LEAGUE of MINNESOTA CITIES

HANDBOOK FOR MINNESOTA CITIES

Chapter 26
Records Management

TABLE OF CONTENTS

145 University Ave. West
Saint Paul, MN 55103-2044
www.lmc.org
(651) 281-1200 or (800) 925-1122
8/14/2024

LEAGUE of MINNESOTA CITIES

HANDBOOK FOR MINNESOTA CITIES

Chapter 26
Records Management

Defines public records and outlines records management issues, including creation, retention, and destruction of records, public inspection of records, and the right to privacy. Understand management concepts for electronic records such as email, text messages, and websites. Learn about metadata, security, backups, and disaster recovery.

RELEVANT LINKS:

The records management laws are found at Minn. Stat. § 15.17. Minn. Stat. § 138.163. Minn. Stat. §§ 138.225-.226. Minn. Stat. §§ 13.01-.99.

I. Importance of records management

City records document city business; provide information to public officials; and act as a check on the honesty, integrity, and completeness of official actions. They are a crucial link in the communication chain between city officials and their constituents.

Cities are required by law to maintain a complete and accurate record of all city transactions and affairs. State laws govern the creation, maintenance, and destruction of city records as well as the public's right to access government data. This chapter discusses how those laws relate to cities.

Records management is an important part of city administration. City records document city actions and have historical significance. Failing to properly manage records can have serious consequences for cities. Improperly managed records make it difficult to conduct city business and could result in flawed decision making. Mismanagement of records that causes a failure to respond appropriately to a data practices request can result in administrative, civil, and criminal penalties. The inability to produce relevant records when a city is involved in litigation could result in monetary penalties or even a default judgment against the city. For these reasons, proper management of city records is vital.

In addition to paper records, cities now have the ability to create and store records electronically. Electronic records a city might have include electronically created documents, emails, text messages, and digital photographs, maps, and video and audio recordings. Government records that are created and stored electronically are still government records and laws governing creation, retention, destruction, and public access to paper documents apply equally to electronic records. This chapter discusses electronic records management and contains links to resources to help cities manage electronic records.

RELEVANT LINKS:

II. What is a government record?

Minn. Stat. § 15.17 subd. 1.

Minn. Stat. § 138.17 subd. 1.

See the Minnesota Historical Society State Archives Department's Government Records Information Leaflet No. 4, Municipal Records for a list of historically important municipal records.

A starting point for understanding how to manage government records is to determine what qualifies as a government record. Cities are required by law to "make and preserve all records that are necessary for a full and accurate knowledge of their activities." State law defines government records to include all cards, correspondence, discs, maps, memoranda, microfilms, papers, photographs, recordings, reports, tapes, writings, optical disks, and other data, information, or documentary material made or received by a city official pursuant to state law or in connection with the transaction of public business. Whether the record is created and stored in paper "hard copy" or on a computer or other electronic storage device does not affect its status as a government record.

However, not every document that a city creates is a government record. The definition of government record excludes:

Minn. Stat. § 138.17 subd. 7.

- Information that does not become part of an official transaction.
- Library and museum material made or acquired and kept solely for reference or exhibit purposes.
- Extra copies of documents kept only for convenience of reference and stock of publications and processed documents.

Minn. Stat. § 475.553.

- Bonds, coupons, or other obligations or evidences of indebtedness the destruction or other disposition of which is governed by other laws.

Identifying what does and does not qualify as a government record is the first step for city staff when determining how to manage city records.

III. Who is responsible for managing government records?

Minn. Stat. § 138.17 subd. 7.

Minn. Stat. § 15.17, subd. 2.

Minn. Stat. § 412.151, subd. 1.

Under state law, it is the duty of the city council to establish and maintain an active, continuing program for the economical and efficient management of city records. State law makes the chief administrative officer of each public agency responsible for the preservation and care of government records. The statutory city code and most charters make the city clerk responsible for preserving all city records, except those accounting documents and debt instruments that are kept by the treasurer. Some charters also designate the city manager or chief administrative officer as the officer responsible for managing government records.

Minn. Stat. § 15.17 subd. 3.

When a responsible officer's term of office or authority expires they must deliver all government records in their possession to their successor in office. The successor, in turn, must issue a receipt for all records received, and must file a signed acknowledgment of delivery in the clerk's office.

RELEVANT LINKS:

IV. Creation and retention of records

Minn. Stat. § 15.17, subds. 1, 2.

State law requires all officers and agencies of the state, including statutory and home rule charter cities, to make and preserve all records necessary for a full and accurate knowledge of their official activities. These records include books, papers, letters, contracts, documents, maps, plans, computer-based data and other records made or received pursuant to law or in connection with the transaction of public business.

Minn. Stat. § 15.17, subd.1, 2.

All government records must be kept in a physical medium of a quality that will ensure permanence. The responsible officer must carefully protect and preserve all records from deterioration, mutilation, loss, or destruction and is authorized to make repairs when necessary to preserve them properly. Records may be copied to another format and still retain their authenticity, reliability, and legal admissibility as long as the copies are made in a trustworthy way that clearly and accurately reproduces the records.

Managing Your Government Records: Guidelines for Archives and Agencies. State Archives Department, Minnesota Historical Society.

The State Archives Department of the Minnesota Historical Society has published an educational resource titled *Managing Your Government Records: Guidelines for Archives and Agencies*. The manual is designed to assist local governments and county and local historical societies. It is a comprehensive introduction to basic archival principles and practices.

V. Destruction of records

Some city records have continuing value and must be maintained permanently. For example, minutes of city council meetings have continuing historical value and therefore should be maintained forever. But many documents created or received by city staff do not meet the definition of government records and the vast majority of government records lose their useful value over time. Needlessly maintaining records that no longer have any practical use can result in unnecessary expense for the city in storing and searching through superfluous records. Cities do not have to keep all of their records forever. State law authorizes cities to dispose of government records that are no longer necessary. However, destruction of government records must comply with state law.

