Agenda

City of Minnetonka

Study Session

Monday, Jan. 14, 2019

6:30 p.m.

Council Chambers

1. Boards and Commissions Interviews
2. Council Training
   A. An overview of the Data Practices Act, Minnesota Open Meeting Law and Minnesota Gift Law for City Council Members
3. Closed session - City Manager’s Performance Review
4. Adjournment

The purpose of a study session is to allow the city council to discuss matters informally and in greater detail than permitted at formal council meetings. While all meetings of the council are open to the public, study session discussions are generally limited to the council, staff and consultants.
City Council Study Session Item #1  
Meeting of Jan. 14, 2019

**Brief Description:** Boards and Commissions Interviews

**Background**

The following openings exist on city boards and commissions:

- EDAC – 1 position
- Park Board – 2 positions
- Park Board Student Representative – 1 position

The openings were advertised on the city’s website, newsletter and local newspapers. The list of the candidates to be interviewed at this meeting is shown below. They will last approximately five to eight minutes each. Each applicant will be asked to give a brief (about three minutes) presentation of his/her background. Then the applicant will be asked to respond to questions from the council. The applicants may also ask the council any questions they may have at that time.

<table>
<thead>
<tr>
<th>First Name</th>
<th>Last Name</th>
<th>Ward</th>
<th>Choices indicated (in order)</th>
</tr>
</thead>
<tbody>
<tr>
<td>*Ann Elizabeth</td>
<td>Duginske Cibulka</td>
<td>1</td>
<td>EDAC</td>
</tr>
<tr>
<td>*Mark</td>
<td>Bartholomay</td>
<td>1</td>
<td>Planning, EDAC, Park, Sr. Advisory</td>
</tr>
<tr>
<td>*Tracy</td>
<td>Ingham</td>
<td>3</td>
<td>Planning, EDAC, Park, Sr. Advisory, LMCD, Charter</td>
</tr>
<tr>
<td>*Kristen</td>
<td>Heimerl</td>
<td>2</td>
<td>Park</td>
</tr>
<tr>
<td>Benjamin</td>
<td>Jacobs</td>
<td>1</td>
<td>Park</td>
</tr>
<tr>
<td>*Elena</td>
<td>Imaretska</td>
<td>3</td>
<td>EDAC, Park, LMCD</td>
</tr>
<tr>
<td>Kris</td>
<td>Kniefel</td>
<td>3</td>
<td>Park</td>
</tr>
<tr>
<td>*David</td>
<td>Haeg</td>
<td>3</td>
<td>Park, EDAC</td>
</tr>
</tbody>
</table>

* = confirmed interview attendance at the time packet was distributed

Submitted through:
Brad Wiersum, Mayor  
Geralyn Barone, City Manager

Originated by:
Perry Vetter, Assistant City Manager
City Council Study Session Item #2A
Meeting of Jan. 14, 2019

Brief Description: Council member training

Summary

Historically, the city has placed a high value on providing training opportunities for elected and non-elected officials, as well as city staff. The council is currently comprised of three members with less than two years of council member experience and three members who have served on the council for many years (but may not have received training updates recently).

City staff will provide training on the following subjects at the study session: the Minnesota Open Meeting Law, the Minnesota Government Data Practices Act, Minnesota’s “Gift Law,” and issues related to council communications (use of social media and communications with residents and others outside of council meetings). The training will be focused on what council members need to know, rather than comprehensive coverage of each subject area. Council members may obtain more in-depth coverage of these subjects by attending one of the training opportunities provided by the League of Minnesota Cities: the “Newly Elected Officials: 2019 Leadership Conference” or the “Experienced Officials: 2019 Leadership Conference” (both scheduled for Feb. 1-2 in Plymouth, Minnesota).

The materials included with the staff report were either prepared by the city attorney or by the League of Minnesota Cities (although some League materials have been excerpted). Council members are also reminded that the League of Minnesota Cities has numerous reference materials available through its website on a wide variety of topics, which council members may use whenever looking for general information. Questions on specific legal issues should be directed to the city attorney, but the League materials can be useful to obtain an overview of a subject and frame issues.

The training will include use of an online quiz through www.menti.com for the council, staff and members of the public in attendance. A mobile device, such as an iPad or mobile phone, is required to participate in the quiz.

Submitted through:
Geralyn Barone, City Manager

Originated by:
Corrine Heine, City Attorney
AN OVERVIEW OF THE DATA PRACTICES ACT, MINNESOTA OPEN MEETING LAW AND MINNESOTA GIFT LAW FOR CITY COUNCIL MEMBERS

Prepared by
Corrine A. Heine
Minnetonka City Attorney
January 2019
I. SUNSHINE LAWS

The Minnesota Open Meeting Law (“OML”) and Minnesota Government Data Practices Act (“MGDPA”) are both types of “sunshine laws” – laws enacted to ensure public access to information about what its government is doing.

II. MINNESOTA OPEN MEETING LAW

A. What all council members need to know about the OML:

1. Unless there is an exception provided by statute, all meetings of the city council or of any of its boards, commissions, or committees (“public body”), must be open to the public.

2. A “meeting” is any gathering of a quorum or more of the public body where the body receives or discusses information as a group concerning the business of the public body, even if no decision is made. Social and chance gatherings are not included – provided that no business of the body is discussed.

3. In order to be “open to the public,” a meeting must:
   a. Be held within the city boundaries, except in extraordinary circumstances
   b. Be in a location that is physically accessible by the public (not behind any locked doors or in an area of the building where the meeting location cannot be readily determined)
   c. Be properly noticed as required by the OML. City staff must be informed when meetings will occur so that notices can be given.
   d. At least one copy of all printed materials should be available in the meeting room for public inspection (but materials classified as not public are not required to be made available).

4. Council members need to be careful about email and social media:
   a. Discussions by email may violate the OML if a quorum of the public body’s members participate in the email exchanges.
   b. The law now allows public officials to post to social media sites without violating the OML, but only social media sites that are open to all members of the general public.

5. Meetings must be closed if required by statute and may be closed when allowed by statute. The council must strictly comply with the procedures and stated reasons for closing a meeting.

6. The council may discuss data that is classified as not public during an open meeting without liability if: (1) the meeting was not required by law to be closed; and (2) if the information relates to a matter with the council’s authority; and (3) if disclosure of the information was reasonably necessary to conduct the council’s business. The immunity applies only to the discussion during the meeting and would not apply to any further release of the data. A disclosure that does not meet all three requirements could result in penalties under both the OML and the MGDPA.
7. **Social media.** Since 2014, the OML has provided that use of social media by a member of a public body does not violate the OML “so long as the social media use is limited to exchanges with all members of the general public.” This means that any social media account (Facebook, Twitter, etc.) that a council member uses to communicate with other council members about city business must be a public page. E-mail is not considered use of social media under the statute.

8. The penalties for violation of the OML are significant:

   a. Criminal prosecution is possible for an intentional violation.
   b. Repeated intentional violations can result in forfeiture of office.
   c. A civil penalty of $300 can be imposed for an intentional violation, which the violator must pay, not the public body.
   d. The city may be required to pay the suing party’s costs and attorney fees.
   e. The city may, but is not required to, pay its members’ costs and attorney fees.
   f. However, OML violations do not automatically invalidate decisions made during the meeting.

**B. To learn more:**

For further information on the detailed requirements of the OML, see the League of Minnesota Cities’ Information Memo entitled “Meetings of City Councils,” specifically Section II of that memo.

III. MINNESOTA GOVERNMENT DATA PRACTICES ACT.

A. Management of public records.

The Minnesota Government Data Practices Act (“MGDPA”) is one of three statutes that govern public records. Together, the three statutes govern the entire life cycle for government information.

1. **Official Records Act (Minn. Stat. § 15.17).** The Official Records Act requires that public officials “make and preserve all records necessary to a full and accurate knowledge of their official activities.” The statute addresses various preservation methods that may be used, including microfilm, microfiche, optical images, and other means of reproduction. Public agencies are obligated to carefully protect government records from deterioration, mutilation, loss or destruction, and public officials are required to deliver government records to their successors in office. Because it establishes when records must be created, it governs the beginning of the life cycle.

2. **Minnesota Government Data Practices Act (Minn. Stat. Ch. 13)** The MGDPA primarily deals with public access to government records while the records exist. It governs the middle of the life cycle for government information.

3. **Records Management Statute (Minn. Stat. § 138.17).** The Records Management Statute prohibits public officials from destroying government records, except as approved by a three-member state panel or according to a record destruction
schedule that has been approved by the state panel and adopted by the local government entity. The prohibition only applies to “official records,” which is not defined by the law. In general, official records are permanent records of official actions – all of which are preserved by city staff. Council members may destroy duplicates of official records (like copies of agenda packets), transitory records (like emails) and unofficial records like personal notes, at any time – unless the city attorney has provided other direction pursuant to a litigation hold.

**B. What all council members need to know about the MGDPA:**

1. **The MGDPA is broad in scope.** It applies to “all government data” – meaning, all data that is collected, created, received or maintained by any government official or employee in the course of performing that official’s or employee’s duties. For example, it applies not only to the records that the city staff create but it also applies to records that council members create or receive – e.g., emails from constituents about a proposed development.

2. **Location doesn’t matter.** “Government data” is governed by the MGDPA, regardless of where it is located. It can be located in city file drawers, city computers, or on a home computer or personal phone. No matter where government data is located, the city and its public officials are responsible for providing access as required by law.

3. **Conflicting values.** The MGDPA tries to achieve a balance between conflicting values: public access and individual privacy. One of the principal purposes of the MGDPA is to provide public access to government records, to secure the public’s right to be informed and aware of what its government is doing. Another purpose of the MGDPA is to protect individual rights to privacy.

4. **Presumption of Access.** The MGDPA attempts to achieve its balance of public access and privacy through a classification scheme. The MGDPA establishes a general presumption that all data is public, unless the data is classified by a state statute or federal law as not being public. The classification assigned to the data determines who may have access to the data. Understanding the classification scheme is central to an understanding of the MGDPA.

5. **Classification Defines Access.** The MGDPA uses classification labels to determine who gets to access data. In general, there are three different levels of access:

   a. **Public data (on individuals or not on individuals).** Public data is accessible to anyone, for any reason. In general, a city cannot require an individual to identify themselves or to state the reason they want the data, if the data is public. An example would be council meeting minutes.

   b. **Private data on individuals or nonpublic data not on individuals.** Data with a private or nonpublic classification is accessible to the subject of the data but not the public generally. It is also available only to those government officials and employees whose jobs require them to have access. An example would be personnel records: although some information is public by law, most personnel data is private.
c. Confidential data on individuals or protected nonpublic data not on individuals. Data with a confidential or protected nonpublic classification can be accessed only by government officials and employees whose jobs require them to have access. An example would be records in an active criminal investigation.

6. Responsible Authority. A city council is required to appoint a responsible authority and, if it fails to do so, the city clerk is the responsible authority (the “RA”). The RA is the official charged by law with responsibility of ensuring the city’s compliance with the MGDPA. Minnetonka’s RA is the city clerk.

7. Internal Security. Cities are required to maintain the security of data that is classified as not public—not only to prevent release to the public, but also to prevent release to city officials and employees whose jobs do not require access. For example, in a city manager form of government, where the manager hires and fires employees, the RA would be legally required to refuse a council member’s request to access an employee’s personnel file.

8. Classifications change. The MGDPA is exceedingly complex. Classifications of data can change depending upon various events occurring. The MGDPA is not the only statute that classifies data, and compliance requires knowledge of other state statutes, federal laws, and federal regulations.

9. Inspection is always free. If a person asks to inspect public data, the city can’t charge, no matter how much staff time is consumed by collecting the data. The city can only charge if copies are requested, and the statutes regulate what can be charged—a flat rate per page in some circumstances, actual cost of making the copy in some circumstances, and, sometimes, the cost of staff time to make and certify copies.

10. Penalties for violation. The penalties for violating the MGDPA include:

   a. Action for damages. Any person who suffers damage as the result of a violation of the MGDPA may sue for damages, plus costs and attorney fees. If the violation was willful, the person may be entitled to punitive damages of not less than $1,000 nor more than $15,000 per violation.

   b. Injunctive action. A person can bring an action to prevent a government entity from violating the MGDPA.

   c. Action to compel compliance. An aggrieved person can bring an action to compel a government entity to comply with the MGDPA. If successful, the person may recover costs and attorney fees. If the action was frivolous, the court can award costs and attorney fees to the responsible authority. The court can issue a civil penalty of up to $1,000 against the government entity for noncompliance, but must assess a series of factors before it may impose the penalty.

   d. Criminal prosecution. Any person who willfully violates the MGDPA or rules adopted under the MGDPA is guilty of a misdemeanor.
e. Willful violation of the MGDPA is grounds for discipline of a public employee, including suspension or discharge.

