident report number.
- The name and address of the individual making the request (unless the identity of the individual qualifies for protection, including an undercover law enforcement officer, a victim of or witness to a crime, a paid or unpaid informant, a witness or a juvenile witness, a deceased person whose body was improperly removed from a cemetery, a 911 caller, or a mandated reporter).

Minn. Stat. § 13.82, subd. 17.

DPO 01-050.

See Section VIII-C-5 *Protection of identities*.

c. Response or incident data

Minn. Stat. § 13.82, subd. 6.

DPO 02-040.

The following data created or collected by law enforcement agencies to document the agency's response to a request for service (including, but not limited to, responses to traffic accidents) or which describes actions taken by the agency on its own initiative, is public government data:

Minn. Stat. § 13.82, subd. 17.

- Date, time, and place of the action.
- Agencies, units of agencies, and individual agency personnel participating in the action (unless agency personnel qualify for protection).
- Any resistance encountered by the agency.
- Any pursuit engaged in by the agency.
- Whether any weapons were used by the agency or other individuals.
- A brief factual reconstruction of events associated with the action.

Minn. Stat. § 13.82, subd. 17.
DPO 08-006.

- Names and addresses of witnesses to the agency action or the incident (unless they qualify for protection).
- Names and addresses of any victims or casualties (unless any of those individuals qualify for protection).

Minn. Stat. § 13.82, subd. 17.

- Response or incident report number.
- Dates of birth of the parties involved in a traffic accident.
- Whether the parties involved were wearing seat belts.
- The alcohol concentration of each driver.

Minn. Stat. 13.82, subd. 6.

- Whether the agency used a portable recording system to document the agency's response or actions.

RELEVANT LINKS:

Minn. Stat. § 13.82, subd. 17.

See Section VIII-C-5 *Protection of identities*.

DPO 17-002.

(i) Protected identities

Law enforcement agencies may withhold access to what is normally public data on individuals to protect their identity in a limited number of circumstances. Data concerning individuals whose identities are protected are classified as private data about those individuals. The commissioner of Administration advised that law enforcement agencies must exercise their discretion to protect certain identities on a case-by-case basis, and must document those determinations.

(ii) Temporarily withholding data

Minn. Stat. § 13.82, subd. 14.

DPO 03-042.

DPO 08-006.

A law enforcement agency may temporarily withhold response or incident data if the agency reasonably believes that public access would likely endanger the physical safety of an individual or cause a perpetrator to flee, evade detection, or destroy evidence.

In such instances, the agency shall provide a statement that explains the necessity for its action upon request. Any person may apply to a district court for an order requiring the agency to release the data. If the court determines that the agency's action is not reasonable, the court must order the release of the data and may award costs and attorney fees to the person who sought the order. The disputed data is examined by the court in camera.

d. Booking photographs

Minn. Stat. § 13.82, subd. 26.

DPO 08-030.

A "booking photograph" is a photograph or electronically produced image taken by law enforcement for identification purposes in connection with the arrest of a person. Booking photographs are classified as public, but may be temporarily withheld if the agency determines that access will adversely affect an active investigation.

e. Missing children bulletins

Minn. Stat. § 13.82, subd. 23.

Minn. Stat. § 299C.54.

The commissioner of the Department of Public Safety issues quarterly missing children bulletins to all local law enforcement agencies, county attorneys, and public and nonpublic schools. The information included within the missing children bulletins is public data.

f. Use of surveillance technology

Minn. Stat. § 13.82, subd. 31.

The existence of all surveillance technology maintained by a law enforcement agency is public data.

RELEVANT LINKS:

2. Not public law enforcement data

Some law enforcement data will generally fall under one of the not public classifications.

a. Child abuse

Minn. Stat. § 13.82, subd. 8.

Minn. Stat. § 626.556, subd. 11.

Investigative data (active or inactive) that identifies a victim of reported child abuse or neglect is private data. Investigative data (active or inactive) that identifies a reporter of child abuse or neglect is confidential data, unless the subject of the report compels disclosure under state law.

Minn. Stat. § 13.82, subds. 7(a), 7(b), 9.
Minn. Stat. § 626.556, subd. 2.
DPO 94-048.

Inactive investigative data in a child abuse case (inactive due to a decision not to pursue the case, or because the applicable statute of limitations has run) that relates to the alleged abuse or neglect of a child by a person responsible for the child's care is also private data.

b. Vulnerable adults

Minn. Stat. § 13.82, subd. 10.

Minn. Stat. § 626.557.

Minn. Stat. § 626.5572, subd. 21.

Investigative data (active or inactive) that identifies a vulnerable adult as a victim of maltreatment is private data. Investigative data (active or inactive) that identifies a person who reports maltreatment of a vulnerable adult is also private data.

Minn. Stat. § 13.82, subds. 7(a), 7(b), 11.

DPO 95-010.

Inactive investigative data in a vulnerable adult case (inactive due to a decision not to pursue the case, or because the applicable statute of limitations has run) that relates to the alleged maltreatment of a vulnerable adult by a caregiver or facility is private data on individuals.

c. Property

Minn. Stat. § 13.82, subd. 20.

Data that uniquely describes stolen, lost, confiscated, or recovered property is classified (depending on content) as either private data on individuals or as nonpublic data.

d. Reward programs

Minn. Stat. § 13.82, subd. 21.

To the extent that the release of data would reveal the identity of an informant or adversely affect the integrity of the fund, financial records of a program that pays rewards to informants, are classified as confidential data on individuals or protected nonpublic data.

RELEVANT LINKS:

3. Mixed law enforcement data (public and/or not public)

Some law enforcement data is classified as either public or not public, depending on various factors considered in conjunction with the provisions of the MGDPA.

a. Criminal investigative data

Minn. Stat. § 13.82, subd. 7.

Investigative 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, is confidential or protected nonpublic data while the investigation is active. Despite this classification, some information related to the ongoing criminal investigation (such as arrest data or request for service data) will still be accessible by the public.

DPO 01-050.
See Section VIII-C-1 *Public law enforcement data.*

Minn. Stat. § 13.82, subd. 7.

An investigation becomes inactive upon any of the following events:

DPO 97-024.

- A decision by the law enforcement agency or appropriate prosecutorial authority to not pursue the case.
- 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 is earlier).
- Exhaustion or expiration of all rights of appeal by a person convicted on the basis of the investigative data.

Minn. Stat. § 13.82, subd. 7.

Inactive investigative data is public unless the release of the data would jeopardize another ongoing investigation or would reveal the identity of individuals whose identity qualifies for protection.

See Section VIII-C-5 *Protection of identities.*

Minn. Stat. § 13.82, subd. 7.

Any investigative data presented as evidence in court is public. Data determined to be inactive because of a decision by the agency or appropriate prosecutorial authority not to pursue the case becomes active if the agency or appropriate prosecutorial authority decides to renew the investigation.

DPO 04-069.

(i) Images, recordings and photographs

2016 Minn. Laws ch. 171 § 3, *amending* Minn. Stat. § 13.82, subd. 7.

Images and recordings, including photographs, video, and audio records that are part of inactive investigative files and that are clearly offensive to common sensibilities are private or not public data, provided that the existence of the images and recordings must be disclosed to any person requesting access to the inactive investigative file.

DPO 99-032.

RELEVANT LINKS:

(ii) Crime victim access

Minn. Stat. § 13.82, subd. 13.
Minn. Stat. § 13.821.
Minn. Stat. § 260B.171, subds. 4(c), 5(h).

DPO 05-028.

Upon receipt of a written request, a prosecuting authority is required to release investigative data collected by law enforcement to the victim of a criminal (or alleged criminal) act or to the victim's legal representative, unless the release is prohibited because it is a videotape of a child abuse victim.

A prosecuting authority may withhold law enforcement data from a crime victim if the prosecuting authority reasonably believes that either:

- The release will interfere with the investigation.
- The request is prompted by a desire on the part of the requester to engage in unlawful activities.

(iii) Judicial review and disclosure

Minn. Stat. § 13.82, subd. 7.

When an investigation is active, any person may bring an action in the district court located in the county where the data is being maintained to authorize disclosure of investigative data.

State v. Bagley, Nos. C4-00-1866, C5-00-1911 (Minn. Ct. App. Apr. 10, 2001) (unpublished decision).

The court may order that all or part of the data relating to a particular investigation be released to the public or to the person bringing the action.

In making the determination as to whether investigative data shall be disclosed, the court shall consider whether the benefit to the person bringing the action or to the public outweighs any harm to the public, to the agency, or to any person identified in the data. The data in dispute shall be examined by the court in camera.

(iv) Public benefit exception

Minn. Stat. § 13.82, subd. 15.

Any law enforcement agency may make any not public criminal investigative data or portable recording system data, classified as confidential or protected nonpublic, accessible to any person, agency, or the public, if the agency determines that the access will aid the law enforcement process, promote public safety, or dispel widespread rumor or unrest.

(v) Name changes

Minn. Stat. § 13.82, subd. 12.

Minn. Stat. § 259.10, subd. 2.

Data on court records relating to name changes resulting from participation in a witness protection program may be released, upon request, to a law enforcement agency conducting an investigation. The data is classified confidential while an investigation is active, and private when the investigation becomes inactive.

RELEVANT LINKS:

b. 911 calls

Minn. Stat. § 13.82, subd. 4.

DPO 05-031.
DPO 08-006.

See Section VIII-C-5 *Protection of identities*.

The audio recording of a call placed to a 911 system for the purpose of requesting service from a law enforcement, fire, or medical agency is private data on the individual making the call. A written transcript of the audio recording is public, unless it reveals the identity of an individual otherwise protected.

Minn. Stat. § 13.82, subd. 4.

DPO 96-052.

Minn. Stat. § 13.03, subd. 3.