DPO 07-006.

A. Records retention schedule

Minn. Stat. § 138.17.

Some city records must be kept permanently, but other records may be destroyed after a certain period of time. State law prescribes the procedure that cities must follow to dispose of government records. Under state law a city may dispose of government records pursuant to an approved records retention schedule.

RELEVANT LINKS:

A records retention schedule is a plan for managing government records. It lists the city's records and the minimum length of time each record should be kept. A records retention schedule gives the city continuing authority to dispose of government records it no longer needs. A records retention schedule applies to the contents of the records regardless of the format (e.g. paper, microfilm, electronic) in which the record is kept.

You can download a copy of the General Records Retention Schedule for Minnesota Cities from the Municipal Clerks and Finance Officers Association of Minnesota web site. A General Records Retention Schedule for Fire Relief Associations is also available for downloading at the Minnesota Historical Society's web site.

A General Records Retention Schedule for Minnesota Cities has been developed by the State Department of Administration's Data Practices Office and the Minnesota Historical Society's Division of Archives and Manuscripts. The General Records Retention Schedule is updated by the Municipal Clerks and Finance Officers Association of Minnesota. The Records Disposition Panel has approved the General Records Retention Schedule for use by cities. A city can begin destroying records in accordance with the General Records Retention Schedule after it adopts the schedule and notifies the State Archives Department of the Minnesota Historical Society that the city has adopted the schedule.

Minn. Stat. § 138.17 subd. 1.

In the alternative to adopting the General Records Retention Schedule for Minnesota Cities, a city could develop its own records retention schedule based upon an inventory of the specific records it maintains. The city must submit its records retention schedule to the Records Disposition Panel for approval. The Records Disposition Panel is a statutorily created body made up of the state attorney general, state auditor, and director of the Minnesota Historical Society. State archives employees may inspect any documents listed on a proposed records retention schedule to determine if they have continuing value and should be retained permanently. The city may only begin disposing of records listed on its records retention schedule after the Records Disposition Panel approves the schedule.

General Records Retention Schedule for Minnesota Cities.
Minn. Stat. § 138.17 subd. 1(b)(4).

The retention period listed in the records retention schedule applies only to the official version of the record regardless of whether the record is maintained in paper, microfilm, or electronic format. Duplicate copies of the official record need not be maintained according to the city's record retention schedule. It is the city's responsibility to identify the official version of the government record.

B. Application for Authority to Dispose of Records (PR-1 form)

The PR-1 form is available at the Minnesota Historical Society web site.

A city may not destroy government records that are not listed on a records retention schedule without specific authorization from the Records Disposition Panel.

RELEVANT LINKS:

However, if the city has records that are not on a records retention schedule and if the records are no longer being created and are no longer of any use to the city, the city may destroy the records after submitting an Application for Authority to Dispose of Records (PR-1form) and obtaining approval from the Records Disposition Panel. Approval of the PR-1 form gives the city approval to dispose of only those records listed on the form.

If the city is still creating records that are not listed on its records retention schedule, it should seek approval from the Records Disposition Panel to add those records to its retention schedule. This will give the city continuing authority to dispose of the records.

C. Destruction of government records must comply with the Minnesota Government Data Practices Act

Minn. Stat. § 138.17 subd. 7.

City records classified under the Minnesota Government Data Practices Act or other law as not public must be destroyed in a way that prevents their contents from becoming known.

D. Transfer of records to Minnesota Historical Society State Archives

Minn. Stat. § 138.17, subds. 1a, 1b, and 1c.
Preserving and Disposing of Government Records. Minnesota Historical Society, State Archives Department.

The General Records Retention Schedule for Minnesota Cities identifies records that have permanent historical value. If a city does not wish to continue to store these archival records, it may transfer them to the Minnesota Historical Society's State Archives or, if approved by the Records Disposition Panel, to local or county historical societies.

Minn. Stat. § 138.17 subd. 1b.

Minn. Stat. § 138.17 subd. 1c.

The city transferring the records to the State Archives must notify the archivist of the Minnesota Government Data Practices Act classification of the records transferred. State law allows public access to state archive records unless the archivist determines special circumstances exist requiring limited access.

E. Penalty for improperly disposing of government records

Minn. Stat. § 138.225.

Cities may only dispose of government records by following the procedure prescribed by state law. Government records may not be destroyed except pursuant to an approved records retention schedule or PR-1 form. It is a crime to destroy government records except by the authority provided for in state statute.

RELEVANT LINKS:

Preserving and Disposing of Government Records. Minnesota Historical Society, State Archives Department.

F. Additional resources

The Minnesota Historical Society State Archives Department's *Preserving and Disposing of Government Records* has information on how to identify records, assess their value, properly store them, determine how long to keep them, and how to destroy them. It provides a general overview of state and local governmental entities' records-management responsibilities.

Municipal Clerks and Finance Officers Association of Minnesota: Model Disaster Recovery Plan for Vital Records.

The Municipal Clerks and Finance Officers Association of Minnesota has prepared a *Model Disaster Recovery Plan for Vital Records* that explains how to prevent the destruction of government records in case of disasters, such as fire or water damage. Cities can tailor the plan to their individual needs.

VI. Public access to city records

Minn. Stat. Ch. 13. For more information, see LMC information memo, *Data Practices: Analyze, Classify and Respond.* Concerning personnel data, see LMC information memo, *Management of Personnel Files.*

Public access to government records is governed by the Minnesota Government Data Practices Act (MGDPA). The MGDPA governs when and how the public may access government records. Every city in Minnesota must comply with the MGDPA, which in conjunction with other state and federal laws, classifies all government data. Government data are classified in different categories, which determine who may have access to the data.