C. To learn more:

For further information on the detailed requirements of the MGDPA, see the League of Minnesota Cities’ Information Memo entitled “Data Practices: Analyze, Classify, Respond.”

IV MINNESOTA GIFT LAW.

A. Prohibition on gifts.

The Minnesota legislature enacted gift law provisions in 1994. There are two statutes that are generally the same. One applies to state public officials, legislative employees, and local officials of metropolitan governmental units (which includes cities over 50,000 population in the metropolitan area). The other statute applies to elected and appointed officials of counties, cities and school boards that are not covered by the first statute.

B. General rule.

There are three basic elements to a gift law violation:

1. a "local official" (which includes city council members)
2. who accepts a "gift" (anything that has value greater than what the local official paid for it) from
3. an "interested person" (a person or association that has a direct financial interest in a decision that the local official is authorized to make; also, a representative of the person or association that has the financial interest).

C. Exceptions:

1. Exceptions based on the type of "gift":
   a. a political campaign contribution, as defined by election law;
   b. services to assist the official in performing official duties, including but not limited to providing advice, consultation, information and communication in connection with legislation, and services to constituents;
   c. services of "insignificant monetary value" (generally, less than $5);
   d. a plaque or memento recognizing individual services in a field of specialty or to a charitable cause;
   e. a trinket or memento costing $5 or less;
   f. informational material of unexceptional value;
   g. food or beverage given at a reception, meal or meeting away from the recipient’s place of work by an organization before whom the recipient makes a speech or answers questions as part of a program (needs to be a formal speech, not just an introduction at the meeting).

2. Exceptions based on who is giving the gift or why it is given:
a. Gift is given because of membership in a group, a majority of whose members are not local officials, and an equivalent gift is given or offered to the other members of the group; (think: membership in professional association related to other employment, or similar);

b. Gift is given by an interested person who is a member of the family of the recipient, unless the family member gives the gift on behalf of someone who is not a family member (only family members matter, not long-time friends, if they are “interested persons”);

c. Gift is given by a national or multistate organization of governmental organizations or public officials (think National League of Cities or similar), if a majority of the dues to the organization are paid from public funds, to attendees at a conference sponsored by that organization, if the gift is food or a beverage given at a reception or meal and an equivalent gift is given or offered to all other attendees.

D. Related ordinances and laws

This paper only addresses the law we call “the Gift Law.” Remember that other rules and requirements may apply as well. For example:

1. Minnetonka has a code of ethics ordinance, City Code § 115 which addresses a number of topics, including: conflicts of interest; acting as an agent or attorney for someone before the city; compliance with state laws regarding gifts, loans and contracting; accepting compensation or expense reimbursement for performing public duties; use of public money or other resources; disclosure of information gained through public office; intentional violation of the city charter or city ordinances.

2. State laws related to official interest in contracts and conflicts of interest, Minn. Stat. §§ 471.87, 471.88 and 471.89.

The major areas of council authority and responsibility include:

- Judging the qualifications and election of its own members.
- Setting and interpreting rules of procedure.
- Legislating for the city.
- Enforcing city ordinances.
- Appointing and dismissing administrative personnel.
- Transacting city business.
- Managing city finances.
- Making appointments to boards, commissions, and committees.
- Protecting the welfare of the city and its inhabitants.
- Providing community leadership.

The city council is a continuing body. New members have no effect on the body except to change its membership. This means that all ordinances and resolutions remain in effect until the council alters or rescinds them, or until they expire through their own terms. At any time, the council can change any resolution, ordinance, or administrative order, whether or not the individuals presently on the council are the same members as when the council originally took action.

Councilmembers fulfill their statutory duties, almost without exception, by acting as a council as a whole. For example, the council, not individual councilmembers, supervise administrative officers, formulate policies, and exercise city powers.

### III. Gifts

State law defines a “gift” as money, property (real or personal), a service, a loan, the forbearance or forgiveness of debt, or a promise of future employment, given and received without the giver receiving something of equal or greater value in return.

#### A. General prohibition

Elected and appointed “local officials” generally may not receive a gift from any “interested persons.”

#### 1. Local officials

A “local official” represents any elected or appointed official of a city, or of an agency, authority, or instrumentality of a city. The gift prohibition clearly applies to the members of the city council. However, the law does not further define the term “local official”, making it unclear if the law intends to cover all city employees, or just certain high-level employees (such as city managers or administrators) and other appointed officials.
Since so many individuals can get involved in the decision-making process, trying to distinguish between city “employees” and “officials” becomes quite difficult. As a result, the safest course of action is to assume the law applies to all employees, regardless of their title or job responsibilities.

2. Interested persons

State law defines an “interested person” as a person or representative of a person or association that has a direct financial interest in a decision that a local official is authorized to make.

An interested person likely includes anyone who may provide goods or services to a city such as engineers, attorneys, financial advisers, contractors, and salespersons. However, virtually every resident or person doing business in the city could have a direct financial interest in a decision that an official is authorized to make. These may include:

- Property tax levies.
- Special assessments.
- Licenses and permits.
- Land use decisions.

If an individual could benefit financially from a decision or recommendation that a city official would be authorized to make, he or she might qualify as an interested person for purposes of the gift law.

B. Exceptions

The gift law allows the following types of gifts:

- Lawful campaign contributions.
- Services to assist an official in the performance of official duties. Such services can include (but are not limited to) providing advice, consultation, information, and communication in connection with legislation and services to constituents.
- Services of insignificant monetary value.
- A plaque or similar memento. Such items are permitted when given in recognition of individual services in a field of specialty or to a charitable cause.
- A trinket or memento costing $5 or less.
- Informational material of unexceptional value.
- Food or beverage given at a reception, meal, or meeting. This exception only applies if the recipient is making a speech or answering questions as part of a program located away from the recipient’s place of work.
Gifts between family members. However, the gift may not be given on behalf of someone who is not a member of the family.

- Gift because of the recipient’s membership in a group. The majority of this group’s members must not be local officials and an equivalent gift must be given or offered to the other group members.

- Food or beverages given to national or multi-state conference attendees. The majority of dues paid to the organization must be paid from public funds and an equivalent gift must be given or offered to all other attendees.

C. Gifts to cities

The law prohibits gifts to city officials, not to cities themselves. Cities may accept gifts of real or personal property and use them in accordance with the terms prescribed by the donor. A resolution accepting the gift and the donor’s terms must receive an affirmative vote of two-thirds of the members of the council. A city may not, however, accept gifts for religious or sectarian purposes.

D. Metro area cities over 50,000

Metropolitan cities with a population over 50,000 must comply with additional regulations. Under the Ethics in Government Act, local officials in these cities also may not receive gifts from “lobbyists,” though similar exceptions may apply.

The Minnesota Campaign Finance and Public Disclosure Board issues advisory opinions regarding the lobbyist gift ban. These opinions may be relevant to any Minnesota city struggling with the application or implication of a gift ban to a particular situation.

E. Municipal liquor stores

Municipal liquor store employees may not suggest, request, demand, or accept any gratuity, reward, or promise thereof from any representative of a manufacturer or wholesaler of alcoholic beverages. Any manager or employee who violates this provision is guilty of a gross misdemeanor.

IV. Conflicts of interest

Two broad types of conflicts of interest exist that city officials and municipal bodies may encounter: those involving contractual decisions, and those involving non-contractual decisions.
INFORMATION MEMO

Meetings of City Councils

Learn about the open meeting law, taking meeting minutes, scheduling and conducting meetings, including use of parliamentary procedure, audience participation, and regulating attendance of councilmembers. Most principles apply also to city boards, commissions, and other public bodies. Includes table of privileged, subsidiary, and main motions, and links to sample council bylaws.

RELEVANT LINKS:


Minn. Stat. § 412.191, subd. 1. Minn. Stat. § 645.08 (5).

Minn. Stat. § 13D.04, subd. 1.

Minn. Stat. § 13D.04, subd. 2. Minn. Stat. § 645.44, subd. 5.

I. Types of meetings and notice requirements

A meeting is a gathering of a quorum of public officials to discuss, decide, or receive information on official matters over which they have authority. The city council exercises its authority when it meets as a group. There are certain requirements for council meetings under state law.

A quorum of a public body is the number of people that must be present before a public body can conduct business. A majority of the members of a statutory city council constitutes a quorum. A majority of the qualified members of any board or commission also constitutes a quorum. Home rule charter cities may have different quorum requirements.

A public body that is subject to the open meeting law must generally provide advance public notice of its meetings and hold them open to the public. The notice requirements depend on the type of meeting. However, if a person receives actual notice of a meeting at least 24 hours before it takes place, all notice requirements under the open meeting law are satisfied, regardless of the method of receipt of notice.

A. Regular meetings

Regular meetings of a statutory city council are held at times established by the council. A council will typically meet once a month on a particular day, although some councils may have regular meetings scheduled more frequently. Home rule charter cities should consult their charters and any council rules concerning the scheduling of regular meetings.

The council must keep a schedule of its regular meetings on file at its primary office. The council should also set an alternate meeting day for any regular meeting day that falls on a legal holiday. If the council decides to hold a meeting at a different time or place from that stated in its schedule of regular meetings, it must generally give the notice required for a special meeting.
Special meetings are meetings held at a time or place that is different from the regularly scheduled meetings. These are often scheduled to deal with specific items that need to be addressed before the next regular meeting. Generally, any matter that can be addressed at a regular meeting can also be addressed at a special meeting if it has been properly noticed. The commissioner of the Minnesota Department of Administration has advised that a city council should not discuss or decide topics that have not been included as the stated purpose of a special meeting in the notice provided to the public. All state laws governing regular meetings, including the open meeting law, apply to special meetings.

In statutory cities, special meetings may be called by the mayor or by any two members of a five-member council or three members of a seven-member council. Special meetings are called by filing a written statement with the city clerk. Home rule charter cities may have different requirements for special meetings.

Unless otherwise expressly established by statute, the following notice requirements apply to special meetings.

1. **Notice to council**

When a special meeting has been called, the clerk must mail, at least one day before the meeting, a notice to all councilmembers stating the time and place of the meeting. If all councilmembers attend and participate in the meeting, the notice requirements will be considered to have been satisfied.

2. **Notice to public**

The clerk also must post written notice of the date, time, place, and purpose of the special meeting on the city’s principal bulletin board at least three days before the meeting. A principal bulletin board must be located in a place reasonably accessible to the public. If the city does not have a principal bulletin board, the notice must be posted on the door of its usual meeting room.

In addition to posting notice, the city must also mail or deliver notice to each person who has filed a written request for notice of special meetings with the city. Notice to these individuals must be mailed or delivered at least three days before the meeting. As an alternative to mailing or delivering the notice, the city may publish the notice once in its official newspaper at least three days before the meeting.
If there is no official newspaper, notice may be published in a qualified newspaper of general circulation that covers the city.

If, through no fault of the city, an error occurs in the publication of a notice, the error generally does not impact the validity of a public meeting.

In calculating the number of days for providing notice, the first day the notice is given should not be counted, but the last day should be. But if the last day is a Saturday, Sunday, or a legal holiday, that day is omitted from the calculation and the following day is considered the last day. For example, if a special meeting is scheduled for a Thursday, notice has to be given by Monday at the latest to meet the three-day notice provision. In this example, Tuesday is day one, Wednesday is day two, and Thursday is day three. Monday is not included in the time computation. Similarly, if a special meeting is planned for Monday, notice must be given by Friday at the latest; Saturday is day one, Sunday is day two, and Monday is day three. Saturday and Sunday are included in the time computation since they are not the last day of the time period.

A person filing a written request for notice of special meetings may limit the request to notification of special meetings that cover a particular subject. In this case, the city only needs to send notice of special meetings addressing those subjects.

Cities may set an expiration date for requests for notice of special meetings and require each request to be re-filed once each year. The city must provide each person, who has filed such a request, notice of the requirement to re-file the request not more than 60 days before re-filing is due.

If a council committee or other public body meets and a quorum of city councilmembers attend the meeting, the city most likely does not need to give additional notice of a special city council meeting as long as proper notice of the committee or other public meeting has been given. If council members participate in the discussions or deliberations, however, an additional separate notice of a special meeting of the city council may be required.

The commissioner of the Minnesota Department of Administration has advised that when a town board changed the time and location of a meeting on the same day it was scheduled to occur, the town board violated the open meeting law by failing to provide the required three-day notice for a special meeting. The town board had changed the time and place of the meeting due to the weather and lack of air conditioning in the regular meeting room.

C. Emergency meetings

An emergency meeting is a special meeting called by the council due to circumstances that, in its judgment, require immediate council consideration.
The procedure for notifying councilmembers of an emergency meeting is the same as that for a special meeting. The public-notice requirements, however, are different.