A transcript of a 911 call must be prepared upon request. The person requesting the transcript is required to pay the actual cost of transcribing the call (in addition to any other applicable or allowed costs). The audio recording may be disseminated to law enforcement agencies for investigative purposes. The audio recording may also be used for public safety and emergency medical services training purposes.

c. Domestic abuse

Minn. Stat. § 13.82, subd. 5.

A victim of domestic abuse, the victim's attorney, or an organization designated as providing services to victims of domestic abuse (by the Minnesota Center for Crime Victims Services, the Department of

Corrections, or the Department of Public Safety) must be allowed access at no charge to the following data arising out of an incident of domestic abuse or out of an alleged violation of an order for protection:

Minn. Stat. § 629.341, subd. 4.
Minn. Stat. § 13.82, subd. 2.

Minn. Stat. § 13.82, subd. 3.
Minn. Stat. § 13.82, subd. 6.

- The written police report.
- Arrest data.
- Request for service data.
- Response or incident data.

d. Arrest warrant indices

Minn. Stat. § 13.82, subd. 19.

DPO 06-022.

Data in arrest warrant indices is classified as confidential data until the defendant has been taken into custody, served with a warrant, or appears before the court, unless the law enforcement agency determines that a public purpose is served by making the information public. The MGDPA does not define the term "warrant indices," but the commissioner of Administration considers the term to apply to a listing of active warrants.

e. Registered criminal predatory offenders

Minn. Stat. § 13.82, subds. 22, 28.
Minn. Stat. § 243.166, subds. 7, 7a.
Minn. Stat. § 244.052.

DPO 98-004.

With some exceptions, data relating to the registration of criminal predatory offenders is private data and may only be used for law enforcement and corrections purposes. For example, data regarding offenders (16 years of age or older) who have failed to provide their primary or secondary address as required, may be made available to the public.

RELEVANT LINKS:

f. Pawnshops and scrap metal dealers

Minn. Stat. § 13.82, subd. 27.

Data that reveals the identity of persons who are customers of a licensed pawnbroker, secondhand goods dealer, or a scrap metal dealer is private. Data describing the property in a regulated transaction with a licensed pawnbroker, secondhand goods dealer, or scrap metal dealer is public.

g. Deliberative processes

Minn. Stat. § 13.82, subd. 25.

Data that reflects deliberative processes or investigative techniques of law enforcement agencies is not public data. Information, reports, or memoranda that have been adopted as the final opinion or justification for a decision of a law enforcement agency are public.

DPO 95-003.

For data to reflect a deliberative process, it must explain or describe the actions, changes, or functions that the agency follows to conduct formal discussion (or debates) on all sides of an issue. Actual implementation of the process or practice of the investigative technique would be public data.

For example, if law enforcement uses a particular technique when questioning a suspect or witness, data related to the decision-making process to use that technique, or the training in that technique, would be not public data, but data related to an actual interrogation using the technique would be public.

4. Access to law enforcement data

Minn. Stat. § 13.82, subd. 16.

DPO 94-054.

DPO 04-031.

When comprehensive law enforcement data is classified as public, a law enforcement agency is not required to make the actual physical data available if it is not administratively feasible to segregate the public data from the not public data. However, the agency must make the information described as public data available to the public in a reasonable manner.

Minn. Stat. § 13.82, subd. 7.

When investigative data becomes inactive, the actual physical data associated with that investigation, including the public data, must be available for public access.

5. Protection of identities

Minn. Stat. § 13.82, subd. 17.

The identity of certain individuals is protected under the MGDPA. A law enforcement agency (or a law enforcement dispatching agency working under direction of a law enforcement agency) must withhold public access to data when access to the data would reveal the identity of:

RELEVANT LINKS:

Minn. Stat. § 13.43, subd. 5.

- All personnel data maintained by a government entity relating to an individual employed as or an applicant for employment as an undercover law enforcement officer are private data on individuals until the officer is no longer assigned to the undercover position, unless revealing the data would jeopardize the officer's safety, or the integrity of an active investigation. (When no longer assigned to an undercover position, the general law on personnel data applies to an officer).

Minn. Stat. § 13.43, subd. 2.

- A victim (or alleged victim) of criminal sexual conduct.

Minn. Stat. § 617.246, subd. 2.

- A minor engaged in (or assisting others) in a sexual or pornographic performance.

- A paid or unpaid informant being used by the agency (if the agency reasonably determines that disclosure would threaten the personal safety of the informant).

DPO 08-006.
DPO 04-033.

- A victim of or a witness to a crime if the victim or witness specifically requests to not be identified in public (unless the agency reasonably determines that disclosure would not threaten the personal safety or property of the individual).

- A deceased person whose body was unlawfully removed from a cemetery in which it was interred.

DPO 01-050.

- A person who placed a call to a 911 system or the identity or telephone number of a service subscriber whose phone is used to place a call to the 911 system and: (1) the agency determines that revealing the identity may threaten the personal safety or property of any person; or (2) the object of the call is to receive help in a mental health emergency (under these circumstances, a voice recording of a call placed to the 911 system is deemed to reveal the identity of the caller).

DPO 03-042.

- A juvenile witness (and the agency reasonably determines that the subject matter of the investigation justifies protecting the identity of the witness).

Minn. Stat. § 609.456.
Minn. Stat. §§ 626.556-.557.

- A mandated reporter.

Minn. Stat. § 13.82, subd. 17.
DPO 03-042.

Data concerning individuals whose identities are protected under these provisions is private. Law enforcement agencies are required to establish procedures to acquire the data and make the decisions necessary to protect the identity of individuals as required. The commissioner of Administration advised that law enforcement agencies must exercise their discretion to protect certain identities on a case-by-case basis, and must document those determinations.

DPO 17-002.

6. Accident reports

Although the terms are often used interchangeably, an "accident report" and a "police report" are not necessarily the same thing for purposes of the MGDPA.

RELEVANT LINKS:

Minn. Stat. § 169.09, subds. 7, 8.

Law enforcement officers are required to fill out an accident report when they, in the regular course of their duty, investigate a motor vehicle accident that results in one of the following:

- Bodily injury (or death) to any individual.
- Property damage to an apparent extent of $1,000 or more.

Minn. Stat. § 169.09, subd. 7.

The drivers involved in these types of vehicle accidents are also required to file an accident report. These reports (submitted in written or electronic form to the Department of Public Safety) are confidential data and are only to be used by the State of Minnesota, or any other state, federal, county, and municipal agency for accident analysis purposes.

Minn. Stat. § 169.09, subd. 13(a).

Minn. Stat. § 169.09, subd. 13(a)(1).

Upon written request of any individual involved in an accident (or the representative of the individual's estate, surviving spouse, one or more surviving next of kin, a trustee appointed by law, or other injured person), the commissioner of Public Safety or any law enforcement agency must disclose the accident report to the requestor, the requestor's legal counsel, or a representative of the insurer.

Minn. Stat. § 169.09, subd. 13(b).

Accident reports (and the data contained within) are not discoverable under any provision of law or rule of court. No report may be used as evidence in any civil or criminal trial, or in any action for damages or criminal proceedings arising out of an accident.

However, upon the demand of any person who has or claims to have made a report, or upon demand of any court, the commissioner must furnish a certificate showing that a specified accident report has or has not been made, solely to prove compliance or failure to comply with the requirements that the report be made to the commissioner.

Minn. Stat. § 169.09, subd. 13(c).

An individual who has made an accident report to the commissioner may provide information to any individuals involved in that particular accident or their representatives, or testify in any civil or criminal trial that arises out of an accident as to facts within the individual's knowledge. State statute makes the required reports privileged, but doesn't prohibit one from proving the facts to which the reports relate.

Minn. Stat. § 169.09, subd. 13(d).

DPO 07-003.

DPO 07-013.

Disclosing any information contained in any accident report, except as provided for in statutes (such as a request for service data, or response or incident data), is a misdemeanor offense. However, the information may also be contained in other city reports and/or databases, and those other law enforcement documents may be accessible upon request.

7. Driver and motor vehicle records

Some cities have facilities where city staff process driver's license renewals and motor vehicle records.

RELEVANT LINKS:

Accordingly, cities should be aware of the state and federal regulations related to the classification and release of this data.

a. State law

Minn. Stat. § 171.07, subd. 1a.

A city (acting as an agent of the state Department of Public safety) is required to file, or contract to file, all photographs or electronically

produced images obtained in the process of issuing driver's licenses or Minnesota identification cards. The photographs or electronically produced images are classified as private data. Contrary to the general right of data subjects to access and copy private data, a city is not required to provide copies of photographs or electronically produced images to data subjects.

Minn. Stat. § 13.02, subd. 12.

Minn. Stat. § 171.07, subd. 1a.

Minn. Stat. § 171.07, subd. 1a.

The use of the photograph or image files is restricted to:

- The issuance and control of driver's licenses.
- Criminal justice agencies for the investigation and prosecution of crimes, service of process, enforcement of no contact orders, location of missing persons, investigation and preparation of cases for criminal, juvenile, and traffic court, and supervision of offenders.
- Public defenders for the investigation and preparation of cases for criminal, juvenile, and traffic courts.
- Child support enforcement purposes.

Minn. Stat. § 299C.46, subd. 2.

Minn. Stat. § 611.272.

Minn. Stat. § 256.978.

Accordingly, cities may not use driver's licenses photos for other purposes.

b. Federal law

18 U.S.C. § 2721.

18 U.S.C. § 2725(3).

Federal law also regulates state motor vehicle records. Cities should not release any personal data contained in motor vehicle records.

"Personal data" in this context includes an individual's:

- Photograph.
- Social Security number.
- Driver identification number.
- Name.
- Address (but not the five-digit zip code).
- Telephone number.
- Medical or disability information.