A. Government Data

Minn. Stat. § 13.02 subd. 7.

Minn. R. 1205.0200 subp. 4.

Under the MGDPA "government data" is defined as all data collected, created, received, maintained, or disseminated by the city regardless of its physical form, storage media or conditions of use. Data regulated by the MGDPA includes not only paper documents but also electronic documents, e-mails, spreadsheets, photographs, charts, maps, videotapes, audio tapes, and handwritten notes and working documents.

Note that the definition of "government data" is broader than the definition of "government record" under the Government Records Act because it includes all data even if it is not part of an official transaction. So, for example, while the draft minutes of a city council meeting are not a government record under the Government Records Act, the draft minutes are government data under the MGDPA. There is a presumption that government data are public and are accessible by the public for inspection and copying unless there is a federal law, state statute, or temporary classification of data that provides differently.

RELEVANT LINKS:

B. Classification of government data under the MGDPA

The MGDPA classifies government data as: (1) public, (2) private, (3) confidential, (4) nonpublic, or (5) protected nonpublic. The data's classification under the MGDPA determines who may access it.

Minn. Stat. § 13.02 subd. 14, 15.
Minn. R. 1205.0300 subp. 2.
Minn. Stat. § 13.02 subd. 12.
Minn. R. 1205.0400 subp. 2.

- Public data are accessible to any person, without regard to the nature of that person's interest in the data.
- Private data are not accessible by the public but are accessible by the individual subject of the data and city staff whose work assignments reasonably require access. Private data is also accessible by outside entities or agencies that are authorized by state or federal law to access the data and by entities or individuals given access by the express written approval of the data subject.

Minn. Stat. § 13.02 subd. 3.
Minn. R. 1205.0600 subp. 2.

- Confidential data are not accessible by the public and are not accessible by the individual subject of the data. Confidential data are accessible to city staff whose work assignments reasonably require access and outside entities and agencies authorized by state or federal law to access the data.

Minn. Stat. § 13.02 subd. 9.

- Nonpublic data is data that is not on an individual that is not accessible to the public. Nonpublic data is accessible by the subject, if any, of the data.

Minn. Stat. § 13.02 subd. 13.

- Protected nonpublic data is data that is not on an individual that is not accessible to the public or to the subject of the data.

C. Responsible Authority

Minn. Stat. § 13.02, subd 16.
Minn. Stat. § 13.03, subd. 2.
Minn. Stat. § 13.025.
Minn. Stat. § 13.05.
See LMC information memo, *Data Practices: Analyze, Classify, Respond* and its model resolution "Appointing a Responsible Authority and Assigning Duties."

The MGDPA requires every city to appoint a specific person as its responsible authority. If the city has not appointed a responsible authority, the MGDPA provides that the city clerk is the responsible authority until the city designates another individual. The appointment of the responsible authority should be made by resolution and must confer full administrative authority on the individual to carry out the duties imposed by the MGDPA.

The MGDPA makes the responsible authority responsible for the collection, use, and dissemination of any governmental data. The responsible authority must review and identify all types of data maintained by the city, determine what data are private or confidential, and keep records containing government data in such an arrangement and condition so they are easily accessible for convenient use. The responsible authority must also prepare written policies for access to government data.

RELEVANT LINKS:

Minn. Stat. § 13.03 subd. 2.

A responsible authority may designate one or more designees to assist in administering the MGDPA. A designee must be a city employee and the designation must be made in writing. The responsible authority must post a notice of, or make available to the public, a document identifying the name of the responsible authority and any designees.

D. Compliance Official

Minn. Stat. § 13.05, subd. 13.

Each responsible authority is required to designate an employee to act as the data practices compliance official. This official is responsible for responding to questions or concerns from persons who are attempting to access data or enforce their rights under the MGDPA. The data practices compliance official may be the same person as the responsible authority or another city employee.

E. Public access procedures

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

Sample Data Access Policy for Members of the Public.

Sample Data Access Policy for Data Subjects.

Worksheet for Developing Data Access Policies.

Cities are required to adopt written procedures for public access to government data. Cities must make copies of their public access procedures easily available to the public through free distribution or posting. The Department of Administration's Data Practices Office has published sample public access policies that cities can adopt in order to comply with this requirement. The procedures must be updated annually by August 1 and as needed to reflect changes in city personnel or data. Also, because the state legislature has historically amended the MGDPA every session, cities should review and possibly amend their public access procedures after each legislative session.

F. Ensuring the security of not public data.

Minn. Stat. § 13.05, subd. 5. Policy for ensuring the security of not public data.

Cities must adopt a policy with procedures for ensuring that not public data is only accessible to persons whose work assignments reasonably require access to the data and is only accessed for work purposes.

Minn. Stat. § 13.09.

Intentional unauthorized access of not public data is a misdemeanor and constitutes just cause to suspend without pay or dismiss a public employee.

G. Data breaches

Minn. Stat. § 13.055.

A data breach occurs when data maintained by a city is accessed by a person who is not authorized to access the data and the access compromises the security and classification of the data. Cities must provide written notification to any individual whose private or confidential data is subject of a data breach.

RELEVANT LINKS:

Cities must also investigate data breaches and prepare a report on the facts and results of the investigation.

H. Data requests

Minn. Stat. § 13.03, subd. 3.

Minn. Stat. § 13.05, subd. 12.

Data practices requests should be directed to the responsible authority. The responsible authority must provide any person access to public data without regard to the nature of the person's interest in the data. Cities may not require individuals to identify themselves or explain or justify a request for access to public data unless specifically authorized to do so by statute. However, cities may ask individuals to provide information about themselves or the information they are seeking for the sole purpose of facilitating a response to the data request.