The council must make a good faith effort to provide notice of the emergency meeting to all media that have filed a written request for notice. Notice must be by telephone or by any other method used to notify councilmembers. The notice must include the subject of the meeting. A published or posted notice is not necessary.

If matters not directly related to the emergency are discussed or acted upon at an emergency meeting, the meeting minutes must include a specific description of them.

### D. Closed meetings

A closed meeting is a meeting of a public body that the public is not allowed to attend.

A meeting of a public body only may be closed to the public if it meets the requirements of one of the specific exceptions listed in the open meeting law that authorize such closure. The same notice requirements that apply to open meetings also apply to closed meetings. For example, if a closed meeting takes place at a regular meeting, the notice requirements for a regular meeting apply. Likewise, if a closed meeting takes place at a special meeting, the notice requirements for a special meeting apply.

### E. Annual meeting (first meeting of the year)

There is no date set by statute for the first meeting of the year. In most statutory cities, the date is set by council bylaws establishing rules of procedure for the council. A home rule charter city should consult both its charter and any procedural rules the council has adopted for any requirements regarding the first meeting of the year.

The annual meeting is usually held on or shortly after the first Monday in January, which is when the terms of new councilmembers begin. In the meantime, all previously chosen and qualified councilmembers shall serve until their successors qualify.

The notice required for the annual meeting will depend on whether it occurs at a regularly scheduled meeting or at a special meeting that occurs at a different time and place from the regular meetings.

In statutory cities, the council must do the following at the first meeting of the year:
• Designate an official newspaper.
• Appoint an acting mayor from among the councilmembers. The acting mayor shall perform the duties of the mayor if there is a vacancy in the mayor’s position or during the mayor’s disability or absence.
• Select an official depository for city funds. (This must be done within 30 days of the start of the city’s fiscal year).

In addition, although not required by statute, many city councils will also do the following at the first meeting of the year:
• Review different council appointments to city boards and commissions. For example, the council must appoint one elected city official and one elected or appointed city official to serve with the city’s fire chief on the board of trustees for a city fire department’s volunteer relief association.
• Review council bylaws and make any needed changes.
• Assign committee duties to members.
• Approve official bonds that have been filed with the clerk.

Home rule charter cities may have additional requirements for their first meeting of the year.

F. Adjourned meetings
Cities often use the terms: “adjourned,” “continued,” and “recessed” interchangeably when referring to meetings that are postponed to a future time for lack of a quorum, for convenience, or to complete pending business from a regular meeting.

Although a quorum (majority of councilmembers in a statutory city) is necessary in order to conduct business, less than a quorum may adjourn or postpone a meeting to a fixed, future time.

If the date, time, and place of the adjourned meeting are announced at the previous meeting and this information is recorded in the minutes, no additional public notice is necessary for the adjourned meeting. Otherwise, the notice for a special meeting is needed.

G. Meetings conducted by interactive television
A city council meeting may be conducted by interactive television if all four of the following requirements are met:
• At least one councilmember is physically present at the regular meeting location.
• All councilmembers must be able to hear and see each other and all discussion and testimony presented at any location at which at least one councilmember is present.
• All members of the public at the regular meeting location must be able to hear and see all discussion, testimony, and votes of all councilmembers.
• Each location at which a councilmember is present must be open and accessible to the public.

If possible, a member of the public should be able to monitor the meeting electronically from a remote location.

If interactive television is used to conduct a regular, special, or emergency meeting, the public body shall provide notice of the regular meeting location and notice of any site where a member of the public body will be participating by interactive television. The timing and method of providing notice will depend on whether the meeting is a regular, special, or emergency meeting.

The open meeting law does not define the term “interactive television.” Therefore, it is not clear what technology is authorized to be used under this authority. Although school boards have express authority to use “interactive technology with an audio and visual link” to conduct a meeting if all of the other requirements for interactive television are satisfied, city councils do not have similar authority.

However, the commissioner of the Minnesota Department of Administration has advised that a city council meeting where a city councilmember participated through Skype, while physically present at a remote location outside Minnesota, complied with the statutory authority for conducting meetings through interactive television. After the meeting occurred, a newspaper article suggested that the meeting violated the open meeting law because the councilmember’s remote location was not accessible to the city’s residents. The advisory opinion noted that the meeting met each of the four requirements in the statute and reasoned that the “plain language of the statute does not forbid a member of a public body from ‘attending’ a public meeting at a location ‘open and accessible to the public’ outside of the entity’s geographic area, as long as all other conditions of the section are met.”

H. Telephone or electronic meetings

Meetings may be conducted by telephone or other electronic means if the following conditions are met:

• The presiding officer, chief legal counsel, or chief administrative officer for the affected governing body determines an in-person meeting or a meeting conducted through interactive television is not practical or prudent because of a health pandemic or an emergency declared under chapter 12 of the Minnesota Statutes.
• All members of the governing body participating in the meeting can hear each other and can hear all discussion and testimony.

• Members of the public present at the regular meeting location can hear all discussion, testimony, and votes of the members of the body, unless attendance at the regular meeting location is not feasible due to the health pandemic or emergency declaration.

• At least one member of the governing body, chief legal counsel, or chief administrative officer is physically present at the regular meeting location, unless unfeasible due to the health pandemic or emergency declaration.

• All votes are conducted by roll call so that each member’s vote on each issue can be identified and recorded.

Each member of the governing body participating in a meeting by telephone or other electronic means is considered present at the meeting for purposes of determining a quorum and participating in all proceedings.

If telephone or another electronic means is used to conduct a meeting, to the extent practical, the governing body shall allow a person to monitor the meeting electronically from a remote location. The governing body may require the person making a connection to pay for the documented additional cost incurred as a result of the additional connection.

If telephone or another electronic means is used to conduct a regular, special, or emergency meeting, the public body shall provide notice of the regular meeting location, of the fact that some members may participate by telephone or other electronic means, and, if practical, of the option of connecting to the meeting remotely. The timing and method of providing notice will depend on whether the meeting is a regular, special, or emergency meeting.

I. Public Hearings

A public hearing is a meeting that is held where members of the public can express their opinions. The council is there to regulate the hearing and make sure that people who want to speak get the opportunity to do so. The council does not deliberate or discuss matters during the public-hearing portion of this type of meeting; instead, it listens to the public. Once the public-comment period is finished, the council will often wrap up the meeting.

In order to recess or continue a meeting of this sort, the council should not formally end the public-comment part of the hearing.

There are two types of public hearings, those that are discretionary and those that are required by a specific statute, ordinance, or charter provision.
1. Discretionary public hearings

Many city councils will hold public hearings even when they are not legally required to do so. Generally, hearings of this type allow the public to comment on a specific issue. Such hearings can be helpful in raising concerns about an issue that the council may not have considered.

If a discretionary public hearing takes place at a time or place that is different from a regularly scheduled meeting, notice for a special meeting must be provided.

2. Required public hearings

When a specific statute, ordinance, or charter provision requires a council to hold a public hearing, the notice requirements must be followed carefully. Often there are special notice requirements that are more substantial than the notice that must be provided for a special meeting. For example, public hearings required to amend a zoning ordinance and to adopt special assessments have special notice requirements.

Here are some actions that require public hearings:

- Street vacation.
- Annexation by ordinance.
- Local improvement projects that will be paid for with special assessments.
- When special assessments are made to property.
- Purchase and improvement of waterworks, sewers, drains, and storm sewers by storm sewer improvement districts.
- Adoption of a housing redevelopment authority (HRA) enabling resolution.
- Adoption of an economic development authority (EDA) enabling resolution.
- Sale of port authority land.
- Sale of EDA land.
- Increase of levy for an EDA.
- Continuation of a municipal liquor store after a net loss for two of three consecutive years.
- Truth-in-taxation.
- Adoption or amendment of a zoning ordinance.
- Subdivision applications.
- Granting of a conditional use permit.
- Adoption of a charter amendment by ordinance.
- Certain interim ordinances.
There are other situations that may require public hearings. Contact the League for further information if you are unsure about a particular situation.

**J. Days and times when meetings cannot be held**

State law defines a set of public holidays when no public business may be transacted except to deal with emergencies. The transaction of public business includes conducting public meetings.

The public holidays are:

- New Year’s Day (Jan. 1).
- Martin Luther King’s Birthday (the third Monday in January).
- Washington’s and Lincoln’s Birthday (the third Monday in February).
- Memorial Day (the last Monday in May).
- Independence Day (July 4).
- Labor Day (the first Monday in September).
- Christopher Columbus Day (the second Monday in October).
- Veterans Day (Nov. 11).
- Thanksgiving Day (the fourth Thursday in November).
- Christmas Day (Dec. 25).

All cities have the option, however, of deciding whether Christopher Columbus Day and the Friday after Thanksgiving shall be holidays. If these days are not designated as holidays, public business may be conducted on them.

If a holiday falls on a Saturday, the preceding Friday is considered to be a holiday. If a holiday falls on a Sunday, the next Monday is considered to be a holiday.

In addition, city council meetings may not be held during the following times:

- After 6 p.m. on the evening of a major political party precinct caucus.
- Between 6 p.m. and 8 p.m. on a day when there is an election being held within the city’s boundaries.

State law does not prohibit meetings on weekends. However, state law regulating how time is computed for the purpose of giving any required notice provides that if the last day of notice falls on either a Saturday or Sunday, that day cannot be counted.
II. The open meeting law

A. Purpose

The Minnesota open meeting law generally requires that all meetings of public bodies must be noticed and open to the public. This presumption of openness serves three vital purposes:

- It prohibits 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 detect improper influences.
- It ensures the public’s right to be informed.
- It gives the public an opportunity to present its views to the public body.

B. Public notice

Public notice generally must be provided for meetings of a public body subject to the open meeting law. The notice requirements depend on the type of meeting. However, if a person receives actual notice of a meeting at least 24 hours before it takes place, all notice requirements under the open meeting law are satisfied, regardless of the method of receipt.

C. Location

The Minnesota Supreme Court has held that, to meet the statutory requirement that meetings of public bodies shall be open to the public, “it is essential that such meetings be held in a public place located within the territorial confines of the [public body] involved.”

D. Printed Materials

At least one copy of the printed materials relating to agenda items that are provided to the council at or before a meeting must also be made available for public inspection in the meeting room while the governing body considers the subject matter.

This requirement does not apply to materials classified by law as other than public or to materials relating to the agenda items of a closed meeting.

E. Groups governed by the open meeting law

The open meeting law applies to all governing bodies of any school district, unorganized territory, county, city, town or other public body, and to any committee, sub-committee, board, department or commission of a public body.
Thus, the law applies to meetings of all city councils, planning commissions, firefighter relief associations, economic development authorities, and housing redevelopment authorities, among others.

The Minnesota Supreme Court has held, however, that the governing body of a municipal power agency, created under Minn. Stat. §§ 453.51-453.62, is not subject to the open meeting law because the Minnesota Legislature granted these agencies authority to conduct their affairs as private corporations.

**F. Gatherings governed by the open meeting law**

The open meeting law does not define the term “meeting.” The Minnesota Supreme Court, however, has ruled that meetings are gatherings of a quorum or more of the members of the governing body, or a quorum of a committee, subcommittee, board, department, or commission thereof, at which members discuss, decide, or receive information as a group on issues relating to the official business of that governing body.

A majority of the members of a statutory city council constitutes a quorum. A majority of the qualified members of any board or commission also constitutes a quorum. Home rule charter cities may have different quorum requirements.

The open meeting law does not generally apply in situations where less than a quorum of the city council is involved. However, serial meetings in groups of less than a quorum that are held in order to avoid the requirements of the open meeting law may be found to violate the law, depending on the specific facts.

**G. Open meeting law exceptions**

There are seven exceptions to the open meeting law that authorize the closure of meetings to the public. Under these exceptions, some meetings may be closed and some meetings must be closed. Before a meeting is closed under any of the exceptions, the council must state on the record the specific grounds permitting the meeting to be closed and describe the subject to be discussed.

The commissioner of the Minnesota Department of Administration has advised that a member of the public body (and not its attorney) must make the statement on the record. The open meeting law does not define the phrase “on the record,” but the commissioner has advised that the phrase should be interpreted to mean a verbal statement in open session.
The commissioner has also advised that citing the specific statutory authority that permits the closed meeting is the simplest way to satisfy the requirement for stating the specific grounds permitting the meeting to be closed.

Both the commissioner and the Minnesota Court of Appeals have concluded that something more specific than a general statement is needed to satisfy the requirement of providing a description of the subject to be discussed.

All closed meetings, except those closed as permitted by the attorney-client privilege, must be electronically recorded at the expense of the public body. Unless otherwise provided by law, the recordings must be preserved for at least three years after the date of the meeting.