18 U.S.C. § 2725(3).

Personal data does not include information on vehicular accidents, driving violations, and driver's status.

18 U.S.C. § 2721(a)(2).

18 U.S.C. § 2725(3).

Additional safeguards and restrictions for permitted uses are provided for "highly restricted personal data," which are an individual's:

RELEVANT LINKS:

- Photograph or image.
- Social Security number.
- Medical or disability information.

18 U.S.C. § 2721(b).

There are some permitted uses for state motor vehicle records, including the use by law enforcement for motor vehicle safety and recovery of stolen vehicles, recalls, emissions, or other legitimate business purposes.

DPO.

DVS.

The city should consult its city attorney before releasing the data when it is requested. The Data Practices Office (DPO) of the Department of Administration and the Driver and Vehicle Services (DVS) division of the Department of Public Safety are additional resources.

8. Predatory sex offender notification

Minn. Stat. § 244.052.

Law enforcement agencies receive pre-release reports for predatory sex offenders, notifying of the offender's intention to live, work, or regularly be found in the city. Prepared by the Department of Corrections, the data contained within the report is not public data. However, law enforcement personnel are authorized to release to the public any data in the report that is relevant and necessary to protect the public and to counteract the offender's dangerousness, consistent with the guidelines based on their offender classification.

DPO 98-004.
Minn. Stat. § 244.052, subd. 4.

Semler v. Klang, 743 N.W.2d 273 (Minn. Ct. App. 2007).

9. Ambulance records

DPO 01-017.

Whether records of an ambulance service are accessible depends, in part, on the ownership and operation of the service. If the service is privately owned, the data would not be government data subject to the MGDPA (it would be governed by the Minnesota Health Records Act and HIPAA regulations). If the city "owns" the service, the data would be government data and subject to the MGDPA.

Minn. Stat. §§ 144.291-.298.

45 C.F.R. § 160.

45 C.F.R. § 162.

45 C.F.R. § 164.

If the ambulance service is operated by the city hospital, any medical data created would be private data on individuals. If the ambulance service is operated by the city's fire department, the data would likely be considered law enforcement data. Accordingly, request for service data as described in the MGDPA would be public, but medical data would not.

Minn. Stat. § 13.384, subd. 3.

Minn. Stat. § 13.82, subd. 3.

10. Juvenile data

DPO 03-042.
Minn. Stat. § 260B.171.

Law enforcement data about children (persons 18 years of age or younger) who are or may be delinquent or engaged in criminal acts are classified private, but data may be disseminated:

DPO 12-014.

RELEVANT LINKS:

Minn. Stat. § 121A.28.

Minn. Stat. § 13.82, subd. 2.

Minn. Stat. § 611A.56, subd. 2.

Minn. Stat. § 260B.171.

- By order of the juvenile court.
- To chemical abuse pre-assessment teams.
- As provided by the MGDPA (age and sex of juvenile arrest data is public).
- To the child or the child's parent or guardian (unless disclosure would interfere with an ongoing investigation).
- To the Minnesota Crime Victims Reparations Board to process claims for crime victims' reparations.
- As otherwise provided in the statutory provisions related to delinquency.

Law enforcement records on juveniles should be kept separate from adult records (this does not require a separate computer system for juvenile records). Law enforcement agencies may exchange information pertinent and necessary to law enforcement purposes.

a. Traffic investigation reports

Minn. Stat. § 260B.171, subd. 5(d).
Minn. Stat. § 169.09, subd. 13.

DPO 97-007.

Data on children that is derived from traffic investigation reports is open to inspection by persons who have sustained physical or economic loss in a traffic accident involving a juvenile. Law enforcement agencies should be careful to release identifying information about juveniles in traffic reports only according to applicable state law (particularly if the juvenile was taken into custody).

b. Photographs

Minn. Stat. § 260B.171, subd. 5(c).

Law enforcement personnel may take booking photos of juveniles, but are required to destroy the photos when the juvenile reaches age 19. The photos may only be used for institution management purposes, case supervision by parole agents, and to assist law enforcement agencies in apprehending juvenile offenders. In the meantime, the photos must be maintained in the same manner as juvenile court records and names.

Minn. Stat. § 13.82, subd. 29.

DPO 08-030.

Photographs or electronically produced images of children adjudicated delinquent shall not be expunged from law enforcement records or databases.

11. Exchanging data

Minn. Stat. § 13.82, subd. 24.

Law enforcement agencies are able to exchange information, provided that it is pertinent and necessary to the requesting agency in initiating, furthering, or completing an investigation. An exception is provided for not public personnel data and Safe at Home program participant data.

RELEVANT LINKS:

12. Portable recording systems—police-worn body cameras

a. Private data

Minn. Stat. § 13.825, subd. 2(a).

Generally, body camera video and audio is private data on individuals or nonpublic data. Body camera data that is part of active criminal investigative data is generally confidential. There are several notable exceptions to this presumption discussed below.

b. Public data

Body camera data is public in the following situations:

Minn. Stat. § 13.825, subd. 2(a)(1)(4).

- When a peace officer discharges a firearm in the course of duty (but not discharge for training purposes or killing animals).
- When use of force by a peace officer results in "substantial bodily harm."

Minn. Stat. § 13.825, subd. 2(5)(d).

- When a data subject requests that the data be made accessible to the public—after redacting by blurring video or distorting audio of:
  1. Those who have not consented to the release.
  2. Undercover officers.
- When body camera data documenting the basis for discipline is part of personnel data in final disposition of discipline.
- When made public by order of the court.

2017 Minn. Laws ch. 171 *amending* Minn. Stat. § 13.82, subd. 15.

A law enforcement agency may make body camera data that is classified as confidential, protected nonpublic, private or nonpublic data accessible to the public if they have determined that it will aid in the law enforcement process, promote public safety, or dispel widespread rumor or unrest.

Minn. Stat. § 13.825, subd. 2(5)(b).

A law enforcement agency may also redact or withhold access to portions of data that are public when the data is "clearly offensive to common sensibilities." A best practice would be to review the data with the city attorney and determine what portions, if any, can be released to the public.

In addition to the data itself, the following information about a department's use of body cameras is also public data:

Minn. Stat. § 13.825, subd. 5.

- Policies and procedures.
- The total number of devices owned or maintained.
- The daily record of devices deployed by officers.
- If applicable, the specific precincts where the devices are used.
- The total amount of recorded audio and video data collected.
- The records retention schedule for the data.
- The procedures for destruction of the data.

RELEVANT LINKS:

D. Meetings

City officials sometimes have difficulty interpreting their responsibilities under the MGDPA when they are applied to the meetings held by their elected and appointed city officials. This often comes up in the context of personnel data, but would extend to any other not public data as well.

1. Open Meeting Law

Minn. Stat. ch. 13D.
Rupp v. Mayasich, 533 N.W.2d 893 (Minn. Ct. App. 1995).

The Minnesota Open Meeting Law (OML) generally requires that all meetings of public bodies be open to the public. This presumption of openness serves three basic purposes:

- To prohibit actions from being taken at a secret meeting where it is impossible for the interested public to become fully informed concerning decisions of public bodies, or to detect improper influences.
- To ensure the public's right to be informed.
- To afford the public an opportunity to present its views to the public body.

Minn. Stat. § 13D.05.
Minn. Stat. § 13.03, subd. 11.

DPO 09-012.

With a few exceptions, meetings may not be closed to discuss not public data. Cities may discuss not public data at a meeting without liability or penalty, 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.

See LMC information memo, *Meetings of City Councils*.

DPO 12-008.

Cities should use discretion when discussing not public data at an open meeting. City officials should limit the distribution of materials containing not public data, or refer to paragraphs or page numbers in the data during discussions. When closing any meeting, it is important to follow the specific procedures set out in the OML. A closed meeting cannot be adjourned or otherwise concluded (recessed or continued). It must first be reconvened in open form.

a. Classifications

Minn. Stat. § 13D.05, subd. 1(c).

DPO 02-013.

Cities often worry that if they discuss not public data at an open meeting, the data will become public, or that they will be violating the MGDPA by releasing not public data at an open meeting. This is not the case. Data discussed at an open meeting retains the data's original classification (but a record of the meeting, regardless of form, is public).

RELEVANT LINKS:

b. Mandatory closed meetings

Minn. Stat. § 13D.05, subd. 2.

Certain data may not be discussed at an open meeting. A meeting must be closed before discussing:

Minn. Stat. § 13.82, subd. 7.

- Data that would identify alleged victims or reporters of criminal sexual conduct, domestic abuse, or maltreatment of minors or vulnerable adults.
- Active investigative data.
- Internal affairs data (allegations of law enforcement personnel misconduct).

Minn. Stat. § 13.32.
Minn. Stat. § 13.3805, subd. 1.
Minn. Stat. § 13.384.
Minn. Stat. § 13.46, subd. 2.

- Educational data.*
- Health data.*
- Medical data.*
- Welfare data.*

Minn. Stat. § 13.46, subd. 7.
Minn. Stat. §§ 144.291-.298.

- Mental health data. *
- An individual's medical records.*

*Where specifically classified as not public in state statutes.

Minn. Stat. § 13D.05, subd. 2(b).

DPO 96-062.

DPO 03-020.

Meetings must be closed for preliminary consideration of allegations or charges against an individual subject to the body's authority (such as a city employee). However, the meeting must be open at the request of the individual who is the subject of the meeting.

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

c. Discretionary closed meetings

Minn. Stat. § 13D.05, subd. 3.

The city council may close a meeting:

- To evaluate the performance of an individual subject to its authority.
- Under the attorney-client privilege.
- In regard to the purchase or sale of real or personal property.

DPO 08-001.

- To receive security briefings and related reports.