Minn. Stat. § 13.03, subd. 3.

The responsible authority must allow any person to inspect and copy city records at reasonable times and places. Information on the meaning of the data should be provided if requested. Unless ordered by a court, public officials should not permit original copies of records to leave their possession.

Minn. Stat. § 13.43.

Unless a statute or an advisory opinion specifically classifies data as private or confidential, all city records—including assessment and tax records—and all other information or data must be open to public inspection. There is only one general exception: personnel data not explicitly made public is private but may be released pursuant to a court order.

Minn. Stat. § 13.04.

Schwanke v. Dept. of Administration, 851 N.W.2d 591 (Minn. 2014).

Subjects of data have the right to know what data are maintained about them and how the data are classified. They have the right to view all such public and private data, to have it explained, to receive copies of the data, and to challenge its accuracy and completeness. If their challenge results in an adverse decision, they can appeal to the commissioner of the Department of Administration.

I. Denial of access to government data

Minn. Stat. § 13.03, subd. 3.

If the responsible authority determines that requested data are not classified as public, access by individuals that are not the subject of the data must be denied. If the responsible authority determines that access to data must be denied, he or she must cite the specific statutory section, temporary classification, or specific provision of law on which the determination is based. The requesting party may request this information in writing.

RELEVANT LINKS:

J. Electronic data

Minn. Stat. § 13.03, subd. 3.

Cities that maintain public data in a computer-storage medium are required to provide copies, upon request, in electronic form if copies can be reasonably made. There is no obligation to provide the data in an electronic format or program different than that used by the city.

Minn. Stat. § 13.825, subd. 2(a). See LMC information memo, *Data Practices: Analyze, Classify and Respond*: Portable Recording Systems—Police-Worn Body Cameras.

Generally, body camera video and audio are private data if it involves individuals and, otherwise, it is generally nonpublic data. Body camera data that is part of active criminal investigative data is generally confidential. There are several notable exceptions to this presumption.

K. Inspection of data and copying costs

Minn. Stat. § 13.03 subd. 3.
Minn. Stat. § 13.04 subd. 3.
Minn. R. 1205.0400, subp. 5.

Cities may not charge a fee for allowing visual inspection of data. The responsible authority may charge for copies of records. If 100 or fewer pages of black and white, letter or legal-size paper copies are requested, cities may not charge more than 25 cents for each page copied. In other instances, the responsible authority can charge the actual costs of searching for, retrieving, and making copies of the requested data. This can include the cost of labor in making the copies. The city must be able to demonstrate the charges are appropriate.

Minn. Stat. § 13.03 subd. 3.
Minn. R. 1205.0400, subp. 5.
See also DPO 96-014 (Mar. 29, 1996) and DPO 96-037 (Aug. 14, 1996).

Minn. R. 1205.0300.

View the Minnesota Department of Administration Data Practices Office's informational video on copying costs.

When determining what is a reasonable fee for copies, the city may consider:

- The cost of materials, including paper, used to provide the copies.
- The cost of the labor required to prepare the copies.
- Any schedule of standard copying charges established by the agency in its normal course of operations.
- Any special costs necessary to produce such copies from machine-based recordkeeping systems, including but not limited to computers and microfilm systems; and mailing costs.

Minn. Stat. § 13.03 subd. 3.

Cities cannot charge for separating public data from not public data. If the city is not able to provide copies at the time of request, it must supply them as soon as reasonably possible.

L. The attorney-client privilege

Minn. Stat. § 13.393.

While most data are presumed public under the MGDPA, the Act makes an exception for data covered by the attorney-client privilege. The MGDPA does not expand or narrow the availability of the attorney-client privilege, but it does incorporate existing law to define its scope.

RELEVANT LINKS:

Courts strictly construe the attorney-client privilege because it is invoked to exclude evidence and testimony and tends to suppress relevant facts. Therefore, cities should have clear justification when asserting that the attorney-client privilege bars access to data.

M. Private data and the Open Meeting Law

Minn. Stat. § 13D.05.

The open meeting law generally prohibits the closing of a meeting solely to discuss private data, except in limited circumstances clearly listed in the statute, and provides that private data may be discussed openly at any public meeting without fear of liability or penalty as long as the release of the data is reasonably necessary to conduct the business the data relates to.

If private data must be discussed at a public meeting, it is recommended that the city be discrete and try to protect the private data by assigning numbers, letters, or similar designations to it and then use those designations instead of the actual data during deliberations. This procedure is not required by state law, but nothing prevents the city from protecting private data in this manner.

See the discussion on the Open Meeting Law in Handbook, *Meetings, Motions, Resolutions and Ordinances.*
See also Minn. Stat. § 13D.05, subds. 2(a) and 2(b).

There are some important limitations on the discussion of private data at a public meeting. For example, the council must close a meeting to consider preliminary allegations or charges against an individual subject to its authority, unless the individual requests the meeting be open. The council also must close a meeting if certain specific data listed in state statute is discussed. For example, a meeting must be closed if data that would identify alleged victims of domestic abuse is discussed.

N. Advisory opinions

Minn. Stat. § 13.072.

Cities may request advisory opinions from the commissioner of the Department of Administration on any question concerning public access to government data, rights of subjects of data, or classification of data. Advisory opinions are not binding, but a court must give deference to an advisory opinion when a dispute involves data that was subject of an advisory opinion.

To request an advisory opinion, write to the Commissioner of Administration, c/o Data Practices Office.

Cities that act in conformity with a data practices advisory opinion will not be liable for compensatory or exemplary damages, awards of attorney fees, or penalties. However, penalties can be more severe, if a city fails to act in conformity with an advisory opinion directed to it. Cities interested in requesting an advisory opinion can contact the Department of Administration, Data Practices Office.