The same notice requirements that apply to open meetings also apply to closed meetings. For example, if a closed meeting takes place at a regular meeting, the notice requirements for a regular meeting apply. Likewise, if a closed meeting takes place as a special meeting, the notice requirements for a special meeting apply.

1. Meetings that may be closed

The public body may choose to close certain meetings. The following types of meetings may be closed:

a. Labor negotiations under PELRA

A meeting to consider strategies for labor negotiations, including negotiation strategies or development or discussion of labor-negotiation proposals, may be closed. However, the actual negotiations must be done at an open meeting if a quorum of the council is present.

The following procedure must be used to close a meeting under this exception:

- The council must decide to close the meeting by a majority vote at a public meeting and must announce the time and place of the closed meeting.
- Before closing the meeting, the council must state on the record the specific grounds permitting the meeting to be closed and describe the subject to be discussed.
- A written record of all people present at the closed meeting must be available to the public after the closed meeting.
• The meeting must be tape-recorded.
• The recording must be kept for two years after the contract is signed.
• The recording becomes public after all labor agreements are signed by the city council for the current budget period.

If an action claiming that other public business was transacted at the closed meeting is brought during the time the tape is not public, the court will review the recording privately. If the court finds no violation of the open meeting law, the action will be dismissed and the recording will be preserved in court records until it becomes available to the public. If the court determines there may have been a violation, the entire recording may be introduced at the trial. However, the court may issue appropriate protective orders requested by either party.

b. Performance evaluations

A public body may close a meeting to evaluate the performance of an individual who is subject to its authority.

The following procedure must be used to close a meeting under this exception:

• The public body must identify the individual to be evaluated prior to closing the meeting.
• The meeting must be open at the request of the individual who is the subject of the meeting; so some advance notice to the individual is needed to allow the individual to make a decision.
• Before closing the meeting, the council must state on the record the specific grounds permitting the meeting to be closed and describe the subject to be discussed.
• The meeting must be electronically recorded, and the recording must be preserved for at least three years after the meeting.
• At the next open meeting, the public body must summarize its conclusions regarding the evaluation. The council should be careful not to release private or confidential data in its summary.

c. Attorney-client privilege

Meetings between the governing body and its attorney to discuss active, threatened, or pending litigation may be closed when the balancing of the purposes served by the attorney-client privilege against those served by the open meeting law dictates the need for absolute confidentiality. The need for absolute confidentiality should relate to litigation strategy, and will usually arise only after a substantive decision on the underlying matter has been made.
This privilege may not be abused to suppress public observations of the decision-making process, and does not include situations where the council will be receiving general legal opinions and advice on the strengths and weaknesses of a proposed action that may give rise to future litigation.

The following procedure must be used to close a meeting under this exception:

- Before closing the meeting, the council must state on the record the specific grounds permitting the meeting to be closed and describe the subject to be discussed.
- The council should also describe how a balancing of the purposes of the attorney-client privilege against the purposes of the open meeting law demonstrates the need for absolute confidentiality.
- The council must actually communicate with its attorney at the meeting.

**d. Purchase or sale of property**

A public body may close a meeting to:

- Determine the asking price for real or personal property to be sold by the public body.
- Review confidential or nonpublic appraisal data.
- Develop or consider offers or counteroffers for the purchase or sale of real or personal property.

The following procedure must be used to close a meeting under this exception:

- Before closing the meeting, the council must state on the record the specific grounds for closing the meeting, describe the subject to be discussed, and identify the particular property that is the subject of the meeting.
- The meeting must be tape-recorded and the property must be identified on the tape. The recording must be preserved for eight years, and must be made available to the public after all property discussed at the meeting has been purchased or sold or after the public body has abandoned the purchase or sale.
- A list of councilmembers and all other persons present at the closed meeting must be made available to the public after the closed meeting.
- The actual purchase or sale of the property must be approved at an open meeting, and the purchase or sale price is public data.
e. Security reports

A meeting may be closed to receive security briefings and reports, to discuss issues related to security systems, to discuss emergency-response procedures and to discuss security deficiencies in or recommendations regarding public services, infrastructure, and facilities—if disclosure of the information would pose a danger to public safety or compromise security procedures or responses. Financial issues related to security matters must be discussed, and all related financial decisions must be made at an open meeting.

The following procedure must be used to close a meeting under this exception:

- Before closing the meeting, the council must state on the record the specific grounds for closing the meeting and describe the subject to be discussed.
- When describing the subject to be discussed, the council must refer to the facilities, systems, procedures, services or infrastructure to be considered during the closed meeting.
- The closed meeting must be tape-recorded, and the recording must be preserved for at least four years.

2. Meetings that must be closed

There are some meetings that the open meeting law requires to be closed. The following meetings must be closed:

a. Misconduct allegations

A public body must close a meeting for preliminary consideration of allegations or charges against an individual subject to the public body’s authority.

The commissioner of the Minnesota Department of Administration has advised that a city could not close a meeting under this exception to consider allegations of misconduct against a job applicant who had been extended a conditional offer of employment. (The job applicant was not a city employee). The commissioner reasoned that the city council had no authority to discipline the job applicant or to direct his actions in any way; therefore, he was not “an individual subject to its authority.”

The commissioner has also advised that a tape recording of a closed meeting for preliminary consideration of misconduct allegations is private personnel data under Minn. Stat. § 13.43, subd. 4, and is accessible to the subject of the data but not to the public. The commissioner noted that at some point in time, some or all of the data on the tape may become public under Minn. Stat. § 13.43, subd. 2.
For example, if the employee is disciplined and there is a final disposition, certain personnel data becomes public.

**The following procedure must be used to close a meeting under this exception:**

- Before closing the meeting, the council must state on the record the specific grounds for closing the meeting and describe the subject to be discussed.
- The meeting must be open at the request of the individual who is the subject of the meeting. Thus, the individual should be given advance notice of the existence and nature of the charges against him or her, so that the individual can make a decision.
- The meeting must be electronically recorded, and the recording must be preserved for at least three years after the meeting.
- If the public body decides that discipline of any nature may be warranted regarding the specific charges, further meetings must be open.

**b. Certain not-public data**

The general rule is that meetings cannot be closed to discuss data that are not public under the Minnesota Government Data Practices Act. A meeting must be closed, however, if the following not-public data is discussed:

- Data that would identify alleged victims or reporters of criminal sexual conduct, domestic abuse, or maltreatment of minors or vulnerable adults.
- Internal affairs data relating to allegations of law enforcement personnel misconduct or active law enforcement investigative data.
- Educational data, health data, medical data, welfare data or mental health data that are not-public data.
- Certain medical records.

**The following procedure must be used to close a meeting under this exception:**

- The council must state on the record the specific grounds for closing the meeting and describe the subject to be discussed.
- The meeting must be electronically recorded, and the recording must be preserved for at least three years after the meeting.

**H. Common issues**

This section provides an overview of some of the common issues cities face while attempting to comply with the open meeting law.
1. **Data practices**

Generally, meetings may not be closed to discuss data that is not public under the Minnesota Government Data Practices Act (MGDPA). However, the public body must close any part of a meeting at which certain types of not-public data are discussed.

If not-public data is discussed at an open meeting when the meeting is required to be closed, it is a violation of the open meeting law. Discussions of some types of not-public data may also be a violation of the MGDPA.

However, not-public data may generally be discussed at an open meeting without liability or penalty if both of the following criteria are met:

- The disclosure relates to a matter within the scope of the public body’s authority.
- The disclosure is necessary to conduct the business or agenda item before the public body.

Data that is discussed at an open meeting retains its original classification under the MGDPA. However, a record of the meeting is public, regardless of the form. It is suggested that not-public data that is discussed at an open meeting not be specifically detailed in the minutes.

2. **Interviews**

The Minnesota Supreme Court has held that a school board must interview prospective employees in open sessions.

The Supreme Court concluded that the absence of a statutory exception to the open meeting law for interviews indicated that the legislature had decided that such sessions should not be closed. The reasoning would seem to apply to a city council’s interview of prospective officers and employees as well, if a quorum is present.

In 1996, a district court found that it was not a violation of the open meeting law for candidates to be serially interviewed by members of a city council in one-on-one closed interviews. In this case, five city councilmembers were present in the same building but each was conducting separate interviews in five different rooms. Because there was no quorum present in any of the rooms, the court found there was no meeting. The decision, however, was appealed.

In 1997, the Minnesota Court of Appeals reversed the district court’s decision and remanded the case back to the district court for a factual determination on whether the city used the one-on-one interview process in order to avoid the requirements of the open meeting law.
On remand, the district court found that the private interviews were not conducted for the purpose of avoiding public hearings. The case was again appealed. In an unpublished decision, the court of appeals affirmed the district court’s decision.

The conclusion that can be drawn from this decision appears to be that if serial meetings involving less than a quorum of a public body are held for the purpose of avoiding the requirements of the open meeting law, it will constitute a violation of the law. Cities that are considering holding private interviews with job applicants should first consult their city attorney.

3. Executive sessions

The attorney general has advised that executive sessions of a city council must be open to the public.

4. Informational meetings and committees

The Minnesota Supreme Court has held that informational seminars about school-board business, which the entire board attends, must be noticed and open to the public. As a result, it appears that any scheduled gathering of a quorum of a city council where it receives information about city business must be properly noticed and open to the public, regardless of whether the council takes or contemplates taking action at that gathering.

In addition, many city councils create committees to make recommendations regarding a specific issue. Commonly, such a committee will be responsible for researching the issue and submitting a recommendation to the council for its approval. These committees are usually advisory, and the council is still responsible for making the final decision.

This type of committee may be subject to the open meeting law. Some factors that may be relevant in deciding whether a committee is subject to the open meeting law include: how the committee was created and who are its members; whether the committee is performing an ongoing function, or instead, is performing a one-time function; whether the committee receives public funds or uses public facilities or staff; and what duties and powers have been granted to the committee.

For example, the commissioner of the Minnesota Department of Administration has advised that “standing” committees of a city hospital board that were responsible for management liaison, collection of information, and formulation of issues and recommendations for the board were committees subject to the open meeting law. The advisory opinion noted that the standing committees were performing tasks that relate to the ongoing operation of the hospital district and were not performing a one-time or “ad hoc” function.
In contrast, the commissioner has advised that a city’s Free Speech Working Group was not a committee that was subject to the open meeting law. This group consisted of members, including city officials, that the city council had appointed to develop and review strategies for addressing free-speech concerns relating to a political convention that was going to be held in the city. The commissioner reasoned that the group was not a committee subject to the open meeting law because it did not have any decision-making authority.

City councils also routinely appoint individual councilmembers to act as liaisons between the council and particular groups. These types of groups may be considered a committee that is subject to the open meeting law.

The Minnesota Court of Appeals considered a situation where the mayor and one other member of a city council attended a series of mediation sessions regarding an annexation dispute that were not open to the public. The court of appeals held that the open meeting law did not apply to these meetings, concluding “that a gathering of public officials is not a ‘committee, subcommittee, board, department or commission’ subject to the open meeting law unless the group is capable of exercising decision-making powers of the governing body.”

The court of appeals also noted that the capacity to act on behalf of the governing body is presumed where members of the group comprise a quorum of the body and could also arise where there has been a delegation of power from the governing body to the group.

In addition, a separate notice for a special meeting of the city council may also be required if a quorum of the council will be present at a committee meeting and will participate in the discussion.

For example, when a quorum of a city council attended a meeting of the city’s planning commission, the Minnesota Court of Appeals ruled that there was a violation of the open meeting law, not because of the councilmembers’ attendance at the meeting, but because the councilmembers conducted public business in conjunction with that meeting.

Based on that decision, the attorney general has advised that mere attendance by additional councilmembers at a meeting of a council committee held in compliance with the open meeting law would not constitute a special city council meeting requiring separate notice. The attorney general warned, however, that the additional councilmembers should not participate in committee discussions or deliberations, absent a separate notice of a special city council meeting.
5. Chance or social gatherings

Chance or social gathering of city councilmembers will not be considered a meeting subject to the open meeting law as long as there is not a quorum present, or, if a quorum is present, as long as the quorum does not discuss, decide, or receive information about official city business.

The Minnesota Supreme Court has held that a conversation between two councilmembers over lunch regarding an application for a special-use permit did not violate the open meeting law because a quorum was not present.

6. Serial meetings

The Minnesota Supreme Court has noted that meetings of less than a quorum of the public body held serially to avoid public hearings or to fashion agreement on an issue may violate the open meeting law depending on the circumstances.

A Minnesota Court of Appeals’ decision also indicates that serial meetings could violate the open meeting law. The Minnesota Court of Appeals considered a situation where individual councilmembers conducted separate, serial interviews of candidates for a city position in one-on-one closed interviews. Although the district court found that no meetings had occurred because there was never a quorum of the council present, the court of appeals remanded the decision back to the district court for a determination of whether the councilmembers had used this interview process for the purpose of avoiding the requirements of the open meeting law.