Most likely, at least some of the data discussed at meetings closed at the council's discretion will be classified as not public.

RELEVANT LINKS:

2. Minutes and recordings

Minn. Stat. § 15.17, subd. 4.

DPO 05-029.

See LMC information memo, *Meetings of City Councils*.

Minutes and audio/video recordings of city meetings are widely understood to be public data and available for inspection or copying upon request. As a general rule, if a council (or other official body) chooses to record all meetings as a standard practice, the recordings are public data, unless other applicable law provides otherwise.

However, cities may be unsure how to classify draft or unofficial (not adopted) minutes, or a clerk's notes used in preparation of official minutes. There is also some confusion about the proper classifications for documents related to meetings that are closed (or include a closed portion thereof).

a. Draft documents

DPO 00-030.

DPO 02-026.

DPO 04-018.

Draft documents (including notes used to prepare city records) are government data and subject to the MGDPA. Nothing in the MGDPA specifically classifies draft or unofficial minutes as not public, so they are presumably public and should be released upon proper request to a responsible authority. There is nothing in the MGDPA that prevents draft or unofficial minutes from being identified as such when released, so as to distinguish from subsequent (and perhaps modified) versions.

b. Closed meetings

Minn. Stat. § 13D.05, subd. 1(c).

The MGDPA does not specifically address the classification of any minutes taken at a closed meeting. However, the OML does specifically provide that a record of an open meeting, regardless of the record's form, is public.

Minn. Stat. § 13D.05, subd. 1(d).

Minn. Stat. § 13D.03, subd. 2.

DPO 10-001.

Vik v. Wild Rice Watershed Dist., No. A09-1841 (Minn. Ct. App. Aug. 10, 2010) (unpublished decision).

With the exception of meetings closed pursuant to the attorney-client privilege, all closed sessions must be electronically recorded at the city's expense. The OML provides some specific guidelines regarding accessibility to those recordings.

For example, the record of a meeting closed to discuss strategies for labor negotiations is accessible to the public after the contracts are signed. When the OML doesn't specifically provide guidance, city officials will have to decide who, based upon the subject matter of the recording and its proper classification, has the right to access the recording.

RELEVANT LINKS:

E. Property

1. Complaints and violations

Minn. Stat. § 13.44, subd. 1.

DPO 00-057.
DPO 08-003.

The identities of individuals who register complaints with the city concerning violations of state laws or local ordinances related to the use of real property are classified as confidential data.

Minn. Stat. § 13.44, subd. 2.

Minn. Stat. § 13.39, subd. 2.

Minn. Stat. § 13.82, subd. 7.

Code violation records pertaining to a particular parcel of real property and the buildings, improvements, and dwelling units located on it that are kept by any state, county, or city agency charged by the governing body of the appropriate government entity with the responsibility for enforcing a state, county, or city health, housing, building, fire prevention, or housing maintenance code are public data unless currently classified as civil or criminal investigative data.

2. Appraisals

a. Real property

Minn. Stat. § 13.44, subd. 3(a).
State v. KQRS, Inc., No. A03-426 (Minn. Ct. App. Jan. 27, 2004) (unpublished decision).

A.G. Op. 852 (Apr. 13, 2004).
DPO 10-010.
Minn. Stat. § 13.44, subd. 3(b).

Minn. Stat. § 13.44, subd. 3(c).

Estimated or appraised values of individual parcels of real property that are made by city personnel (or by independent appraisers acting for the city) for the purpose of selling or acquiring land through purchase or condemnation are classified as confidential data on individuals or protected nonpublic data. Similarly, appraised values of individual parcels of real property that are made by appraisers working for owners or contract purchasers who have received an offer to purchase their property from the city are classified as private data on individuals or nonpublic data.

Appraisals become public when:

- Submitted to a court-appointed condemnation commissioner.
- Presented in court in condemnation proceedings.
- The negotiating parties enter into an agreement for the purchase and sale of the property.
- The city council authorizes with a majority vote.

b. Personal property

Minn. Stat. § 13.44, subd. 4.

Preliminary and final market value appraisals of personal and intangible property owned by the city, made by city personnel (or by an independent appraiser acting on behalf of a city), are classified as not public until either:

- A purchase agreement is entered into.
- The parties negotiating the transaction exchange appraisals.

RELEVANT LINKS:

F. Utilities

Cities often have questions concerning the proper classifications of various utility-related data.

1. Customer data

a. Municipal electric utilities

Minn. Stat. § 13.685.

Data on customers of municipal electric utilities are private data on individuals or nonpublic data and may only be released to:

- A law enforcement agency in connection with an investigation.
- Schools to compile pupil census data.
- The Metropolitan Council for use in studies or analyses required by law.
- A public child support authority to establish or enforce child support.
- A person where use of the data directly advances the general welfare, health, or safety of the public.

Minn. R. 1205.0400, subp. 2.
See Section III A2, *Private data*.

Note: Aside from the sharing of information as authorized above, the law limits access to private data. Only the subject of the data and city staff whose work assignments reasonably require access may view it. Accordingly, care should be taken to assure that only those parties may access private data and that it is not openly displayed. For instance, inclusion of this information on postcards may inadvertently provide others with access to this private data.

b. Other city utilities

DPO 00-058.

DPO 02-031.

DPO 03-047.

Data related to any other city-operated utilities (such as water, sewer, or natural gas) is not given any specific designation and is presumed to be public. Since the majority of cities do not operate electric utilities, data on their utility customers will generally be public. However, when electric utility data is combined with another city utility (such as water and sewer), all of the utility information might be classified as private together.

2. Design and operation

Minn. Stat. § 13.37.

DPO 02-014.

Cities have the ability and responsibility to protect the integrity of their utilities for the public's health, welfare, and safety. If the responsible authority determines that the disclosure of any utility-related data "would be 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," then the data may properly be classified as not public security information.

RELEVANT LINKS:

The types of information could include:

- The design, operation of, or methods of access to any equipment, building, or other facility.
- The hardware or software used in providing public utility services.
- Data describing the design, maintenance, or operation of facilities and infrastructure.

DPO 02-014.

A city must have reason to believe that disclosure of such data would likely lead to substantial jeopardy. The entity cannot make this determination arbitrarily; it must be based on reasoned analysis.

3. Disconnection notice

Minn. Stat. § 216B.0976.

A public utility, cooperative electric association, or municipal utility must provide notice to a city (statutory or home rule) of the disconnection of a customer's gas or electric service upon written request from Oct. 15 through April 15. Data on customers provided to cities are classified as private data on individuals or nonpublic data.

DPO 09-002.

G. Contact information

Minn. Stat. § 13.03, subd. 1.

Cities often collect telephone numbers, home addresses, e-mail addresses, and other types of contact or personal information from citizens on license forms, building permits, and various other materials. Because telephone numbers and related types of data are not generally classified in the MGDPA, most are public and accessible (information on city personnel is, however, presumed private).

Minn. Stat. § 13.43, subd. 1.

If cities are uncomfortable releasing personal or contact information, they should consider whether there is a real need for the data prior to collection, and limit collection as much as possible.

DPO 98-046.

DPO 01-029.

See Section VIII-I *Security information*.

If, in limited circumstances, a city has specific reason to conclude that dissemination of the data would be likely to substantially jeopardize information, possessions, individuals, or property, then that specific data might be classified not public.

This is not an easy standard to meet. Such a determination would need to be made on a case-by-case basis.

1. Notification and subscription lists

Minn. Stat. § 13.356.

Certain contact information a city collects, maintains, or receives on individuals for the purposes of notification and subscription lists is classified as private data under the MGDPA. This law applies to lists like snow emergency notices, newsletters, monthly crime reports, and other general information sent by cities to anyone requesting it.

RELEVANT LINKS:

Minn. Stat. § 13.356(c).

The information classified as private includes telephone numbers, email addresses, and internet usernames, passwords, and similar internet account related data. Despite the private classification of those data, however, the names of individuals on these lists remain public data. It is important to know that data collected under this law may only be used for the specific purpose for which the individual provided the data.

Minn. Stat. § 13.04.

Minn. Stat. § 13.356.

Note: A Tennessen warning is ordinarily required in order to obtain private or confidential data from individuals, however, contact information collected for notification and subscription lists is exempt from the general Tennessen warning requirement.

2. Crime prevention volunteers

Minn. Stat. § 13.37.

The home and mailing addresses, telephone numbers and e-mail addresses of volunteers who participate in community crime prevention programs are classified as private or nonpublic data, but may be disseminated to other program volunteers.

See Section VIII-I *Security information*.

3. Recreational programs

Minn. Stat. § 13.548.

See Section VIII-L *Social and recreational data*.

DPO 11-014.

Enrollment data that identifies the names, addresses, telephone numbers, or any other data that identifies an individual enrolled in city recreational or social programs are private data. However, data that is collected or maintained in the course of participation in recreational activities is public and includes, by implication, the recorded names of participants.

4. Unlisted phone numbers

See Section VIII-I *Security information*.

Cities collect unlisted phone numbers, and some city officials feel uncomfortable giving out this information when requested.

An unlisted designation by the phone company does not change the classification of the phone number data when it is in the possession of the city.

5. Parking spaces

Minn. Stat. § 13.37, subds. 1(c), 2.

The following data collected on an applicant for, or lessee of, a parking space is private data on individuals or nonpublic data:

- Residence address.
- Home and work telephone numbers.
- Work hours (beginning and ending).
- Place of employment.
- Location of parking space.

RELEVANT LINKS:

Minn. Stat. ch. 5B.

Minn. R. ch. 8290.

Minnesota Secretary of State.

Minn. Stat. § 5B.05.

Minn. Stat. § 5B.07.