Index to Advisory Opinions of the Commissioner of Administration under Minn. Stat. § 13.072.

The Department of Administration maintains an index to advisory opinions on its web site.

RELEVANT LINKS:

O. Violations of the MGDPA

Actions arising under the MGDPA can be brought before the State Office of Administrative Hearings or filed in district court.

1. Administrative penalties

Minn. Stat. § 13.085, subd. 2.

A person who believes their rights under the MGDPA have been violated may seek to compel compliance with the MGDPA and administrative penalties through the State Office of Administrative Hearings. An action to compel compliance with the MGDPA through the administrative process must be filed with the Office of Administrative Hearings within two years after the occurrence of the act or failure to act that is the subject of the complaint, except that if the act or failure to act involves concealment or misrepresentation by the government entity that could not be discovered during that period, the complaint may be filed with the office within one year after the concealment or misrepresentation is discovered.

The Office of Administrative Hearings must forward a copy of the complaint to the responsible authority of the city that is the subject of the complaint. The city must file a response to the complaint within 15 business days of receipt by the city of notice of the complaint.

Minn. Stat. § 13.085 subd. 5.

Minn. Stat. § 13.085 subd. 6.

If an administrative law judge determines that a violation of the MGDPA occurred, the penalties that could be imposed include a $300 fine, an order compelling the city to comply with the provision of the MGDPA that was violated and referring the matter to the appropriate prosecuting authority for criminal charges. A prevailing complainant is also entitled to reasonable attorney fees not to exceed $5,000. The administrative law judge may deny the award of attorney fees if the judge determines that the violation of the MGDPA was merely technical or the meaning of the governing law was unclear.

2. Civil actions

See *Washington v. Indep. Sch. Dist. No. 625*, 610 N.W.2d 347 (Minn. Ct. App. 2000) (discussing the right of a data subject to see his or her personnel records).

A person may bring a lawsuit in district court to enforce their rights under the MGDPA. Lawsuits may be brought under the MGDPA to recover damages caused by violation of the MGDPA, to prevent violations of the MGDPA, and to compel compliance with the MGDPA. An unauthorized disclosure of data that is classified as private or confidential might also give rise to a lawsuit claiming an invasion of privacy.

RELEVANT LINKS:

a. Actions for civil damages

Minn. Stat. § 13.08. *Navarre v. South Washington County Sch.,* 652 N.W.2d 9 (Minn. 2002).

Any person who is damaged by a violation of the MGDPA may bring a lawsuit against the government entity that violated the Act. A court may award civil damages to a person who is damaged by a violation of the MGDPA. A city that violates any provision of the MGDPA is liable for any damage resulting from the violation. The damaged person may also be entitled to recover court costs and attorney fees expended in bringing the lawsuit. In addition, civil penalties of not less than $1,000 and not more than $15,000 are available for a willful release of private and confidential data and for a willful refusal to release public data.

Freier v. Indep. Sch. Dist. No. 197, 356 N.W.2d 724 (Minn. Ct. App. 1984).

Johnson v. Dirkswager, 315 N.W.2d 215 (1982). *Mooers v. City of Lake City*, No. A13-2197, 2014 WL 3023368 (Minn. Ct. App. 2014) (unpublished opinion).

However, Minnesota appellate courts have ruled that if a city council publishes or releases defamatory matter under the requirements of the MGDPA, there will be no civil liability.

b. Actions to enjoin violation of the MGDPA

Minn. Stat. § 13.08 subd. 2.

Any person may bring a lawsuit to enjoin or prevent a violation of the MGDPA. The court may grant an injunction against a city that violates or proposes to violate the MGDPA. The court may make any order necessary to prevent any practice that violates the MGDPA.

c. Actions to compel compliance with the MGDPA

Minn. Stat. § 13.08, subds. 4. *Quade & Sons Refrigeration, Inc. v. Minn. Mining & Mfg. Co.,* 510 N.W.2d 256 (Minn. Ct. App. 1994). *Baldwin v. Indep. Sch. Dist. No. 2687*, C3-98-92 (Minn. Ct. App. July 14, 1998) (unpublished opinion). *Wiegel v. City of St. Paul,* 639 N.W.2d 378 (Minn. 2002). Minn. Stat. § 13.08, subd. 4 (c).

Any person may also bring a lawsuit against a city to compel compliance with the MGDPA. Court costs and attorney fees are recoverable in an action to compel compliance with the MGDPA. The district court generally has discretion to determine whether the prevailing party in an action to compel compliance is entitled to costs and reasonable disbursements, including attorney fees. However, an award of attorney fees is mandatory to a prevailing plaintiff in an action to compel compliance if the city was the subject of a data practices advisory opinion that was directly related to the cause of action being litigated and the city did not act in conformity with the opinion. If the court issues an order compelling a city to comply with the MGDPA, it may also impose a $1,000 civil penalty.

d. Violation of right to privacy

Lake v. Wal-Mart Stores, Inc., 582 N.W.2d 231 (Minn. 1998).

Release of data on individuals classified as private or confidential may not only result in a lawsuit alleging violation of the MGDPA, it may also result in a lawsuit claiming violation of an individual's right to privacy.

RELEVANT LINKS:

Kampschroer v. Anoka Cty., 57 F. Supp. 3d 1124 (D. Minn. 2014), aff'd, No. 14-3527, 2016 WL 4547351 (8th Cir. 2016).

A release of private or confidential government data could result in a claim that the city improperly provided access to private facts about an individual. To establish a claim for publication of private facts, a plaintiff must show the release of the information is highly offensive to a reasonable person and is not of legitimate concern to the public.

e. Statute of limitations on actions

Minn. Stat. § 541.05, subd. 1(2).
Manteuffel v. City of N. St. Paul, 570 N.W.2d 807 (Minn. Ct. App. 1997).