On remand, the district court found that the private interviews were not conducted for the purpose of avoiding the requirements of the open meeting law. This decision was also appealed, and the court of appeals, in an unpublished decision, agreed with the district court’s decision.

A city that wants to hold private interviews with applicants for city employment should first consult with its city attorney.

7. Training sessions

Whether the participation of a quorum or more of councilmembers in a training program should be considered a meeting under the open meeting law would likely depend on whether the program includes a discussion of general training information or a discussion of specific matters relating to an individual city.

The attorney general has advised that a city council’s participation in a non-public training program devoted to developing skills at effective communication was not a meeting subject to the open meeting law.
However, the opinion also stated that if there were to be any discussions of specific city business by the attending members, such as where councilmembers exchange views on the city’s policy in granting liquor licenses, such discussions would likely violate the open meeting law.

The commissioner of the Department of Administration has likewise advised that a school board’s participation in a non-public team-building session to “improve trust, relationships, communications, and collaborative problem solving among Board members,” was not a meeting subject to the open meeting law if the members are not “gathering to discuss, decide, or receive information as a group relating to ‘the official business’ of the governing body.”

However, the opinion also advised that if there were to be any discussions of specific official business by the attending members, either outside or during training sessions, it could be a violation of the open meeting law.

8. **Telephone, email, and social media**

It is possible that communication through telephone calls, email, or other technology could violate the open meeting law. The Minnesota Supreme Court has indicated that communication through letters and telephone calls could violate the open meeting law under certain circumstances.

The commissioner of the Minnesota Department of Administration has advised that back-and-forth email communication among a quorum of a public body in which official business was discussed violated the open meeting law. However, the opinion also advised that “one-way communication between the chair and members of a public body is permissible, such as when the chair or a staff sends meeting materials via email to all board members, as long as no discussion or decision-making ensues.”

In contrast, the Minnesota Court of Appeals, in an unpublished decision, has concluded that email communications are not subject to the open meeting law because they are written communications and are not a “meeting” for purposes of the open meeting law.

The decision also concluded that even if the email messages were subject to the open meeting law, the substance of the emails in question did not contain the type of discussion that would be required for a prohibited “meeting” to have occurred. The decision noted that the substance of the email messages was not important and controversial; instead, it related to a relatively straightforward operational matter. The decision also noted that the town board members did not appear to make any decisions in their email messages.
Because this decision is unpublished, it is not binding on other courts. In addition, the outcome of this decision might have been different if the substance of the emails had related to something other than operational matters, for example, if the emails were attempting to build agreement on a particular issue that was going to be presented to the town board at a future meeting.

In 2014, the open meeting law was amended to provide that “the use of social media by members of a public body does not violate the open meeting law as long as the social media use is limited to exchanges with all members of the general public.” Email is not considered a type of social media under the new law.

The open meeting law does not define the term “social media,” but this term is generally understood to mean forms of electronic communication, including websites for social networking like Facebook, LinkedIn, and MySpace as well as blogs and microblogs like Twitter through which users create online communities to share information, ideas, and other content.

It is important to remember that the use of social media by city councilmembers could result in other claims, in addition to open meeting law claims, such as claims of defamation or of bias in decision making.

As a result, councilmembers should make sure that any comments they make on social media are factually correct, and they should not make any comments demonstrating bias on issues that will come before the council in the future for a quasi-judicial decision, such as the consideration of whether to grant an application for a conditional use permit.

It is also important to remember that serial discussions between less than a quorum of a public body that is subject to the open meeting law could violate the open meeting law under certain circumstances.

Therefore, city councils and other groups to which the open meeting law applies should take a conservative approach and avoid using letters, telephone conversations, email, and other such technology if the following circumstances exist:

- A quorum of the council will be contacted regarding the same matter.
- City business is being discussed.

Another thing councilmembers should be careful about is which email account they use to receive emails relating to city business because such emails would likely be considered government data that are subject to a public-records request under the Minnesota Government Data Practices Act (MGDPA). The best option would be for each councilmember to have an individual email account that the city provides and city staff manage.
However, this is not always possible for cities due to budget, size, or logistics.

If councilmembers don’t have a city email account, there are some things to think about before using a personal email account for city business. First, preferably only the councilmember should have access to the personal email account. Using a shared account with other family members could lead to information being inadvertently deleted. Also, since city emails are government data, city officials may have to separate personal emails from city emails when responding to a public-records request.

Second, if the account a city councilmember wants to use for city business is tied to a private employer, that private employer may have a policy that restricts this kind of use.

Even if a private employer allows this type of use, it is important to be aware that, in the event of a public-records request under the MGDPA or a discovery request in litigation, the private employer may be compelled to have a search done of a councilmember’s email communication on the private employer’s equipment or to restore files from a backup or archive.

What may work best is to use a free, third-party email service, such as gmail or Hotmail, for your city account and to avoid using that email account for any personal email or for anything that may constitute an official record of city business since such records must be retained in accordance with the state records-retention requirements.

I. **Advisory opinions**

1. **Department of Administration**

The commissioner of the Minnesota Department of Administration has authority to issue non-binding advisory opinions on certain issues related to the open meeting law.

A court or other tribunal must give deference to an advisory opinion. A $200 fee is required. The Data Practices Office (DPO) of the Department of Administration handles these requests.

A public body subject to the open meeting law can request an advisory opinion from the commissioner. In addition, a person who disagrees with the manner in which members of a governing body perform their duties under the open meeting law can also request an advisory opinion.

2. **Minnesota Attorney General**

The Minnesota Attorney General is authorized to issue written advisory opinions to city attorneys on “questions of public importance.”
The Attorney General has issued several advisory opinions on the open meeting law.

Opinions of the Attorney General are not binding on the courts but are entitled to careful consideration when they are of long standing.

J. Penalties

An action to enforce the open meeting law may be brought by any person in any court of competent jurisdiction where the administrative office of the governing body is located. In an unpublished decision, the court of appeals concluded that this broad grant of jurisdiction authorized a member of a town board to bring an action against his own town board for alleged violations of the open meeting law.

This same decision also concluded that a two-year statute of limitations applies to lawsuits under the open meeting law.

A councilmember who intentionally violates the open meeting law can be subject to personal liability in the form of a civil penalty of up to $300. The city may not pay this penalty. A court may take into account a councilmember's time and experience in office to determine the amount of the penalty.

In addition, a court may award reasonable costs, disbursements, and attorney fees of up to $13,000 to the person who brought the violation to court. The court may award costs and attorney fees to a city only if the action is found to be frivolous and without merit. A city may pay for any costs, disbursements, and attorney fees awarded.

If a plaintiff prevails in a lawsuit under the open meeting law, an award of reasonable attorney fees is mandatory if the court determines the public body was the subject of a prior written advisory opinion from the commissioner of the Department of Administration, and the court finds that the opinion is directly related to the lawsuit and that the public body did not act in conformity with the opinion.

A court is required to give deference to the advisory opinion in a lawsuit brought to determine whether the open meeting law was violated.

No monetary penalties or attorney fees may be awarded against a member of a public body unless the court finds there was intent to violate the open meeting law.
If a person is found to have intentionally violated this chapter in three or more separate, sequential actions, the person must be removed from office and may not serve in any other capacity with that public body for a period of time equal to the term of office the person was serving.

If a court finds a separate, third violation that is unrelated to the previous violations, it must declare the position vacant and notify the appointing authority or clerk of the governing body.

As soon as practicable, the appointing authority or governing body shall fill the position as in the case of any other vacancy.

The open meeting law does not address whether actions taken at an improper meeting would be invalid. The Minnesota Supreme Court once held that an attempted school district consolidation was fatally defective when the initiating resolution was adopted at a meeting that was not open to the public.

However, in more recent decisions, Minnesota courts have refused to invalidate actions taken at improperly closed meetings. The Minnesota Supreme Court has noted that the open meeting law does not provide for such a remedy because the open meeting law “does not specify that actions taken at a meeting which is not public shall be invalid.”

### III. Meeting procedures

#### A. Agendas

The city clerk generally prepares an agenda for council meetings. The agenda is then given to councilmembers and other interested individuals such as department heads and citizens.

The agenda establishes the order in which the matters will be addressed during the meeting.

Many city councils have found the following order of business convenient:

- Call to order.
- Roll call.
- Approval of minutes from previous meeting.
- Consent agenda.
- Petitions, requests, and complaints.
- Reports of officers, boards, and committees.
- Reports from staff and administrative officers.
1. **Consent agenda**

The consent agenda or consent calendar is used by many city councils to help shorten the length of meetings by using time more efficiently. A consent agenda typically groups together many items that are routine and uncontroversial. Although the council must take action on these items, they do not require further discussion.

Examples of items typically included in a consent agenda are the approval of the minutes of the previous meeting, the setting of the next meeting date, approval of routine expenditures, and the final approval of licenses and permits.

The council generally approves all items on the consent agenda with the passage of one motion. If there is any item on the consent agenda that a councilmember feels needs further discussion, it is removed from the consent agenda and dealt with individually. It may be placed anywhere within the regular agenda.

The consent agenda may be a valuable tool for city councils that have to deal with many routine matters. Some city councils may need to amend their bylaws to allow the use of this procedure.

2. **Discussing items not on the agenda**

Whether the council can discuss an item that was not included on the agenda is a question that may not have a clear answer. In part, the answer may depend upon the type of meeting and the meeting rules the council has adopted.

Cities should first check any rules the council has adopted and any charter provisions, if the city is a home rule charter city. These local items may give more specific guidance where state law is vague.

a. **Regular meetings**

State statutes do not specifically address the ability of city councils to address items that are not on the agenda at a regular meeting.
However, it seems to be common practice for councils to address items that were not originally on the agenda of a regular meeting by providing for a time for miscellaneous items on the agenda.

b. **Special meetings**

The open meeting law requires cities to give notice of a special meeting to the public. This notice must include the date, time, place, and purpose of the meeting. At the special meeting, councilmembers should only address the specific issue or issues that the notice lists as the purpose of the meeting.

c. **Emergency meetings**

The open meeting law requires that the notice provided for an emergency meeting must include the subject of the meeting. Councils should avoid discussing other topics. The open meeting law also provides that if matters not directly related to the emergency are discussed or acted upon in an emergency meeting, the meeting minutes shall include a specific description of the matters.

B. **Minutes**

City officers must keep all records necessary to provide a full and accurate knowledge of their official activities.

A statutory city clerk must record the minutes of council proceedings. In the clerk’s absence, the council should delegate the duty of taking minutes for that meeting. Generally, the clerk has wide discretion as to how to keep the minutes. A verbatim record of everything that was said is not normally required. However, in any case where the law or charter requires a word for word record, using a tape recorder instead of a court reporter to accomplish that objective is probably valid.

Minutes should be written in language average people can understand. Reference to numbers of ordinances, resolutions, and other matters should include a brief description of their subject matter.

If the council finds a mistake in the minutes of the previous meeting, the clerk should correct the minutes. If the clerk declines to make the correction, the council can order the change by motion and a vote. The clerk must then make the change and show in the minutes that the change was made by order of the council.
The council may provide books and stationery for keeping minutes. State law requires all cities to keep minutes on a physical medium that is of a quality that will ensure permanent records. It appears that a city may keep minutes and other official records in an electronic format if the format is of a quality that will ensure permanent records.

Because minutes would likely be considered official papers of the city, they should be signed by the clerk. Although not required by law, in many cities the mayor also signs the minutes after the council approves them. If the minutes include only a clipping from the published proceedings, the clerk should sign the clipping even though the signatures of the clerk and mayor are already printed on the clipping. Minutes of open meetings are public records and must be available for public view at any reasonable time.

1. Required contents

The following items must be included in the minutes:

- The members of the public body who are present.
- The members who make or second motions.
- Roll call vote on motions.
- Subject matter of proposed resolutions or ordinances.
- Whether the resolutions or ordinances are defeated or adopted.
- The votes of the members of the council.
- The votes of each member, including the mayor must be recorded on each appropriation of money, except for payments of judgments, claims, and amounts fixed by statute.

2. Other items that should be in the minutes

The Office of the State Auditor has also recommended that meeting minutes include the following information in addition to the information required by state statute.

- Type of meeting (regular, special, emergency, etc.)
- Type of group meeting (city council, planning committee, etc.)
- Date and place the meeting was held.
- Time the meeting was called to order.
- Approval of minutes of the previous meeting, with any corrections.
- Identity of parties to whom contracts were awarded.
- Abstentions from voting due to a conflict and the member’s name and reason for abstention.
- Reasons the governing body awarded a particular contract to a bidder other than the lowest bidder.
3. Making a good record

It is important to make a good record of council decisions and of the factual information on which council members base their decisions. Minutes are the primary record of the decision-making process and are critical if council actions are challenged.