6. Safe at Home Program

Safe at Home is a program offered by the Secretary of State's office in collaboration with local victim service providers. This program is designed to help survivors of domestic violence, sexual assault, stalking, or others who fear for their safety though a confidential address. Participants are provided a mailing address, and any correspondence is forwarded to their actual mailing address, which is not disclosed. When a participant presents his or her designated address, it must be accepted.

Data related to applicants, eligible persons, and program participants is private data on individuals. A program participant's name and address maintained by a local government entity in connection with an active investigation or inspection of an alleged health code, building code, fire code, or city ordinance violation allegedly committed by the program participant are private data.

7. Lodging Tax Data

Minn. Stat. § 13.495.

Many Minnesota cities impose a lodging tax on lodging businesses within the city. Data, other than basic taxpayer identification data, collected from taxpayers under a lodging tax ordinance are nonpublic.

H. Social Security numbers

See DPO, Collection of Social Security Numbers. Minn. Stat. § 13.355. *AFSCME v. Grand Rapids Pub. Utils. Comm'n*, 645 N.W.2d 470 (Minn. Ct. App. 2002).

State and federal laws impose restrictions on the collection and use of Social Security numbers. Security numbers collected or maintained by a city are private data on individuals. Accordingly, a Social Security number may not be released to the public, except where specifically authorized by law.

If the city does not need Social Security numbers, they shouldn't be collected. Cities may also not use an individual's Social Security number as the employee identification number. The responsible authority should make a decision in each circumstance about whether to collect or disseminate Social Security numbers.

1. Federal Privacy Act

Minn. Stat. § 13.43, subd. 2(a)(1).

Manson v. State, 613 N.W.2d 778 (Minn. Ct. App. 2000).

5 U.S.C. § 552a note 7.

DPO 04-048.

Federal law requires that whenever a Social Security number is collected, an individual must be informed:

- Whether the disclosure of the number is mandatory or voluntary.
- The statutory or other authority for requesting the number.
- How the number will be used.

RELEVANT LINKS:

2. Tennessen warnings

Minn. Stat. § 13.04, subd. 2.

DPO 02-015.
DPO 04-016.

See Section V-B-1 *Tennessen warning*.

A Tennessen warning is required any time the city collects private or classified information for an individual. Because Social Security numbers are classified as private data by the MGDPA, an individual must also receive a Tennessen warning at the time the data is collected. At a minimum, the warning must provide:

- The purpose and intended use of the data.
- Whether the individual is required to provide the number or may refuse to do so.
- Any known consequences for refusing to provide the number.
- The identities of other persons or entities outside the city authorized by state or federal law to receive the number.

I. Security information

Minn. Stat. § 13.37, subd. 1(a).

Security information is government data that, if disclosed, would be likely to substantially jeopardize the security of information, possessions, individuals, or property against:

- Theft.
- Tampering.
- Improper use.
- Attempted escape.
- Illegal disclosure.
- Trespass.
- Physical injury.

Minn. Stat. § 13.37, subd. 1(a).

Minn. Stat. § 13.37, subd. 2(a).

Security information includes checking account numbers, crime prevention block maps and lists of volunteers (and home and mailing addresses, telephone numbers and e-mail addresses) who participate in community crime prevention programs. Security information is classified as private or nonpublic data.

1. Substantially jeopardize

DPO 98-046.

DPO 02-014.

What it means to "substantially jeopardize" security under the MGDPA is not clearly defined and, as a result, cities do have some discretion in making the determination. As a general rule, when determining whether to withhold data under the security exception, the responsible authority cannot rely on a general security risk, but rather must know of a specific risk to a specific individual or group if the data at issue were to be released.

DPO 00-010.

This must be done on a case-by-case basis and the city must be able to document or support its position.

RELEVANT LINKS:

a. Employee information

DPO 00-071.

DPO 01-006.

The commissioner has concluded that a public employer may withhold the name of a specific employee, which is usually public data, from a specific requestor if the public employer determines that the release of the employee's name to that requestor would substantially jeopardize the security of the individual employee.

b. Building plans

DPO 00-010.

DPO 01-029.

DPO 11-011.

The commissioner has also concluded that plans required for the issuance of a building permit under certain circumstances might be classified as security data. One possible example would be the situation where the building plans reveal the location of a hidden safe or security system details.

c. Emergency response

Cities occasionally receive requests related to the city's disaster or emergency response plan (or even for a copy of the entire plan itself). Although cities want to assure the general public that it is appropriately prepared for a natural disaster or other devastating event, cities may struggle to balance this against the need to protect the data from getting into the hands of a person or group with questionable or dangerous intentions.

Northwest Publications, Inc. v. City of Bloomington, 499 N.W.2d 509 (Minn. Ct. App. 1993).

It is likely that a plan would contain both public and not public data. If possible, a plan may be redacted for any not public data and released in an amended form.

DPO 10-003.

However, if public and not public data are so inextricably intertwined within such a plan that it is effectively impossible for them to be separated, it is perhaps permissible for the city to withhold the entire document, including the public data. In these situations, it is important to get legal advice from the city's attorney.

Minn. Stat. § 13.82, subd. 25.

DPO 01-068.

Some cities have determined that the data contained in emergency or disaster response plans reflects deliberative processes or investigative techniques of law enforcement agencies and as such, is not public data. As the commissioner of the Department of Administration has not offered an opinion concerning the appropriateness of this determination, cities should consult their city attorney before withholding data on this basis.

RELEVANT LINKS:

2. Dissemination

Minn. Stat. § 13.37, subd. 3(a).

Crime prevention block maps and names, home addresses, and telephone numbers of volunteers who participate in community crime prevention programs may be disseminated to volunteers participating in crime prevention programs. The location of a National Night Out event is public.

Minn. Stat. § 13.37, subd. 3(b).

Security information may be made accessible to any person or entity, or to the public, if the city determines that the access will aid public health, promote public safety, or assist law enforcement.

The responsible authority must make this determination on a case-by-case basis after consulting with the appropriate chief law enforcement officer, emergency manager, or public health official.

Minn. Stat. § 13.37.

The responsible authority may deny a data request based on the determination that the data are security information. A short description about the necessity for classifying the data as security information must be provide by the responsible authority if requested.

J. Trade secret information

Minn. Stat. § 13.37, subd. 1(b).

Trade secret information is government data, including a formula, pattern, compilation, program, device, method, technique, or process that:

- Was supplied by the affected individual or organization.
- Is the subject of efforts by the individual or organization that are reasonable under the circumstances to maintain its secrecy.
- Derives independent economic value—actual or potential—from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use.

Minn. Stat. § 13.37, subd. 2(a).

Trade secret information is classified as private or nonpublic, but needs to be applied to city data narrowly on a case-by-case basis. The city bears the burden of proving that the data at issue is actually trade secret information.

Prairie Island Indian Cmty. v. Minn. Dep't. of Public Safety, 658 N.W.2d 876 (Minn. Ct. App. 2003).
DPO 99-035.
DPO 03-009.

The commissioner of Administration and our Minnesota courts have analyzed claims of the trade secret exception by looking at each element of the definition in the MGDPA when making a determination of whether the data at issue is in fact trade secret information.

1. Site plans

DPO 01-029.

In addressing the claims of a private property owner's assertion that data about the property, such as site plans or designs, is itself the owner's private property, the commissioner has concluded that such a claim is inadequate to prove that the data is trade secret information.

RELEVANT LINKS:

DPO 00-010.

2. Building permits

The commissioner has also concluded that plans required for the issuance of a building permit might be classified as trade secret information under certain circumstances.

3. Redaction

Prairie Island Indian Cmty. v. Minn. Dep't. of Public Safety, 658 N.W.2d 876 (Minn. Ct. App. 2003).

DPO 03-017.

As with security information, it is possible that public data could be so inextricably intertwined with trade secret information that it would be permissible for a city to withhold an entire document. However, to whatever extent possible, trade secret information should be redacted and public data released upon request.

K. Copyrights

Federal Copyright Act (FCA), Title 17, U.S. Code.
U.S. Copyright Office.

Cities maintain documents and other information protected by the Federal Copyright Act. Since individuals may generally inspect and receive copies of public government data, city officials worry about the possible consequences when the data requested is copyrighted.

1. Third party ownership

DPO 00-042.
DPO 02-012.
DPO 08-009.

For example, cities often collect copyrighted blueprints as part of a building permit application process. Although the permit data is generally public, the city should not release copyrighted data without permission, as the release could infringe on the copyright owner's rights.

Inspection of copyrighted data is permissible, but copying (without permission) is not.

2. Government works

A.G. Op. 852 (Dec. 4, 1995).

The Minnesota attorney general has given the opinion that government entities may not assert their copyright ownership to deny members of the public their right to inspect and copy public government data. Certain restrictions may be placed upon the use of the data, such as a prohibition on the third party publishing the information without obtaining a license from the copyright owner.

L. Social and recreational programs

Minn. Stat. § 13.548.

DPO 08-025.

Cities maintain membership lists and other data in regard to the use of their parks, beaches, ice arenas, community centers, and similar facilities. The following data collected and maintained for the purpose of enrolling individuals in recreational and other social programs are private:

RELEVANT LINKS:

- Names.
- Addresses.
- Telephone numbers.
- Any data that describes the health or medical condition of the individual, family relationships, and living arrangements of an individual or which are opinions as to the emotional makeup or behavior of an individual.

DPO 99-028.

The commissioner has concluded that not all activities related to a city's recreational services require enrolling in a program and therefore do not fall under this exception. Examples of public data may include the identity of individuals who:

- Reserve and pay for ice time.
- Reserve and pay for space in community centers or city parks.
- Obtain permits for park use.
- Obtain season passes for beaches.
- Purchase memberships in city recreation centers.

DPO 99-028.

However, data from scholarship applicants for enrollment in a program may be classified as private.