Although the MGDPA does not specify a limitations period, courts have determined the applicable limitations period is six years from the date of the violation.

VII. Electronic records

Electronic communication has become commonplace.

The ability to communicate through electronically created documents, emails, text messages, and web sites has many advantages. Consequently, cities are conducting more and more of their business electronically and, as a result, there has been a significant increase in the amount of records stored electronically. In fact, some official government records now only exist in digital form.

The ease and speed with which electronic documents can be created and transmitted means that in the future more and more official city business will be done electronically and increasing numbers of electronic documents will be created.

However, electronically created government records also pose significant recordkeeping challenges for cities. Cities have been managing paper documents for many years and have strategies for filing paper documents. However, electronic records are a relatively new technology and pose new recordkeeping challenges. If electronic records are not managed properly, useful information may be lost making it impossible to determine what has transpired. Therefore, it is vitally important that cities appropriately manage electronic records.

A. What is an electronic record?

An electronic record is a document or image that is created or stored on a computer or other electronic device. Emails, text messages, web pages, digital images, databases, spreadsheets, and word-processing documents are electronic records.

RELEVANT LINKS:

B. Applicable law

1. Records Management

Minn. Stat. § 15.17 subd. 1.

Government records may be kept in the form of computerized records. The same state laws that govern creation, retention, destruction, and access to paper government records govern management of electronic records as well. Cities have the same duties to maintain government records in electronic format as they do with paper records, including following the city's records retention schedule when disposing of electronic government records and complying with the Minnesota Government Data Practices Act.

2. Uniform Electronic Transactions Act (UETA)

The purpose of the Uniform Electronic Transactions Act (UETA) is to promote the use of electronic documents in business and government. It provides that electronic documents and signatures are equivalent to paper documents and signatures.

Minn. Stat. Ch. 325L.
Minn. Stat. § 325L.02 (p).

The UETA applies to all electronic transactions, which are defined by law as an action or set of actions occurring between two or more persons relating to the conduct of business, commercial, or governmental affairs.

Minn. Stat. § 325L.07.

Minn. Stat. § 325L.02 (m).
Minn. Stat. § 325L.07.
Minn. Stat. § 325L.13.

The UETA provides that if a record is required to be in writing, an electronic record satisfies the law. The UETA broadly defines a "record" as "information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form." Under the UETA if the law requires a signature, an electronic signature satisfies the law. An electronic record or signature may not be excluded from evidence in a legal proceeding merely because it is in electronic form.

Minn. Stat. § 325L.18.

With certain exceptions as to types of records, the UETA provides that each city must determine for itself whether and to what extent it will send and accept electronic records and electronic signatures to and from other persons and otherwise create, generate, communicate, store, process, use, and rely upon electronic records and electronic signatures.

Minn. Stat. § 325L.12.

Minn. Stat. § 325L.17.

If a law requires that a record be retained, the UETA provides that the requirement is satisfied by retaining an electronic record of the information that is accurate and accessible for later reference. The UETA leaves it up to each individual city to determine whether and to what extent it will create and retain electronic records, as opposed to paper records, and to what extent it will convert written records to electronic records.

RELEVANT LINKS:

C. Managing electronic records

The development of electronic records has a significant impact on cities. While the ability to create and store records electronically has obvious benefits, it has also resulted in a massive increase in the volume of records. Therefore, it is more important than ever for cities to have an effective records management strategy.

1. Why is it important to have a strategy for managing electronic records?

It is important to have an effective strategy for managing electronic records because electronic records have certain unique characteristics that make them difficult to manage.

a. Easy creation

Electronic records are easy to create. For example, emails are more conversational and less formal than a traditional paper letter. Also, one email can easily be sent to many recipients.

The recipients may all respond to the first email, exponentially increasing the number of electronic documents created. As a result, cities are creating and storing prolific amounts of electronic documents. Having vast amounts of electronic documents on hand can make it difficult to search for and retrieve electronic records.

b. Multiple storage locations

Electronic records can be stored in many different places, including desktop computers, laptops, servers, flash drives, personal digital devices, cell phones, and disaster recovery backups. Electronic records may even be stored on city officials' or employees' personal computers or storage devices. Consequently, the city may not know where electronic records are stored or if they even exist. Electronic information can be difficult to manage because it can be created and stored in so many different locations.

c. Records not easily destroyed

Electronic records are not easily destroyed. Hitting delete does not always mean records have been deleted. You might delete an email from your inbox, but the email may still exist in several other places, including other recipients' computers, servers, and disaster recovery backups.

RELEVANT LINKS:

These records could remain long after city staff believes they have been destroyed which could create problems for the city when responding to a data practices request or document request during litigation because the city does not know it still has the records.

2. Electronic records management strategy

For more information on managing electronic records see the Minnesota Historical Society State Archives Department's Electronic Records Management Guidelines.

The goal of an effective records management strategy is to maintain records that are trustworthy, complete, accessible, and durable. Records should be kept in a way that ensures that they are reliable and have all of the information necessary to ensure they remain useful. Staff should be able to retrieve records promptly and records should be retrievable throughout their entire useful life.

The following are guidelines for an effective records management strategy:

a. Establish a records management team.

Effective electronic records management requires knowledge of how city records are created and the content of those records, legal recordkeeping requirements, and the city's computer system. It also requires training employees about the city's record management policy and enforcing the policy.

Since it is unlikely that any one person at the city is an expert in all of these areas, departments need to work together to create an electronic records management team. If possible, the electronic records management team should include representatives from:

- The Information Technology department for expertise with the city's computer system.
- The City Attorney's office for expertise in the law pertaining to record management.
- Administration for knowledge of city records and the financial and personnel resources available for records management, and to train employees and enforce the city's record management policies.
- Human Resources for knowledge of city records and to train employees and enforce the city's record management policies.