Council actions are generally classified as either legislative or administrative. The establishment of general policies and procedures is legislative action and is subject to limited judicial review. Courts typically will not substitute their judgment for a council’s judgment on these topics.

Administrative or quasi-judicial actions involve the application of a general policy to a specific person or situation. An example of a quasi-judicial decision is a city council’s decision regarding whether an applicant has satisfied the criteria for the issuance of a conditional use permit. Administrative actions are subject to greater judicial scrutiny and will be set aside if they are arbitrary or unreasonable. Therefore, it is important for the council to develop a good record with findings of fact to support this type of decision.

The term “findings of fact” is commonly used to refer to a public body’s written explanation supporting a particular decision. Making a record of a city council’s findings of fact can help a city defend its decisions if they are challenged.

When the city council or other public body holds a hearing, the record usually consists of two separate parts: the transcript, which preserves testimony, and the final order or determination. Following is a sample outline of the different parts of a record supporting a city council’s decision on an application for a conditional use permit.

Swanson v. City of Bloomington, 421 N.W.2d 307 (Minn. 1988).
Dietz v. Dodge County, 487 N.W.2d 237 (Minn. 1992).
See Handbook, Comprehensive Planning, Land Use, and City-Owned Land, section III for more information about findings of fact.
4. Approval of minutes by council

Although it is not statutorily required, the council generally approves the minutes at the next council meeting. After the minutes have been approved, they become the official permanent record of the council meeting.

A member of a public body may vote to approve minutes of a meeting even if the member was not at the meeting in person unless a city council has adopted procedural rules that prohibit it.

Robert’s Rules of Order Newly Revised provides that a member’s absence from the meeting for which minutes are being approved does not prevent the member from participating in their correction or appeal.

Someone may request a copy of the minutes before the council approves them. The draft of the minutes is public data, and the clerk must give out such information if someone requests it, but should clarify that the draft minutes have not been officially approved.

5. Publication

A statutory city with a population of 1,000 or more must publish the council’s official proceedings or a summary of them in its official newspaper within 30 days after every regular and special meeting. If the city council conducts regular meetings not more than once every 30 days, however, it need not publish the meeting minutes until 10 days after the council has approved them. A less expensive alternative is also available; instead of publishing the minutes, the city may mail a copy, at city expense, to any resident upon request. Statutory cities with a population of less than 1,000 are exempt from both of these requirements. Home rule charter cities should check their charters for any publication requirements.

If a statutory city chooses to publish a summary or condensed version of the official minutes, it must meet the following criteria:

- It must be written in a clear and coherent manner.
- It must avoid the use of technical or legal terms not generally familiar to the public.
• The publication must indicate it is only a summary.
• The publication must indicate the full text of the minutes is available for public inspection at a designated location.

C. Rules of procedure
The city council has the power to regulate its own procedure. While many city councils operate without written rules or regulations, written rules may facilitate the conduct of city business and reduce the risk of mishandling important matters.

Council bylaws usually cover issues like the place and time of regular council meetings, the order of business, parliamentary rules governing council procedures, minutes, and standing and special committees.

D. Parliamentary procedure
The council usually adopts rules or bylaws that govern procedural rules. Adoption of council rules may be supplemented by the use of a standard work on parliamentary procedure, such as Robert’s Rules of Order.

Because of the small size of most city councils, procedures at council meetings, particularly in discussions, tend to be quite informal and many cities prefer to keep things simple and use just the basic rules regarding motions and voting, rather than adopting a more complex set of procedures.

The council should follow whatever procedural rules it adopts. Although the council can vote to change or suspend its rules if the occasion calls for it, it is probably better to stick with the adopted rules except on rare occasions.

E. Audience participation
The people attending a council meeting do not normally take part in the council’s discussion at a meeting. Only city councilmembers and the elected city clerk in Standard Plan statutory cities can make motions and vote at council meetings. However, many city councils schedule a portion of their meeting for public comment. This is often referred to as an open forum. During this part of the meeting the chair of the council will recognize members of the audience to speak briefly on topics that concern them.

If a large number of audience members wish to speak, the meeting may not progress efficiently. Likewise, if one person spends a long time expressing his or her view, others may not get the opportunity to present their views. The following sections discuss ways to address some of these problems.
1. Limiting time

Some councils have addressed this problem by placing a limit on the amount of time audience members are allowed to speak at a meeting. For example, the council may ask people to limit their remarks to no more than three minutes or allow only a specified number of people to speak.

A number of cities have established rules or guidelines that citizens must follow when speaking at a meeting. Often, the speaker must notify the city at least one day in advance so that he or she can be put on the agenda. When a person notifies the city of his or her desire to speak at the meeting, he or she is given a copy of the “rules of conduct,” which lists the time limit for speaking and any other city limitations. This gives the person time to plan his or her speech so it fits within the time limit. The mayor then reminds the speaker of the time limit before the speaker begins to speak. Some cities will have a clock visible to the speakers so they can see when their time for speaking is over.

2. Limiting topic

Another option may be to limit the scope of comments to those matters being addressed by the council at the specific meeting.

While this may be a way to focus the meeting on the matters being addressed by the council, it might also keep people from making the council aware of any new issues. Cities considering this approach might need to allow for other ways for people to bring up other topics.

Some cities will establish general rules outlining when citizens may speak at council meetings. Often these guidelines will require that the topic be identified in writing a few days before the actual meeting. The specific topic and the speaker’s name are then put on the agenda. Such procedures are helpful in allowing the council to plan an efficient meeting and to prepare a response to the issue if needed. It also helps to remind the speaker that he or she may only address those issues on the agenda.

F. Maintaining order

A statutory city council is authorized to preserve order at its meetings. The mayor, as the presiding officer, is also vested with some authority to prevent disturbances.

While council meetings must be open to the public, no one who is noisy or unruly has a right to remain in the council chambers. When the council decides that a disorderly person should not remain in the meeting hall, the police may be called to execute the orders of the presiding officer or the council.
No matter how disorderly the meeting, it will still be a legal meeting and any action taken at it in proper form will be valid.

If the audience becomes so disorderly that it is impossible to carry on a meeting, the mayor has the right to declare the council meeting adjourned to some other time (and place, if necessary). The members of the council can also move for adjournment.

If the mayor is not conducting the meeting in an orderly fashion, there is relatively little the other councilmembers can do to control the action of the presiding officer. However, a majority of the council can force adjournment if they feel it is necessary.

A person who disturbs a lawfully held public meeting may be guilty of disorderly conduct. Any conduct that disturbs or interrupts the orderly progress of council proceedings is a disturbance that may generally be prevented, or punished if an ordinance violation is involved.

G. Role of Mayor, Clerk, and City Manager

1. Mayor

The mayor of a statutory city is a member of the council, and has the same right to vote and make and second motions at meetings as the other council members.

The mayor is the presiding officer of the meeting. In the absence of the mayor, the acting mayor must perform the duties of the mayor. The acting mayor is chosen at the first meeting of each year.

In some charter cities, the mayor might abstain from voting or participating unless there is a deadlock. This practice can help to preserve the neutrality of the chair of the meeting. However, counting votes at a meeting where a member abstains can sometimes be tricky.

In some charter cities, the mayor has veto power. Charter cities should consult their charters for more information.

2. Clerk

In a Standard Plan statutory city, the clerk is an elected member of the council. As such, he or she has the same voting powers and other privileges as do the other councilmembers. Like the mayor, the clerk in a Standard Plan city is able to make and second motions.
In Plan A or Plan B statutory cities, the clerk is not a member of the council, and therefore, cannot vote or participate in council proceedings. Again, home rule charter cities may have different provisions in their charters.

3. City managers

In a Plan B statutory city, the city manager must attend all council meetings.

He or she has the right to take part in the discussions, but not to vote. The council has the power to exclude the city manager from any meeting at which the manager’s removal is considered.

4. Voting

City councils meet to discuss matters relating to city business and to make decisions for the city. When a matter is brought to a vote, the votes must be recorded in the minutes. The vote of each individual councilmember (including the mayor) must also be recorded on each appropriation of money, except for the payment of judgments, claims, and amounts fixed by statute.

Because of this requirement, city councils may not vote by secret ballot on matters addressed at council meetings unless the vote can be taken in such a manner that would comply with the statute’s requirement.

In addition, The Minnesota Court of Appeals has concluded that secret voting violates the purposes of the open meeting law. The Court of Appeals reasoned that a meeting is not “open” to the public if voting is conducted in secret because it denies the public the right to observe the decision-making process, to know councilmembers’ stance on issues, and to be fully informed about the council’s actions.

a. Counting votes

Most of the time, a city council acts by majority vote; however, sometimes a simple majority vote is not enough for a matter to pass. Depending upon the matter before the council, more votes may be needed. Likewise, a home rule charter city may have additional requirements in its charter.

(1) Entire council is present

When the entire council is present and all members vote, it is generally simple to determine if a matter has passed.

(a) Achieving a quorum

A majority of the members of a statutory city council shall constitute a quorum.
Obviously, when all members are present, a quorum has been achieved.

(b) Motions and resolutions

A majority of the quorum is needed to pass most motions and resolutions. Since most statutory cities have a five-member council, this means that three votes are normally needed if all members are present and voting.

In a statutory city with a seven-member council, it would take at least four votes to pass most motions or resolutions if all members are present and voting.

(c) Most ordinances

A simple majority vote of an entire statutory city council is needed to pass most ordinances, regardless of the number of councilmembers present. This means that three votes are needed to pass an ordinance in a city with a five-member council. In a statutory city with a seven-member council, four votes are needed to pass most ordinances. However, some ordinances require more than a simple majority vote.

(d) Situations where statutes require extraordinary votes

Several statutes require more than a simple majority to take certain kinds of actions. The following are some examples:

- Adoption or amendment of zoning ordinances that change existing zoning from residential to commercial or industrial.
- Adoption or amendment of comprehensive plans.
- Abolishment of a planning agency.
- Some capital improvements and acquisition or disposal of real property if the city has a comprehensive plan.
- Contracts that are allowed even though one of the officers has a personal financial interest. Generally, a councilmember may not have a financial interest in a city contract. However, the statutes allow certain exceptions to this rule. If such a contract is permitted under an exception, the statute requires that it be approved by unanimous vote of the council. In some cases, state law specifically requires an interested officer to abstain from voting, but it is probably advisable for an interested officer to abstain from discussion and voting, regardless of whether the statute specifically requires it.
- Some local improvements that will be paid for with special assessments.
- Some types of charter amendments.
- Summary publication of ordinances in statutory cities.
- Abolishing or changing the size of a statutory city park board.
- Some street vacations.
- Abolishment of a hospital board.
Home rule charter cities may have other supermajority vote requirements in their charters.

(2) Vacancies

A vacancy temporarily reduces the size of the council; therefore, when there is a vacancy on a five-member council, the entire council consists of four people. For actions that require approval by a specified portion of the council, the required number of votes is calculated using the current number of seats that are filled.

(a) Achieving a quorum

Since a majority of a statutory city council is needed to achieve a quorum, a vacancy can affect the number of members that must be present in order to hold a meeting. One vacancy on a five-member council would not reduce the number of members needed to achieve a quorum (since both a majority of five and a majority of four is three).

However, if there were two vacancies on a five-member council, the council would consist of three members and a majority of the council would be two members.

(b) Motions and resolutions

Since most motions and resolutions must be approved by a majority of those present at a meeting, a vacancy generally will have the same effect as an absence. A majority of those present must vote to approve in order for most motions and resolutions to pass.

(c) Most ordinances

Since most ordinances must be approved by a majority of the entire council, vacancies on the council can affect the number of votes needed to pass an ordinance. For example, if there were two vacancies on a five-member council, the entire council would consist of three members. In this case, a majority of the entire council would be two rather than three.

(d) Situations where statutes require extraordinary votes

If a statute or charter provision requires a specific number of votes (rather than a percentage of the council), the vacancy probably won’t affect the required numbers of votes.

(3) Absences

A councilmember’s absence from a meeting does not affect the number of votes needed if a statute requires an affirmative vote by a specified portion of the entire council.
(a) Achieving a quorum

Absences can certainly affect the ability of a city council to achieve a quorum, since a majority of a statutory city council is needed to achieve a quorum. For example, if one or two members of a five-member council are absent, the three remaining council members would constitute a quorum. However, if three members are absent, the remaining two members would not be able to hold a meeting because a quorum would not be present.

(b) Motions and resolutions

Since most motions and resolutions must be approved by a majority of those present in order to pass, an absence can affect the number of votes needed. The general rule is that if a quorum is present, a majority of the quorum can pass any action unless a statute or charter provision requires a larger number. The fewer members present, the fewer needed to constitute a majority.