M. Licenses

DPO 09-005.

Cities occasionally receive requests for data related to city licenses (such as pet licenses). Some are reluctant to give out this data, especially when they suspect that the requestor is going to use the data to send advertisements to license holders.

However, nothing in the MGDPA specifically classifies all license-related data as not public.

Minn. Stat. § 13.05, subd. 12.

Minn. R. 1205.0300, subp. 2.

See Section V-B-1 *Tennessen warning*.

Because a responsible authority is not allowed to ask about the proposed use of requested data (and not allowed to withhold data based on knowledge or suspicion of a proposed use), there is no legal basis to withhold the data. It is entirely appropriate for the responsible authority to provide a license applicant with a warning (similar to a Tennessen warning), informing the applicant of the public nature of the data and the possibility that it would be provided upon request.

Minn. Stat. § 13.41.
Minn. Stat. § 13.411.

DPO 95-050.

Sections in the MGDPA do classify certain types of licensing data as not public. However, they only apply to state agencies, not city licensing activities.

RELEVANT LINKS:

N. Permits

1. Generally

Minn. Stat. § 13.37.

See Section VIII-I *Security information*.

See Section VIII-J *Trade secret information*.
See Section VIII-K *Copyrights*.

Applications for permits (such as building permits), or the permits themselves, are not specifically classified and are therefore presumed to be public data and generally accessible.

Although some information submitted as part of applications (perhaps as security system information in a building plan) may be classified as security, trade secret, or copyrighted data, it is unlikely that all permit-related data could be withheld.

2. Firearms

Minn. Stat. § 624.714, subd. 2(d).
Minn. Stat. §§ 624.712-.719.

Minn. Stat. § 13.87, subd. 2.

DPO 10-005.

Some police chiefs process applications for personal firearm permits, including applications under the Minnesota Citizens' Personal Protection Act of 2003 (commonly referred to as the "conceal-and-carry" law). All data pertaining to the purchase or transfer of firearms and applications for permits to carry firearms that are collected by cities are private data.

O. Business contracts

DPO 03-027.
DPO 12-009.

City contracts and related business information can present some unique data practices challenges for the city, as well as the contracting parties. Contracts are public, but some not public classifications may apply to the contracting process.

1. Financial assistance

Many cities offer financial assistance to attract and retain businesses within their communities.

While these businesses may expect that the information they provide as part of the application process will be not public (they may even stamp the data "confidential" themselves), most of the data provided will be classified as public. Therefore, it is important to make this clear before the business applies for assistance.

a. Assistance requested

Minn. Stat. § 13.591, subd. 1.

DPO 09-009.
DPO 11-016.

The following information, when submitted to a government entity by a business requesting financial assistance (or a benefit financed by public funds), is private or nonpublic data:

- Financial information about the business (including credit reports).
- Financial statements.

RELEVANT LINKS:

- Net worth calculations.
- Business plans.
- Income and expense projections.
- Balance sheets.
- Customer lists.
- Income tax returns.
- Design, market, and feasibility studies not paid for with public funds.

Minn. Stat. § 13.03, subd. 1.

Any other information provided in support of the request for financial assistance is public data.

b. Assistance received

Minn. Stat. § 13.591, subd. 2.
DPO 09-009.

When a business receives financial assistance or a benefit, the following financial data remains not public:

- Business plans.
- Income and expense projections (not related to the financial assistance provided).
- Customer lists.
- Income tax returns.
- Design, market, and feasibility studies not paid for with public funds.

DPO 09-023.

See Section VIII-O-1-a *Assistance requested*.

If an applicant does not receive financial assistance (or other benefit financed by public funds), all of the data classified not public (when assistance is requested) remains not public.

2. Competitive bidding

See LMC information memo, *Competitive Bidding Requirements in Cities*.
Minn. Stat. § 13.591, subd. 3(a).

When cities use the competitive bidding process, sealed bids are not public until the time and date specified in the solicitation that bids are due (the number of bids received is also not public).

Minn. Stat. § 13.37, subd. 2(a).

After this time, the name of the bidder and the dollar amount specified become public. All other data in a bidder's response to a bid is not public data until completion of the selection process.

Minn. Stat. § 13.591, subd. 3(a).

Minn. Stat. § 13.37.

DPO 08-021.

"Completion of the selection process" means the city has completed its evaluation and has ranked the responses. After a government entity has completed the selection process, all remaining data submitted by all bidders is public (with the exception of trade secret data).

Minn. Stat. § 13.591, subd. 3(a).

If all bids are rejected prior to completion of the selection process, all data (other than the name of the bidder and the dollar amount specified in the response) remains not public until either:

RELEVANT LINKS:

- The selection process is completed after a re-solicitation of bids.
- The city decides to abandon the purchase.

Minn. Stat. § 13.591, subd. 3(a).

If the rejection occurs after the completion of the selection process, the data remains public. If a re-solicitation of bids does not occur within one year of the bid opening date, the remaining data becomes public.

3. Proposals

Minn. Stat. § 13.591, subd. 3(b).

When competitive bidding is not used, cities will often issue requests for proposals (RFPs).

Data submitted by a business to a city in response to an RFP is not public data until the time and date specified in the solicitation that proposals are due. At that time, the name of the responder becomes public. All other data in a response to an RFP is private or nonpublic data until completion of the evaluation process.

Minn. Stat. § 13.591, subd. 3(b).

"Completion of the evaluation process" means that the city has completed negotiating the contract with the selected vendor. After the city has completed the evaluation process, all remaining data submitted by all responders is public, with the exception of trade secret data.

Minn. Stat. § 13.591, subd. 3(b).

If all responses to an RFP are rejected prior to completion of the evaluation process, all data, other than the names of the responders, remains not public until either:

- The selection process is completed after a re-solicitation of proposals.
- The city decides to abandon the purchase.

Minn. Stat. § 13.591, subd. 3(b).

If the rejection occurs after the completion of the evaluation process, the data remains public. If a re-solicitation of proposals does not occur within one year of the proposal opening date, the remaining data becomes public.

DPO 03-014.

The commissioner has concluded that a business submitting a proposal may consent to the release of non-trade secret data prior to the opening of all proposals, so long as a city informs the business of the possibility that such data could be released during the time that the statute classifies the data as not public.

4. "Proprietary" information

5 U.S.C. § 552(b)(4).

See Section VII *Other laws to consider*.

A statement that data submitted in support of a bid or proposal is copyrighted, "proprietary," or otherwise protected is insufficient to prevent public access to the data contained in the bid. This is important because, while the Federal Freedom of Information Act does allow data to be withheld if marked "proprietary," Minnesota state law is more restrictive.

RELEVANT LINKS:

Minn. Stat. § 13.37, subd. 1(b).

See Section VIII-J *Trade secret information.*

Minn. Stat. § 13.37, subd. 2 (a).

When issuing a request for bids or proposals, a city may indicate the distinction between state and federal law and the need to clearly mark any data claimed to be a trade secret. Potential respondents can be instructed to submit a separate letter to the responsible authority explaining how the data they claim is trade secret data meets the criteria.

It is then the duty of the responsible authority to determine the appropriate classification.

5. Data practices responsibilities

Minn. Stat. § 13.05, subd. 6.

Documents related to city contracts can present some unique challenges.

Whenever a city enters into a contract, and the contract requires that the city provide data to the contracting parties, the entity receiving the government data is required to maintain the data pursuant to the MGDPA.

a. Privatization clause

Minn. Stat. § 13.05, subd. 11(a).

DPO 09-022.

DPO 11-001.

Whenever a city enters into a contract with a private person or entity, including independent contractors, and the contract is to perform any city function, the city is required to include a privatization clause. This clause sets out terms in the contract that make it clear that all of the data created, collected, received, stored, used, maintained, or disseminated by the private person or entity in the performance of those functions is subject to the requirements of the MGDPA and that the private person or entity must comply with those requirements as if it were a government entity.

WDSI, Inc. v. County of Steele, 672 N.W.2d 617, 622 (Minn. Ct. App. 2003).

DPO 01-075.

Even if the contract contains no privatization clause, if the contract went into effect after Aug. 1, 1999, such a clause is inferred to give effect to the Legislature's intent that private entities performing government functions be subject to the MGDPA.

b. Public access

DPO 99-041.

DPO 05-034.

DPO 04-009.

A private company performing city functions may be required to respond to data requests in the same manner as the city itself. For example, if a city enters into a contract with a private company to operate its community center, that private company is also subject to the MGDPA. One could argue that private companies should:

- Appoint and provide public notice of the person acting as their "responsible authority."
- Adopt procedures related to government data.
- Maintain data in the same manner as the government entities.

RELEVANT LINKS:

Minn. Stat. § 13.05, subd. 11(b).
WDSI, Inc. v. County of Steele, 672 N.W.2d 617, 622 (Minn. Ct. App. 2003).

DPO 99-039.

DPO 11-005.

However, unless there are contract provisions addressing the question of public access, the contracted private person or entity does not have a duty to provide access to the public if the public data is available from the city. If a city receives a request for data, the city may, but is not required to, obtain the data from the contracted private person or entity. A city is not allowed to charge a higher copy cost because the data happens to be maintained by the private person or entity.

c. Disclosure of data breach

Minn. Stat. § 13.055.

Cities are required to disclose, investigate and report on any unauthorized access of private or confidential data on individuals held by a contractor.

d. Liability

Minn. Stat. § 13.08.

The civil remedies provided in the MGDPA that a city would be subject to also apply to the private person or entity.

P. Attorneys

Government data in the possession of an in-house or contract city attorney should be classified and maintained pursuant to the MGDPA. Only under specific circumstances would government data in the hands of a city attorney have any special considerations attached to it. However, documents and related data concerning the work of the city attorney may be subject to special considerations, as well as not public classifications. As these are often very complex issues, a responsible authority should always seek the advice of the city attorney when specific questions arise.