The records management team can assess the city's records, its record keeping needs, and the city's technology resources to develop an effective strategy for managing its electronic records.

RELEVANT LINKS:

b. Have a common file naming system.

The city should agree on a common naming system for files, especially those on a network's shared directory. Designations used in the city's approved records retention schedule are good models.

c. Establish folders and directories dedicated to recordkeeping.

Folders and directories dedicated to recordkeeping should be established. Not all of a city's digital documents will become official records, but those digital documents that are government records are more easily managed if they are in separate files. The author or the city must make the determination of which documents are government records. The computer cannot make that decision.

d. Maintain identifying metadata.

Metadata is data that describes data, such as the title, date, author, and data-privacy classification of a document. Identifying metadata should be attached to electronic records. Metadata makes it possible to search for, identify, and retrieve electronic records.

e. Train employees.

All employees should be trained on how the city's electronic recordkeeping system works.

Training should include metadata standards and requirements that will allow others to continue to protect and preserve the records after staffing changes.

f. Back up records.

Cities should back up their computer system. Backup media should be stored at a secure, climate controlled, off-site location. Backups are for system recovery only. Their purpose is to back up the city's system in the event of a catastrophe. They are not designed to be searchable. For this reason, backup copies should not be used as the city's archives nor should they be used for recordkeeping copies.

g. Follow record retention schedule.

If the city maintains government records in electronic format those records should be included on the city's records retention schedule.

RELEVANT LINKS:

This will allow the city to dispose of the records when they have exceeded their useful life. Electronic records should be disposed of when their retention requirements have been satisfied. For permanent records, final disposition may mean that some electronic records will have to be converted to an archival storage medium such as paper or microfilm for historical preservation.

h. Technology and cost considerations in maintaining electronic records

Electronic Records Management Guidelines, Minnesota Historical Society, State Archives.

It is relatively easy to retrieve and view current electronic records. However, it may become more difficult to retrieve records as time passes, computer software is updated, and hardware is replaced. It is important for cities interested in maintaining permanent records electronically to consider that as technology advances, hardware and software become obsolete. Software may be discontinued, and newer versions may not allow viewing records created on older versions. Cities may have to convert records to a different file format or migrate records from one storage medium to another. The cost of converting or migrating records could be substantial and should be considered when developing a records management strategy that involves maintaining permanent government records electronically.

D. Specific technologies

Cities use various technologies to create and communicate electronic data. Cities should carefully consider how these technologies impact record management.

1. Email

DPO 01-075.
DPO 10-023.
DPO 11-006.

Email is now a standard form of communication for city employees. Whether city emails are accessible to the public is governed by the Minnesota Government Data Practices Act. Under the MGDPA the content of the email—not its electronic format—determines whether it is classified as public or not public.

Confusion persists about whether city employees need to retain emails. Whether to retain an email depends on the information contained in the email not upon the electronic format of the communication. Some emails may contain information that qualifies as an official government record. These emails and any attached electronic documents should be kept in accordance with the city's records retention schedule. For example, an email from a citizen to the city clerk complaining about junk on a neighbor's property is a government record.

RELEVANT LINKS:

Pursuant to the General Records Retention Schedule for Minnesota Cities, it must be maintained for 7 years.

However, the subject matter of most city emails does not qualify as a government record. For example, an email from a department head requesting an administrative assistant to complete a routine task, or an email asking whether anyone wants to go out to lunch would generally not qualify as official government records. These transitory or personal emails should generally be deleted when they are no longer needed. Also, duplicate copies generally do not qualify as official government records. Emails that do not qualify as government records do not need to be retained according to a record retention schedule.

There are good reasons to dispose of emails and other electronic documents when they are no longer needed. For one thing, superfluous emails take up memory and affect the efficient operation of city computers. More importantly, even though the emails are not government records, they are still considered data under the Minnesota Government Data Practices Act and would have to be produced in response to a data practices request. Moreover, as emails accumulate on the city's computer system, searching for emails responsive to a document request can be like searching for a needle in a haystack. Accordingly, non-official email should be deleted on a regular basis.

2. Text messages

If city employees or officials use text messages for official government business, their text messages may be government records. If text messages qualify as government records they are subject to records management laws. Text messages are also government data and subject to the Minnesota Government Data Practices Act.

Therefore, cities need to carefully think about and address city officers' and employees' use of text messages to conduct official business.

3. City website

Electronic Records Management Guidelines, Minnesota Historical Society, State Archives.

DPO 08-024.

Many cities have created websites where they post information for the public. Cities use their websites to post meeting notices, minutes of city council meetings, city financial information, employment opportunities, news, information about the community, current events, the city code, city permit applications, contact information, and other resources. Additionally, some city websites receive information from members of the public. Information posted or received on the city's website may qualify as a government record and needs to be managed accordingly.

RELEVANT LINKS:

Cities should think carefully about the information they are posting and receiving on the city website to determine whether it is being managed in compliance with the city's record retention schedule and the Minnesota Government Data Practices Act.

E. Information created and stored on city officials' and employees' home computers

DPO 95-008.
DPO 12-019.

City officials and employees might create and store city information on their home computers or personal laptops. If the information qualifies as a government record, it should be maintained in accordance with the city's records retention schedule. Even if the information does not qualify as an official government record, it may still be government data under the Minnesota Government Data Practices Act and may be subject to a data practices request. If the city becomes involved in litigation, city officials' and employees' personal computers that have been used to create and store government data may become subject to a court order requiring forensic examination of the computer for information relevant to the lawsuit. Cities should therefore have policies in place to address what devices may be used to create and store city information.

F. Computer use policy

Computer Use, LMC Model Policy.
LMC information memo, *Computer and Network Loss Control*.