For example, if two members of a five-member council are absent, the remaining three constitute a quorum. A 2-1 vote is sufficient to pass most motions at such a meeting. However, if all five members are present, at least three votes would be needed to pass the same motion.

(c) Most ordinances

The absence of a council member from a meeting does not affect the number of votes needed if the statutes require that a specified portion of the entire council is needed to approve an action. For example, it takes a majority of the entire council to pass an ordinance in a statutory city. In most statutory cities, a majority is three votes. If one council member is absent, it would still take a majority of the entire council (or three votes) to pass the ordinance.

(d) Situations where statutes require extraordinary votes

The absence of a council member will not affect the number of votes needed if a statute requires approval by a specific number of votes or a certain portion of the entire council.

(4) Abstentions

Sometimes a council member who is present at a meeting will choose not to vote on a matter before the council. In some home rule charter cities, a mayor might not vote unless there is a tie. If a council member or mayor does not vote, it is recorded in the minutes as an abstention. How the abstention should be considered can sometimes depend upon the reason for the member’s abstention.
(a) Achieving a quorum
Whether or not a councilmember abstains would not appear to have an effect on whether or not a quorum exists, and the meeting may be held.

(b) Motions and resolutions
Generally, a motion or resolution is passed if the majority of those voting vote in favor of it. It’s not entirely clear, however, if a court would apply this rule to the extreme case where a quorum is present but because of abstentions the number of affirmative votes is less than a majority of the quorum. Again, it may depend upon the reason behind the abstention.

(c) Most ordinances
An abstention by one or more councilmembers does not reduce the number of votes needed if a statute or charter provision specifies a certain number of votes.

For example, in a statutory city with a five-member council, three affirmative votes are needed to pass most ordinances; two “yes” votes and three abstentions are not enough.

However, if the abstention is required because a councilmember is disqualified from voting (such as when one member has a personal interest in the matter being considered by the council), the abstention is treated like a vacancy. In this type of situation, the size of the council is temporarily reduced.

(d) Situations where statutes require extraordinary votes
An abstention by one or more councilmembers does not reduce the number of votes needed if the statutes require the affirmative vote of a specific number or proportion of the entire council. For example, in a case where a seven-member board attempted to pass a zoning amendment that required a two-thirds vote of its members, three members abstained and four voted in favor of the amendment. The court ruled that this vote was not sufficient to pass the ordinance.

(e) Councilmembers who have a disqualifying interest
Councilmembers who have a disqualifying interest are generally excluded when counting the number of votes needed to approve an action by a supermajority vote. An example of such a situation was a local improvement project where two town board members owned property that was going to be assessed for the improvement. The court found it was proper for the two to abstain in this case, and that three affirmative votes were sufficient to meet the four-fifths majority vote requirement.
Although councilmembers may be tempted to abstain from voting on a controversial matter, they should remember that the abstention will ultimately tend to pass or defeat the matter. The best advice is to avoid the kinds of problems that can arise from abstentions and vote, unless an abstention is required because a councilmember has a personal interest in the matter.

b. **Long-distance voting**

Although the open meeting law permits meetings to be held by interactive television, and in the case of a health pandemic or an emergency, permits meetings to be held by telephone or other electronic means, the use of other types of technology to vote while not physically present at a meeting have not yet been authorized.

(1) **Voting by proxy**

Sometimes councilmembers who are not able to be at a meeting want to vote on a matter that will be addressed at the meeting.

State law does not permit a statutory city councilmember to vote by proxy. Home rule charter cities may find permission in their charters.

(2) **Voting by phone**

Likewise, unless there is a health pandemic or an emergency, state law does not authorize a councilmember to phone-in a vote or to participate in the meeting by conference call, or other electronic means unless it satisfies the requirements for use of interactive television.

H. **Attendance of councilmembers**

It is important for all councilmembers to attend their city council meetings. When members are absent from a meeting, it can be difficult for the council to conduct business. Such difficulties can include the inability of the council to achieve a quorum, the difficulty in getting the needed number of votes to approve an action, and the difficulty in counting votes.

In statutory cities, a majority of all the councilmembers constitutes a quorum. This means that at least three members of a five-member council or four members of a seven-member council must be present in order for the council to hold a meeting. Home rule charter cities may have different quorum requirements.

1. **Time off from employment**

An elected official must be given time off from employment to attend meetings that are required because of the office.
The time off may be with or without pay.

If the time off is without pay, the employer must make an effort to allow the person to make up the hours at another time when he or she is available. An employer cannot retaliate against an employee who must take time off to attend such meetings.

2. Non-attendance

Sometimes, a city council will find that a councilmember is not attending council meetings. The absences may be due to a variety of reasons, such as illness, extended vacations, or refusal to attend. Whatever the reason, such extended absences can make it difficult for the council to do its job. This section discusses some of the things city councils can consider to remedy this type of problem.

a. Reprimands

The attorney general has indicated a city council could reprimand a councilmember for missing meetings.

The council would do this by passing a resolution. While such a reprimand might create political pressure and embarrassment for the absent councilmember, it won’t necessarily compel the councilmember to attend meetings.

b. Compelling attendance

State law authorizes a statutory city council to compel the attendance of its members and punish them for non-attendance. Unfortunately, it is not clear how this power should be exercised.

It might be possible to compel the attendance of a councilmember through a mandamus action, which is a court order to force a public officer to perform a specific duty of his or her office. This type of remedy may be pursued by the city, individual councilmembers, or a citizen. However, city officials should consult with their city attorney before considering this approach.

c. Council pay

State law prohibits cities from diminishing a councilmember’s pay for absences because of illness or vacation. As a result, if the council’s salary is set at a monthly or annual salary, the councilmembers are entitled to receive that pay if they fail to attend meetings because of illness or vacation.

On the other hand, it might be possible to set council compensation on a per-meeting basis. It should be noted that this state statute has not yet been interpreted by the courts or the attorney general.
d. Fines

A system of fines may be an option a statutory city council could use to punish a councilmember for non-attendance. If a city wants to use this approach, it should adopt an ordinance or rule establishing a system of fines for missing meetings. However, as discussed above, a city cannot diminish a councilmember’s salary for absences that are the result of illness or vacation.


e. Temporary replacement of councilmembers

Statutory cities have an option to temporarily replace a councilmember under certain circumstances. A vacancy in the office of mayor or councilmember may be declared by the council if either of the following occurs:

- An officeholder is unable to serve in the office or attend council meetings for a 90-day period because of illness.
- An officeholder refuses to attend council meetings for a 90-day period.

If either of these conditions occurs, the council may declare a vacancy to exist and fill it at a regular or special council meeting. The vacancy may be filled for the remainder of the unexpired term or until the person is able to resume duties and attend council meetings, whichever is earlier. When the person is able to resume duties and attend council meetings, the council shall by resolution remove the temporary officeholder and restore the original officeholder.

Home rule charter cities may use the same procedure described in this statute if their charter is silent on the matter.

f. Abandonment of office

Continued failure to attend council meetings may be grounds for a city council to find that an office has been abandoned and declare that the office is vacant. The attorney general has described abandonment as a form of resignation, and indicated that the officer’s intent is a key issue in determining whether there has been an abandonment of the office.

Whether an office has actually been abandoned is a question of fact that must be determined on a case-by-case basis. The attorney general has said that mere absence by itself does not mean that the office has been abandoned. Following a 90-day period, the office may be declared vacant and the officer replaced on a temporary basis. There are no clear guidelines as to how long a councilmember must be absent in order for the office to be considered permanently vacant.
If the city council believes that the absent councilmember has abandoned the office, it can pass a resolution making this finding. The council should first give the absent councilmember notice and an opportunity to be heard. A city council that is considering declaring an office vacant due to abandonment should first consult with its city attorney.

g. **Criminal penalties**

It is a gross misdemeanor for a public officer to intentionally fail to perform a known mandatory, nondiscretionary, ministerial duty of his or her office. It is arguable that attending council meetings might fall into this category of duties for councilmembers.

This type of remedy may be an extreme measure. Conviction may constitute a violation of the councilmember’s oath of office, which would result in the office being vacant. Again, a city council that is considering this remedy should first consult with its city attorney.

I. **Meeting room**

1. **Smoking**

   The Minnesota Clean Indoor Air Act prohibits smoking at a public meeting to protect city employees and the public from the hazards of secondhand smoke. This prohibition also applies to the use of electronic cigarettes.

2. **Accessibility**

   Both the meeting and the meeting room must be accessible. To ensure accessibility, the meeting should be located in a room that all people, including people with mobility impairments, will be able to reach. Cities may also need to have individuals sign for people with hearing loss and have written materials available in large print, Braille or audio cassette for people with sight impairments.

J. **Broadcasting and recording of meetings**

   The attorney general has advised that the public may tape record a meeting if it will not have a significantly adverse effect on the order of the meeting or impinge on constitutionally protected rights. Neither the public body nor any councilmember may prohibit dissemination or broadcast of the tape.

   A city may tape record or videotape a meeting. The tape is a city record and must be kept in accordance with the city’s record-retention policy. As a city record, such a tape must also be made available to the public if it contains public data.
Even though video tapes and sound recordings may indicate word for word what occurred at a meeting, they are not the official record of the meeting. The approved minutes are the official record of the meeting.

All closed meetings, except those closed as permitted by the attorney-client privilege, must be electronically recorded at the expense of the public body. Unless a different time period is provided by law, the recordings must be preserved for at least three years after the date of the meeting.

Many cities broadcast their council meetings over cable television. Such broadcasts may need to be closed-captioned or signed in order to provide effective communication for persons with disabilities.

While the Americans with Disabilities Act has always required cities to provide auxiliary aids and services when necessary to ensure effective communication, federal regulations now specifically allow for the use of video remote interpreting services as long as the city complies with certain performance standards addressing high-speed internet connection, video and audio quality, and user training.

The regulations also provide guidance on cities’ obligations to communicate with disabled family members and other companions and on using children as interpreters (which is prohibited unless no other interpreter is available and an emergency situation exists). A city should never require an individual to bring his or her own interpreter, but may honor a specific request to allow an adult accompanying a disabled individual to interpret where reliance on that person is appropriate.

K. **Prayer and city council meetings**

City councils sometimes start their meetings with a prayer or religious invocation offered by someone who is not on the council. Courts generally refer to this as “legislative prayer.” City councils have authority to choose whether to include legislative prayer at their meetings. City councils that want to set a serious tone for their meetings could also consider some other ceremonial act, such as reciting the Pledge of Allegiance, as an alternative to opening their meetings with legislative prayer.

The use of legislative prayer raises two main constitutional issues: first, whether it violates the First Amendment to the U.S. Constitution, which prohibits the government from establishing a religion; and second, whether it violates the provisions in the Minnesota Constitution providing for the right to exercise one’s religious beliefs without infringement.

The 8th Circuit U.S. Court of Appeals has held that a county board’s practice of opening its meetings with legislative prayer did not violate either the U.S. Constitution or the Minnesota Constitution.
The Court of Appeals noted that the county’s use of legislative prayer served a secular or non-religious purpose of establishing a solemn atmosphere and serious tone for its meetings.

The U.S. Supreme Court has held that a town board’s practice of opening its meetings with legislative prayer did not violate the Establishment Clause of the First Amendment to the U.S. Constitution. The Supreme Court reasoned that the Establishment Clause must be read with an understanding of its historical tradition and noted that the men who wrote the U.S. Constitution “considered legislative prayer a benign acknowledgment of religion’s role in society.”

The Supreme Court noted several factors that supported its decision to uphold the town board’s use of legislative prayer. First, it noted that the prayer occurred at the beginning of the meetings instead of during the decision-making part of the meetings. Likewise, city councils that choose to include legislative prayer should limit it to the beginning of their meetings. This practice will help reduce the chances that an individual attending a meeting will feel pressured to participate in the prayer because of a concern that the failure to do so may affect how the council will act on a specific decision affecting that individual, such as whether to approve a variance, license, or contract.

Second, the Supreme Court noted that the elected officials were the intended audience of the legislative prayer and found this acceptable. If city councils decide to include legislative prayer at the beginning of their meetings, it is best to view it as a benefit to the city council, not to other meeting attendees.

Third, the Supreme Court noted that participation in the town board’s legislative prayer was voluntary. City councils that include legislative prayer in their meetings also should be careful not to require the public to participate in the prayer and should not criticize anyone who chooses not to bow his or her head, stand, or otherwise engage in the prayer.

Fourth, the Supreme Court noted that the town board “at no point excluded or denied an opportunity to a would-be prayer giver.” City councils that include legislative prayer at their meetings also should not discriminate against any prayer givers based on their religious beliefs and should make efforts to ensure that prayer givers represent a diversity of religious beliefs.