1. City attorneys

Minn. Stat. § 13.393.

As a general rule, the use, collection, storage, and dissemination of data by an attorney acting in a professional capacity for a city is not governed by the MGDPA, but instead, is governed by statutes, rules, and professional standards concerning discovery, production of documents, introduction of evidence, and professional responsibility.

DPO 05-009.

DPO 01-041.

DPO 02-039.

DPO 96-038.

The MGDPA does not classify attorney-related data. Instead, it excludes certain data created, collected, maintained, and/or disseminated by a city's attorney from the provisions of the MGDPA. If data is not subject to the MGDPA, an individual does not have the right to access it. It is important for the responsible authority to carefully analyze the data (as well as the circumstances surrounding any data) to determine whether or not it is subject to the MGDPA.

RELEVANT LINKS:

a. Attorney-client privilege

Minn. Stat. § 595.02, subd. 1(b).

Kobluk v. Univ. of Minnesota, 574 N.W.2d 436, 441 (Minn. 1998).

City Pages v. State of Minnesota, 655 N.W.2d 839, 845 (Minn. Ct. App. 2003).

DPO 00-074.

Some communications between an attorney and a client are subject to attorney-client privilege. However, not every word spoken or written between an attorney and a client is privileged and it is not always readily apparent what communication qualifies and what does not.

Simply marking a document as "confidential" or "privileged" does not necessarily affect its classification under the MGDPA, nor does it automatically subject it to the protection of the attorney-client privilege. Likewise, delivering an otherwise unprivileged, pre-existing document to the city attorney would not afford that document any protection. The attorney-client privilege must be balanced against the public's right to access government data.

Kobluk v. Univ. of Minnesota, 574 N.W.2d 436, 441 (Minn. 1998).

To qualify for protection under the attorney-client privilege, a communication must meet the following criteria:

- Legal advice (of any kind) is sought from a professional legal advisor (in his or her capacity as such).
- The communication is related to the legal advice.
- The communication is made by the client in confidence.
- The client insists it is permanently protected from disclosure by the client or by the legal advisor (but the protection may be waived).

DPO 98-036.

b. Work product

City Pages v. State of Minnesota, 655 N.W.2d 839, 845 (Minn. Ct. App. 2003).

DPO 98-036.
DPO 06-024.
DPO 05-041.
DPO 05-009.

Documents or other data created by an attorney for a city might also be protected by the attorney work-product doctrine. "Work product" is generally understood to include an attorney's mental impressions, trial strategy, and legal theories related to preparing a case for trial. Whether documents were prepared in anticipation of litigation is a factual determination and should be decided on a case-by-case basis. If a document or other data created by an attorney is something that would be created in the ordinary course of business, then it likely would not qualify for protection under the doctrine.

Q. Litigation

DPO 04-073.
DPO 04-074.
DPO 96-038.

City officials struggle with their role in providing access to government data when the city is involved in an active litigation. Individuals cannot be denied access to data simply because they are involved in litigation with the city, or required to make any data requests through their attorney.

RELEVANT LINKS:

1. Discovery

Minn. Stat. § 13.03, subd. 6.

DPO 94-016.

Erickson v. MacArthur, 414 N.W.2d 406 (Minn. 1987).

If a city opposes discovery of government data or release of data pursuant to court order on the grounds that the data is classified as not public, the party seeking access may bring before the appropriate presiding judicial officer, arbitrator, or administrative law judge an action to compel discovery. In order to balance these interests, the data will be reviewed in camera.

Discovery of not public data is subject to a two-part analysis:

Northern Inns Ltd. v. County of Beltrami, 524 N.W. 2d 721 (Minn. 1994).

- Is the data discoverable or releasable pursuant to the rules of evidence and of criminal, civil, or administrative procedure appropriate to the action?

If the presiding officer concludes that the data is discoverable, he or she must then determine:

EOP-Nicollet Mall, L.L.C. v. County of Hennepin, 723 N.W.2d 270 (Minn. 2006).

- Whether the benefit to the party seeking access to the data outweighs any harm to the confidentiality interests of the entity maintaining the data or of any person who has provided the data or who is the subject of the data or to the privacy interest of an individual identified in the data.

Minn. Stat. § 13.03, subd. 6.

In making the decision, the presiding officer must consider whether notice to the subject of the data is warranted and, if warranted, what type of notice must be given. The presiding officer may fashion and issue any protective orders necessary to ensure proper handling of the data by the parties. There are also special considerations related to videotapes of child victims or alleged victims of physical or sexual abuse.

Minn. Stat. § 611A.90, subd. 2(b).

2. Subpoenas

Minn. Stat. § 13.03, subd. 6.

Minn. R. 1205.0100, subp. 5.

DPO 97-051.

Data may become an issue in litigation even though no action had been brought to compel discovery. Nothing in the MGDPA or accompanying rules limits the rights of a party to a civil or criminal case to seek documents or other data by subpoena or other judicial order. If a city receives a subpoena for private or confidential data or a subpoena requiring a city staff member or city official to testify concerning private or

confidential data, the responsible authority should take appropriate steps to inform the court of the statutory provisions, rules, or regulations that restrict the disclosure of the information.

Under these circumstances, it would be appropriate for the responsible authority to seek advice from the city attorney and request to submit the data for an in camera review by the court prior to releasing the data.

RELEVANT LINKS:

EEOC v. Hennepin County, 623 F. Supp. 29 (D. Minn. 1985).

There is also a wide body of law that covers responding to subpoenas from state or federal agencies. Accordingly, it is imperative that a responsible authority seek advice from the city attorney before responding. When dealing with a subpoena from a federal agency—such as the Equal Employment Opportunity Commission (EEOC), the IRS, the Department of Labor, etc.—a responsible authority should determine how applicable state and federal laws interact under the circumstances. Generally, state privacy statutes are preempted by federal administrative agency subpoenas.

R. Electronic data

Minn. Stat. § 13.02, subd. 7.

DPO 00-019.
DPO 01-090.
DPO 99-032.
DPO 00-067.

The MGDPA applies to all government data, regardless of its physical form, storage media, or location. All government data, including electronic data, must be maintained for easy access and convenient use. While cities have an affirmative duty to maintain electronic data pursuant to the MGDPA, this becomes more and more difficult as technology or systems evolve and develop. A city's obligations, however, remain, even if it requires:

- Additional time and resources necessary to update city records and other data to current technology.
- Using outside vendors to respond to data practices requests.
- Retaining electronic data for shorter periods of time (records retention schedule notwithstanding).

See Section IX *Records retention*.

1. Remote locations

Minn. Stat. § 13.02, subd. 7.
DPO 95-008.
DPO 95-013.

As technology evolves, more and more city staff and officials are working from home or other remote locations. As a result, government data is being created or stored offsite and on personal computers. The fact that the data is not on a city computer (or on a computer located within a city facility) does not change its status as government data, nor does it relieve the responsible authority of his or her duties to maintain easy accessibility to government data and to respond promptly to data requests.

2. Computer use policies

LMC information memo, *Computer and Network Loss Control.*

Cities should consider adopting a computer use policy. Computer use policies help regulate:

- The use of non-city computers.
- The storage of government data on personal computers.
- Personal use by city staff or officials (including a "no privacy" disclaimer).

RELEVANT LINKS:

DPO 01-075.

See Section VIII-A-3 *Personal data*.

Personal data (including e-mails) on a city computer would not be government data upon its creation, and a city would have no obligation to provide access to or maintain the data. However, because the personal data would likely have to be separated from government data in order to respond to a data request, such data might interfere with the city meeting its responsibilities to maintain government data so that it is easily accessible.

DPO 02-049.

"Investigating Misuse of City Computers," *Minnesota Cities* (Jan. 2005, p. 25).

Personal data on a city computer could become government data if the data were to be used as the basis for discipline against a city employee. For example, if a city brings charges against an employee for improper use of a city computer, e-mails or other personal electronic data on the city computer become government data, subject to all terms of the MGDPA. This presents a data management problem: to what extent should a city maintain non-government data related to employees because it might become government data at some later date? Neither the MGDPA nor the commissioner's opinions provide a clear answer.

3. E-mail

E-mails present particular challenges related to use, storage, and security.

DPO 00-019.

Minn. Stat. § 13.43, subd. 2.

As the MGDPA does not specifically classify e-mails, they are presumed public, but their actual classification depends on the subject and the purpose for which they are created. For example, if an employee e-mails a supervisor about details related to charges and discipline against the employee, the e-mail is private personnel data. However, an e-mail between employees about the date of a special meeting would be public.

An e-mail may contain a combination of public, not public, and personal data. Cities should carefully consider the appropriate use of e-mail for official actions.

a. Retention

Minn. Stat. § 138.17.

DPO 00-061.

See Section IX *Records retention*.

If e-mail is used for official city business, cities will have data that must be maintained pursuant to the MGDPA and retained pursuant to the records retention schedule (the retention period is based upon its contents). A city's technology policy should also include guidelines for retention of e-mails, perhaps keeping them for a short time, such as 60 or 90 days (unless the records retention schedule provides otherwise) before destruction.

b. Security

Minn. Stat. § 13.05, subd. 5.

Cities are also required to take all necessary steps to prevent improper access or dissemination.

RELEVANT LINKS:

See LMC information memo, *Computer and Network Loss Control*.

DPO 96-042.

Minn. Stat. ch. 13D.

LMC information memo, *Meetings of City Council*.

Because e-mail is so easy and quick to use, people often overlook the potential risks, especially risks related to protecting data sent via e-mail. E-mail systems are vulnerable to "hackers."