Having a computer use policy promotes electronic records management. A computer use policy should direct city staff to where electronic records should be stored which will make it easier to find and retrieve electronic records.

A computer use policy should also notify employees that electronic documents are subject to the city's records retention schedule and the Minnesota Government Data Practices Act to the same extent as paper documents.

A computer use policy can help protect the city's electronic records by keeping the city's computers and computer network secure against viruses, malware, and other threats. It can do this by:

- Identifying who can access city computers.
- Identifying how city technology can be used.
- Identifying when software can be downloaded from the internet or installed on city computers.
- Setting conditions for when an employee's own peripheral tools, like personal laptops, cell phones, tablets, or flash drives may be connected to the city's system.

RELEVANT LINKS:

- Instituting the use of complex passwords, that is passwords that are at least 8 characters long and include both lower- and upper-case characters and at least one non-alpha numeric character (e.g. #, *, % etc.). For example: M!nn&s0ta. When possible, passwords should be forced to expire or require users to change them at defined intervals (e.g. 45, 60, or 90 days).

A city's computer use policy should inform officials and employees about appropriate use of city computers. City computers should not be used to access inappropriate websites or send inappropriate emails. The city's policy should make clear that files and communications on city computers are not private and may be monitored.

A computer use policy should inform employees who they should contact if they have questions about managing electronic records. These questions might include whether an electronic document is a government record, whether an electronic record is public or private under the Minnesota Government Data Practices Act, where and in what format electronic records should be stored, and what the retention period is for an electronic record. A computer use policy should also inform employees who to contact if they have computer problems.

Because technology changes rapidly, the city's computer use policy will need to be reviewed and updated more frequently than other policies.

G. Electronic record security

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

Security has always been an important aspect of records management. However, in the computer age there is more to security than simply locking doors and file cabinets. Computer hackers, viruses, malware or a lost or stolen laptop can compromise a city's record security and release sensitive information. Measures cities should take to maintain the security of their electronically stored records include:

- Keeping an accurate inventory of all computers, servers, and other networked devices.
- Installing a network firewall.
- Installing anti-virus software on every computer.
- Requiring complex passwords (as described above).
- Setting up laptops to encrypt data on the hard drive to prevent thieves from viewing the data contained on it.

RELEVANT LINKS:

- Designing the city's network with file location and security for specific types of documents.
- Implementing a computer use policy with provisions for network security.
- Training employees so that they understand the city's computer use policy, password setup, and where to store data.
- Scrubbing old computer, laptop, tablet, smartphone, and copier hard drives to Department of Defense standards before disposal.

Guidelines for Media Sanitation.

Trustworthy Information Systems Handbook, Minnesota Historical Society State Archives.

The Minnesota Historical Society State Archives Department's *Trustworthy Information Systems Handbook* is a resource cities can use to help ensure that their recordkeeping systems are secure and reliable.

H. Disaster recovery back up

Cities should back up electronic data to protect against loss because of a natural disaster, failed hardware, viruses, hacker attacks, or other disaster. Backup media should be stored at a secure, off-site, climate-controlled location. Backups will enable the city to restore its computer system in the event of a catastrophic loss.

One option for cities is to use the services of an off-site or cloud backup provider to back up electronic records. If a city is considering this option, it should make sure that the off-site backup provider has adequate security. And that the backups will be maintained according to the city's record retention schedule. It is also a good idea to confirm that data will only be stored in data centers located in the United States.

DPO 00-019.

Information stored on backup media is subject to the Minnesota Government Data Practices Act. This means that a city may be required to produce the data in response to a data practices request. A court could also order a city involved in litigation to search through and retrieve data maintained on disaster recovery backups. This could be a very costly and time-consuming endeavor.

This may not apply to inactive data contained in system backups. A record that has reached the end of its retention period and has been properly destroyed from its official storage location pursuant to a records retention schedule, is not being actively maintained by the entity according to the Data Practices Office.

Given the lack of clarity in the law regarding electronic record-keeping practices, cities should review their backup schedule to ensure there is not a large disparity in the data they are actively maintaining and the data in backups.

RELEVANT LINKS:

The purpose of backups is to enable the city to restore its system in case of disaster. They are generally not a good way to archive information because they are not easily searchable and are expensive to restore.

Therefore, system backups should not be used as the city's records archive and backups should not be retained longer than necessary for disaster recovery purposes.

I. Training

It is important for city employees to receive training on how to protect and manage the city's electronic records.

City employees should understand the city's computer use policy, including the creation of secure passwords. City employees should also understand where electronic data should be stored and their responsibilities with respect to creating, managing, and disposing of electronic records.

Additionally, city employees should understand their responsibilities under the Minnesota Government Data Practices Act.

J. Consequences for failing to properly manage electronic records

See Part VI- N, *Advisory opinions.*

The consequences for failing to properly manage electronic records can be severe. Failure to properly respond to a Minnesota Government Data Practices Act request can result in an action for administrative penalties or a civil lawsuit seeking monetary damages.

Learning Care Grp., Inc. v. Armetta, 315 F.R.D. 433 (D. Conn. 2016).

There can also be severe penalties for a city that destroys or loses records that are relevant evidence in a lawsuit. A party that destroys or loses evidence relevant to a threatened or pending lawsuit could be subject to court imposed sanctions, which could include:

- Requiring the city to pay for computer forensic examination of its computers. The cost of this work could be hundreds of thousands of dollars.
- Instructing the jury at trial to presume that the missing record hurts the city's case.
- Precluding the city from putting favorable evidence before the jury.
- Monetary sanctions.
- Default judgment. Ordering judgment against the city without providing the city with an opportunity to make its case at trial.

These severe consequences underscore the importance of proper electronic records management.