The Supreme Court upheld the town clerk’s practice of using the local business directory to contact churches seeking volunteer ministers to offer legislative prayer at town meetings. The Supreme Court reasoned, “So long as the town maintains a policy of nondiscrimination, the Constitution does not require it to search beyond its borders for non-Christian prayer givers in an effort to achieve religious balancing.”
Fifth, the Supreme Court noted that the town board “neither reviewed the prayers in advance of the meetings nor provided guidance as to their tone or content.” The town board’s opening prayers were overwhelmingly Christian in content. But the Supreme Court held that legislative prayer does not need to be nonsectarian, or not identifiable with any one religion, reasoning that adopting such a requirement would not be consistent with the history of legislative prayer and would force the town board to act as a censor of religious speech. City councils that include legislative prayer in their meetings generally should not tell prayer givers what they can or cannot say in their prayers.

However, there are likely some reasonable limits on the content of legislative prayer. The Supreme Court indicated, for example, that legislative prayers that consistently criticize nonbelievers, threaten damnation, or preach conversion do not accomplish an acceptable legislative purpose, and therefore, may raise constitutional concerns. The Supreme Court noted that the town board’s use of legislative prayer served the acceptable legislative purpose of setting a solemn and respectful tone for its meetings.

Finally, it may be constitutional to pay a person to offer legislative prayer. Courts have looked to the history of such a practice, noting that Congress and many state legislatures have paid persons to offer legislative prayer. While this may be more common practice at higher levels of government, the more typical practice for cities is to use unpaid volunteers to offer legislative prayers.
Appendix A: Table of motions

(Note: Also see discussion under Part III – D Parliamentary procedure)

There are three basic types of motions: privileged motions, subsidiary motions, and main motions. Privileged motions take precedence over subsidiary motions; subsidiary motions take precedence over main motions. The following charts of motions are listed in order of precedence and are based upon Robert’s Rules of Order Newly Revised, 10th Edition (2000):

Chart A: Privileged motions. A privileged motion is a motion that does not relate to the business at hand. Such a motion usually deals with items that require immediate consideration.

<table>
<thead>
<tr>
<th>Motion</th>
<th>Requires a second</th>
<th>Can interrupt speaker</th>
<th>Debatable</th>
<th>Amendable</th>
<th>Votes required to pass</th>
<th>Can be reconsidered</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fix a time to adjourn.</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>Majority</td>
<td>✓</td>
</tr>
<tr>
<td>To adjourn.</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Recess. (A motion to take an intermission.)</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td></td>
<td>Majority</td>
<td></td>
</tr>
<tr>
<td>Raise a question of privilege. (A motion referring to a matter of personal concern to a member. Examples are asking to have the heat turned up, the windows opened, less noise, or requesting that the motion be stated again.)</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td>Usually, no vote is taken. The chair decides.</td>
<td></td>
</tr>
<tr>
<td>Call for the orders of the day. (Forces the consideration of a postponed motion.)</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**Chart B: Subsidiary motions.** A subsidiary motion is a motion that assists the group in disposing of the main motion.

<table>
<thead>
<tr>
<th>Motion</th>
<th>Requires a second</th>
<th>Can interrupt speaker</th>
<th>Debatable</th>
<th>Amendable</th>
<th>Votes required to pass</th>
<th>Can be reconsidered</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lay on the table. (To postpone discussion temporarily.)</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td>Majority</td>
<td></td>
</tr>
<tr>
<td>Previous question or call for the question. (To stop debate and force an immediate vote.)</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td>2/3</td>
<td>✓</td>
</tr>
<tr>
<td>Postpone to a definite time.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>Majority</td>
<td>✓</td>
</tr>
<tr>
<td>Commit or refer. (A motion to refer to a smaller committee.)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>Majority</td>
<td>If group has not begun consideration of a question.</td>
</tr>
<tr>
<td>Amend.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>Majority</td>
<td></td>
</tr>
<tr>
<td>Postpone indefinitely.</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>Majority</td>
<td>Affirmative vote only</td>
</tr>
</tbody>
</table>

**Chart C: Main motions.** A main motion is a formal proposal that is made by a member that brings a particular matter before the group for consideration or action.

<table>
<thead>
<tr>
<th>Motion</th>
<th>Requires a second</th>
<th>Can interrupt speaker</th>
<th>Debatable</th>
<th>Amendable</th>
<th>Votes required to pass</th>
<th>Can be reconsidered</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any general motion, resolution, or ordinance.</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>Majority</td>
<td>✓</td>
</tr>
<tr>
<td>Take from the table.</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td>Majority</td>
<td></td>
</tr>
<tr>
<td>Reconsider. (To reconsider a motion already passed/defeated.)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>Majority</td>
<td></td>
</tr>
<tr>
<td>Appeal or challenge a ruling of the chair.</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>Depend</td>
<td>Majority</td>
<td></td>
</tr>
<tr>
<td>Rescind. (A motion to strike out a previously adopted motion, resolution, bylaw, etc.)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>Varies, based on motion</td>
<td>Negative vote only</td>
</tr>
</tbody>
</table>
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

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 responsibly and efficiently. Find model resolutions and forms to help you comply with the law.

This material is provided as general information and is not a substitute for legal advice. Consult your attorney for advice concerning specific situations.
responsibly and efficiently.

**B. Application**

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.

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.”

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.

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:

<table>
<thead>
<tr>
<th>Data On Individuals</th>
<th>Data Not On Individuals</th>
<th>Data On Decedents</th>
<th>Who Has Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public</td>
<td>Public</td>
<td>Public</td>
<td>Anyone</td>
</tr>
<tr>
<td><strong>Not Public</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Private</td>
<td>Nonpublic</td>
<td>Private</td>
<td>Data subjects and government employees and officials with a business need to know.</td>
</tr>
<tr>
<td>Confidential</td>
<td>Protected Nonpublic</td>
<td>Confidential</td>
<td>Only government employees and officials with a business need to know.</td>
</tr>
</tbody>
</table>
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.

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.

A. Data on individuals

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.

1. Public data

“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

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.

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

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.

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**

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.

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

- 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:

- 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.
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.

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

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.

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.

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.

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

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.
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

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

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.
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.

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

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.

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.

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

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.
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

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

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.
- 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.
1. Classifying, maintaining, and securing data

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.

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.

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.

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.

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.

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:

- 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.
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.

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.

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.

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.

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:

- 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.
- 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.
2. **Access to data**

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**

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.

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.
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.

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

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.

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.

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.

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.
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.

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

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.

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

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.
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.

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.

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.

“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.
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.

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.

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**

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.

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.

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.

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.
h. Standing requests

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

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

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

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

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.
V. Rights regarding government data

A. General public

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

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.

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.

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.

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.

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.
1. **Tennessee warning**

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:

- 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.

This notice is commonly referred to as a “Tennessee warning,” named after Sen. Robert Tennessen, the author of the original data privacy law in Minnesota. A Tennessee 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 Tennessee warning on the form itself, or to have the warning on a sheet or card that the data subject may keep.

In situations where a Tennessee 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**

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

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 Tennessee warning.
- If it wants to use not public data in a way that is different than was explained in the Tennessee warning.
- When the data subject wants his or her private data released to another entity or person (e.g., a prospective employer).
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**

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.

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.

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.
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.

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

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:

- 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.

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).

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.”

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).

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.

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.
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

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

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

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

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.

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:
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.

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.

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:

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

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.
See Section VI-E Criminal penalties.

**E. Criminal penalties**

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

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.
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

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

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

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

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).

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

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 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.

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.

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.
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

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.

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)

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.

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.
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.
b. Access to personnel files

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

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.

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

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.
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

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:

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

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.

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

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.
(ii) Pre-employment examinations

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.

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

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.

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

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

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

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**

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.

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

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.

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.

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.
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)

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.

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.”

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.

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.

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.
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**

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.

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.

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.

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**

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:
• 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.

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.

i. **Volunteers**

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**

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).
**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).

**I. 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.
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.

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

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

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.

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

\[ \text{Section VIII-A-2-e} \]

Advisory boards and commissions.
• 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.

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.

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.

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.
#### e. Advisory boards and commissions

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).

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.

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.

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.

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.

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

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.
1. Requestor is not the subject of the data

a. 100 or fewer pages

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

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.

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.

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:
• Costs related to inspection.
• Costs related to verifying the accuracy of data.
• Staff time separating public from not public data.
• Purchase or rental of a copier.
• Maintenance or depreciation of a copier.
• Normal operating expenses (such as electricity).
• Administrative costs not related to copying.
• Records storage (obtaining and returning data to off-site storage facility).
• Sales tax.

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

c. Commercial value

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.

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

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

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.
2. Requestor is the subject of the data

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.

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.

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

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

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

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.
a. **Arrest data**

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:

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

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.
b. Request for service data

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).

DPO 98-008.

DPO 00-078.

See Section VIII-C-5 Protection of identities.

Minn. Stat. § 13.82, subd. 3.

Minn. Stat. § 13.82, subd. 17.

Minn. Stat. § 13.82, subd. 6.

c. Response or incident data

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:

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

Minn. Stat. § 13.82, subd. 17.

DPO 01-050.

Minn. Stat. § 13.82, subd. 17.

DPO 02-040.

Minn. Stat. § 13.82, subd. 17.

DPO 08-006.
(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

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

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

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

The existence of all surveillance technology maintained by a law enforcement agency is public data.
2. **Not public law enforcement data**

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

**a. Child abuse**

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.

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**

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.

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**

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**

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.
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**

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.

An investigation becomes inactive upon any of the following events:

- 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.

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.

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.

### (i) **Images, recordings and photographs**

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.
(ii) Crime victim access

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

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.

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

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

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.
b. 911 calls

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.

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

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:

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

d. Arrest warrant indices

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

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.
f. Pawnshops and scrap metal dealers

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.

DPO 95-003.

Minn. Stat. § 13.82, subd. 27.

Minn. Stat. § 13.82, subd. 25.

Minn. Stat. § 13.82, subd. 16.

DPO 94-054.

DPO 04-031.

Minn. Stat. § 13.82, subd. 7.

Minn. Stat. § 13.82, subd. 17.

4. Access to law enforcement data

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.

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

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:
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).

- A victim (or alleged victim) of criminal sexual conduct.
- 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).
- 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.
- 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).
- A juvenile witness (and the agency reasonably determines that the subject matter of the investigation justifies protecting the identity of the witness).
- A mandated reporter.

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.

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.
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.

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.

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.

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.

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.

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

a. State law

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.

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.

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

b. Federal law

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.

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

Additional safeguards and restrictions for permitted uses are provided for “highly restricted personal data,” which are an individual’s:
• Photograph or image.
• Social Security number.
• Medical or disability information.

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.

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

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.

9. Ambulance records

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.

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.

10. Juvenile data

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:
• 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

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

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.

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

11. Exchanging data

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.
12. Portable recording systems—police-worn body cameras

a. Private data

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:

- 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.”
- 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.

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.

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:

- 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.
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

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.

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.

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

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).
b. Mandatory closed meetings

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

- 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).
- Educational data.*
- Health data.*
- Medical data.*
- Welfare data.*
- Mental health data.*
- An individual’s medical records.*

*Where specifically classified as not public in state statutes.

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

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.
- 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.
2. Minutes and recordings

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

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

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.

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.
E. Property

1. Complaints and violations

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.

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

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

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.
F. Utilities

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

1. Customer data

a. Municipal electric utilities

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.

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

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

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.
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.

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

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.

G. Contact information

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).

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.

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

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.
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.

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**

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.

3. **Recreational programs**

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**

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**

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.
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**

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**

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**

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.
2. **Tennessen warnings**

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**

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.

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**

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.

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

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**

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.

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.

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.

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.
2. **Dissemination**

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.

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.

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**

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.

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.

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**

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.
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**

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**

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**

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**

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**

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:
• 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.

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.

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

M. Licenses

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.

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.

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.
N. Permits

1. Generally

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

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

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

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.
• 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.

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

b. Assistance received

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.

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

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).

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.

“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).

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

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**

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.

“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.

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.

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.

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**

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.
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

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

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.

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

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.
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

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

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

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.

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.
a. Attorney-client privilege

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.

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).

b. Work product

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

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.
1. Discovery

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:

- 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:

- 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.

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.

2. Subpoenas

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.
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
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).

1. Remote locations
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
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).
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.

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.

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

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

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

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).

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

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

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).

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)

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:
• Hospital.
• Nursing home.
• Medical center.
• Clinic.
• Health or nursing agency.

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

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:

• 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

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

a. Legal commitments

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.
b. Patients

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

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

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.

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

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.

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.
• 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.

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

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.

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.

B. Continuing education

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

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.
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.