In the words of the commissioner, e-mail is "widely known to be subject to unauthorized access," and the commissioner has warned government entities to use caution in their use of e-mail, especially when transmitting private data.

c. Open Meeting Law

In addition to the concerns that arise under the MGDPA, a responsible authority should be aware of potential issues related to the Open Meeting Law. Because of the possibility that e-mail communication might constitute a meeting under the Open Meeting Law, elected and appointed officials should not use e-mail as a means to discuss city business. This is true even for communication from, for example, one councilmember to another. E-mails tend to be easily forwarded, and it would take little effort to turn an innocent communication into a serial meeting, in violation of the law.

d. Disclaimers

As a good-faith effort to protect data transmitted by e-mail, some cities automatically attach a disclaimer to e-mail messages. These disclaimers might include language identifying the data as private or confidential, or include language such as:

- "If you are not the intended recipient of this e-mail, please delete it and notify the sender."
- "Unauthorized use of the data contained in this e-mail is prohibited."

While disclaimers show that the city is aware of its obligations, they are not a cure-all, blanket protection. In fact, disclaimers may give a sender a false sense of security. Senders might not be as careful as they should be, relying on the disclaimer to forgive any improper dissemination of not public data. Also, if the message is added automatically and in common boiler-plate language, its impact on an unintended recipient may be minimal.

S. Reference data

Many cities operate libraries and city cemeteries, and maintain volumes of information of interest to local historians as well as the general public.

RELEVANT LINKS:

1. Libraries

Minn. Stat. § 13.40, subd. 2(a).

DPO 04-016.

The following data maintained by a library is private data on individuals and may not be disclosed for purposes other than library purposes, except pursuant to a court order:

- Data that links a library patron's name with materials requested or borrowed by the patron or that links a patron's name with a specific subject about which the patron has requested information or materials.
- Data in applications for borrower cards (other than the name of the borrower).

Minn. Stat. § 13.40, subd. 2(b).

A library may release reserved materials to a family member or other person who resides with a library patron and who is picking up the material on behalf of the patron. A patron may request that reserved materials be released only to the patron.

2. Researchers

Minn. Stat. § 13.03, subd. 2(c).

The responsible authority must allow full convenience and comprehensive accessibility to researchers including historians, genealogists and other scholars to carry out extensive research, and must allow complete copying of all records containing government data, unless there is an exception in the MGDPA or other applicable law preventing access.

3. Vital records

Minn. Stat. ch. 144.

Minn. Stat. § 144.212, subd. 8.

Minn. Stat. § 144.225, subd. 1.

Although cities generally do not maintain vital records (as counties and the state do), occasionally a city might have such data in its possession. A vital record is a record or report of birth, stillbirth, death, marriage, dissolution and annulment, and related reports. The birth record is not a medical record of the mother or the child. As a general rule, data included in vital records is public data (however, certain birth records might contain confidential data).

DPO 00-039.

DPO 01-082.

The responsible authority must make sure that any vital records are maintained in such a way that access to public data is available, while maintaining confidential data separately.

T. Medical data (municipal hospitals)

Minn. Stat. § 13.384, subd. 1(b).
Lehman v. Zumbrota-Mazeppa Pub. Schs, No. A04-1226 (Minn. Ct. App. Apr. 19, 2005) (unpublished decision).

Some cities, based upon the health-related services they provide, are creating and maintaining medical data. "Medical data" is data collected because an individual was or is a patient or client at a state agency or a political subdivision's:

RELEVANT LINKS:

- Hospital.
- Nursing home.
- Medical center.
- Clinic.
- Health or nursing agency.

Minn. Stat. § 13.384, subd. 1(b).

Medical data includes business and financial records, data provided by private health care facilities, and data provided by or about relatives of the individual.

1. Classifications

Minn. Stat. § 13.384, subd. 3.
Minn. Stat. §§ 144.291-.298.

Unless the data is summary data, or a statute specifically provides a different classification, medical data is private and available only to the subject of the data as provided by the law governing general access to medical records.

Medical data may not be released except:

Minn. Stat. § 13.05.
Minn. Stat. § 253B.0921.

- Pursuant to the MGDPA.
- Pursuant to the law governing civil commitments.
- Pursuant to a valid court order.
- To administer federal funds or programs.
- To the surviving spouse, parents, children, and/or siblings of a deceased patient or client, or—if there are no surviving spouse, parents, children or siblings—to the surviving heirs of the nearest degree of kindred.
- To communicate a patient's or client's condition to a family member or other appropriate person in accordance with acceptable medical practice, unless the patient or client directs otherwise.
- As otherwise required by law.

2. Directory information

Minn. Stat. § 13.384, subd. 1(a).

"Directory information" in this context means the name of the patient, date admitted, and general condition.

a. Legal commitments

Minn. Stat. § 13.384, subd. 2(a).
K. E. N. v. Department of Admin., No. C1-94-2513 (Minn. Ct. App. Sept. 5, 1995) (unpublished decision).

For cities that own municipal hospitals, during the time that a person is a patient in that hospital under legal commitment, directory information is public data. After the person is released by termination of the person's legal commitment, the directory information is private data on individuals.

RELEVANT LINKS:

b. Patients

Minn. Stat. § 13.384, subd. 2(b).

DPO 96-018.

If a person is a patient (other than pursuant to commitment) in a hospital controlled by a government entity, directory information is public unless the patient requests otherwise, in which case it is private data on individuals.

c. Emergency patients—notification

Minn. Stat. § 13.384, subd. 2(c).

Directory information about an emergency patient who is unable to communicate, which is public under this subdivision, shall not be released until a reasonable effort is made to notify the next of kin or health care agent. Although an individual has requested that directory information be private, the hospital may release directory information to a law enforcement agency pursuant to a lawful investigation pertaining to that individual.

IX. Records retention

Minn. Stat. § 15.17.
DPO 08-026.

Handbook, *Records Management*.

Cities are required to make records "necessary for a full and accurate knowledge of their official activities." City records perform crucial functions; they:

- Record what has occurred.
- Inform officials how the city did things previously.
- Act as a check on the honesty, integrity, and completeness of official actions.
- Serve as the basis for public reports.
- Help develop a crucial link in the communication chain between city officials and their constituents.

Minn. Stat. § 15.17, subd. 3.

City officials must carefully protect and preserve all records from deterioration, mutilation, loss, or destruction and deliver them to their successors in office.

DPO 05-039.

Minn. Stat. § 138.17.

Although clearly interrelated (particularly in regard to accessibility), the terms "government records" and "government data" are not synonymous. A record is broadly defined as all cards, correspondences, discs, maps, memoranda, microfilms, papers, photographs, recordings, reports, tapes, writings, optical disks, or other data (regardless of physical form) made or received pursuant to state law or in connection with the transaction of public business.

DPO 00-042.

However, not all city data has to be considered city records. Specifically, city records do not include:

- Data that does not become part of the official transaction.

RELEVANT LINKS:

- Library and museum material made or acquired and kept solely for reference or exhibit.
- Extra copies of documents kept only for convenience of reference.
- Bonds, coupons, or other obligations of indebtedness, where the destruction or disposition is governed by other laws.

DPO 96-048.
"Preserving and Disposing of Government Records" Minnesota Historical Society, May 2008.
General Records Retention Schedule for Minnesota Cities.

Cities must preserve records based upon their administrative, legal, fiscal, and historical value. The specific length of time any record must be maintained depends on the information contained and the records retention schedule adopted (many cities have adopted the "General Records Retention Schedule for Minnesota Cities").

X. Accessibility—disabilities

The 2010 Legislature reinforced government's responsibility to provide access to persons with disabilities.

A. Public records

Minn. Stat. § 363A.42, subd. 1.

Upon request, records must be made available (within a reasonable time) to persons with disabilities in a manner consistent with state and federal laws Prohibiting discrimination against persons with disabilities. A "record" is any publicly available recorded information collected, created, received, maintained, or disseminated by the city, regardless of physical form or method of storage.

Minn. Stat. § 363A.42, subd. 2a.

Notwithstanding any law to the contrary, the requirements do not apply to:

- Technology procured or developed prior to Jan. 1, 2013 (unless substantially modified or substantially enhanced after Jan. 1, 2013).
- Records that cannot be reasonably modified to be accessible without an "undue burden" to the public entity.

Minn. Stat. § 16E.015, subd. 4.

B. Continuing education

Minn. Stat. § 363A.43.

Upon request, any continuing education or professional development course, offering, material, or activity approved or administered by the state or a political subdivision of the state must be made available within a reasonable time period to persons with disabilities in a manner consistent with state and federal laws prohibiting discrimination against persons with disabilities.

C. Reasonable modifications

Minn. Stat. § 363A.42, subd. 1.
Minn. Stat. § 363A.43, subd. 2.

Reasonable modifications must be made in any policies, practices, and procedures that might otherwise deny equal access to records, continuing education, or professional development to individuals with disabilities.

RELEVANT LINKS:

Minn. Stat. § 363A.42, subd. 3.
Minn. Stat. § 363A.43, subd. 2.

Minn. Stat. § 363A.03, subd. 36.

D. Penalties

Violations will be subject to a penalty of $500 per violation, plus reasonable attorney fees, costs and disbursements, payable to a "qualified disabled person" who sought the access. The total amount of penalties payable to any individual or class (regardless of the number of violations) is $15,000. In any class action (or series of actions) which arise from a violation, the amount of attorney fees awarded may not exceed $15,000. Actions must be commenced within one year of the occurrence of the alleged violation.

XI. Conclusion

Cities have significant responsibilities in regard to the data they collect, create, receive, maintain, or disseminate. While this memo provides a general overview of the Data Practices Act, city officials cannot blindly rely on the generalities provided, but must apply the law to the specific requests they receive and the data they actually have. The Data Practices Act is difficult to master, but a necessary component within all city operations.