CITY OF WINONA
GUIDELINES AND PROCEDURES
FOR THE
MINNESOTA GOVERNMENT DATA PRACTICES ACT
UPDATED JANUARY 2022

TABLE OF CONTENTS

INTRODUCTION

The Minnesota Government Data Practices Act (MGDPA) gives members of the public the right to see and have copies of public data that the City keeps. The law also controls how the City keeps government data and what the City tells the public when they ask to see the data the City has.

The law says that all the data the City has is public (can be seen by anybody) unless there is a state or federal law that classifies the data as not public.

- Chapter 13 of the Minnesota Statutes, also known as the Minnesota Government Data Practices Act (MGDPA), is the primary resource the City uses in determining the public/not public nature of data.
- Unless there is a specific citation from the Data Practices Act or elsewhere in state or federal law, the City presumes that the data is public.
- The requestor has the right to look at all public data the City keeps.

These policies and procedures are written to assist you in making decisions in the areas listed above. If you have any questions, please call the City Clerk's Office at (507) 457-8200 or the City Attorney's Office at (507) 205-4905.

I. RESPONSIBLE AUTHORITY

The person who is the responsible authority for compliance with the Act for the City of Winona is Monica Hennessy Mohan, City Clerk. The responsible authority has designated Debra Beckman, Human Resources Manager, and Tom Williams, Chief of Police, as designees to assist in complying with the Act.

II. COLLECTION, STORAGE AND DISPOSITION OF GOVERNMENT DATA

A. Collection

Government data means all data created, collected, received, maintained or disseminated by any state agency, political subdivision or statewide system regardless of the data's physical form, storage media or conditions of use. Government data includes all papers, cards, correspondence, discs, maps, memoranda, microfilms, photographs, recordings, reports, tapes, writings, computer medium and other data, information or documentary material.

The information collected must be accurate, complete, and current for the purposes for which it was collected. At any time a data subject may contest the accuracy and completeness of the data.

Minnesota Statute Chapter 13 "establishes a presumption that government data are public and are accessible by the public for both inspection and copying unless there is federal law, a state statute, or a temporary classification of data that provides that certain data are not public." Minn. Stat. § 13.01, subd. 3 (1998).

B. Storage And Disposition

While some records must be kept for a period prescribed by law, a specific retention period for many government records is not prescribed. Those records may not be disposed of without the prior approval of the Records Disposition Panel. Unauthorized destruction of government records is a misdemeanor.

To obtain application forms for either a records retention schedule or disposition of specific records, please contact the Records Management Division of the Minnesota Department of Administration.

Each City department must keep its records in such an arrangement and condition as to make them easily accessible for convenient use.

III. CLASSIFICATION OF GOVERNMENT DATA

A. Data On Individuals

Data on individuals means all government data in which any individual is or can be identified as the subject of the data unless the appearance of the name or other identifying date 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.

Public data on individuals is data on individuals, living or dead, which is accessible to the public. Unless classified otherwise by state or federal law or temporary classification, all data on individuals is accessible to the public regardless of its interest in the data.

Private data on individuals is data which is not accessible to the public but is accessible to the data subject. Data on individuals is private if so classified by state or federal law or temporary classification. In addition to the data subject, private data is also accessible to the data subject's representative, individuals, entities or persons given express written permission by the data subject, a minor's parent or guardian, personnel within the governmental entity whose work assignments reasonably require access, individuals, entities or persons authorized by state or federal law, and pursuant to a court order.

Except when asked to supply investigative data to a law enforcement officer, an individual asked to supply private data concerning the individual must be informed of certain facts as set forth in Minnesota Statutes Section 13.04, Subd. 2. This is known as the *Tennessen* Warning. This warning must contain the following:

- the purpose and intended use of the requested data,
- whether the individual may refuse or is legally required to supply the requested data,
- any known consequences from supplying or refusing to supply the information, and
- the identity of other persons or entities authorized by state or federal law to receive the data.

Challenge to Data Accuracy. An individual who is the subject of public or private data may contest the accuracy or completeness of that data maintained by the City. The individual must notify the City's responsible authority in writing describing the nature of the disagreement. Within 30 days, the responsible authority or designee must respond and either (1) correct the data found to be

inaccurate or incomplete and attempt to notify past recipients of inaccurate or incomplete data, including recipients named by the individual, or (2) notify the individual that the authority believes the data to be correct.

An individual who is dissatisfied with the responsible authority's action may appeal to the Commissioner of the Minnesota Department of Administration, using the contested case procedures under Minnesota Statutes Chapter 14. The responsible authority will correct any data if so ordered by the Commissioner.

Data Protection

A. Accuracy and Currency of Data.

- All employees will be requested, and given appropriate forms, to provide updated personal information to the appropriate supervisor, City Clerk, or Finance Director, which is necessary for tax, insurance, emergency notification, and other personnel purposes. Other people who provide private or confidential information will also be encouraged to provide updated information when appropriate.

- Department heads should periodically review forms used to collect data on individuals to delete items that are not necessary and to clarify items that may be ambiguous.

- All records must be disposed of according to the City's records retention schedule.

B**. Data Safeguards.**

- Private and confidential information will be stored in files or databases which are not readily accessible to individuals who do not have authorized access and which will be secured during hours when the offices are closed.

- Private and confidential data must be kept only in City offices, except when necessary for City business.

- Only those employees whose job responsibilities require them to have access will be allowed access to files and records that contain private or confidential information. These employees will be instructed to:

    - not discuss, disclose, or otherwise release private or confidential data to City employees whose job responsibilities do not require access to the data,

    - not leave private or confidential data where non-authorized

individuals might see it, and

- shred private or confidential data before discarding.

Private data on decedents means data which, prior to the death of a data subject, were classified by state or federal law or temporary classification as private data. Private data on decedents is accessible to the representative of the decedent, the trustee appointed in a wrongful death action, individuals, entities or persons given express written permission by the data subject or the representative of the decedent, persons, individuals or entities authorized by state or federal law, personnel within the entity whose work assignments reasonably require access, and pursuant to a court order. Private data on decedents is public ten years after the actual or presumed death of the data subject **and** thirty years after the creation of the data. "Nonpublic data concerning a decedent, created or collected after death, are accessible by the representative of the decedent." Minn. Stat. § 13.10, subd. 3 (1998).

Confidential data on individuals means data which by state or federal law or temporary classification is not accessible to the public or to the subject of the data. Confidential data on individuals is accessible to individuals authorized by state or federal law, personnel within the entity whose work assignments reasonably require access, and pursuant to a court order.

Except when asked to supply investigative data to a law enforcement officer, an individual asked to supply confidential data concerning the individual must be informed of certain facts as set forth in Minnesota Statutes Section 13.04, Subd. 2.

Confidential data on decedents means data which, prior to the death of a data subject, were classified by state or federal law or temporary classification as confidential data. Confidential data on decedents is accessible to individuals authorized by state or federal law, personnel within the entity whose work assignments reasonably require access, and pursuant to a court order. Confidential data on decedents is public ten years after the actual or presumed death of the data subject **and** thirty years after the creation of the data. "Nonpublic data concerning a decedent, created after death, are accessible by the representative of the decedent." Minn. Stat. § 13.10, subd. 3 (1998).

B. Summary Data

Summary data means statistical records and reports derived from data on individuals but in which the individuals are not in any way identifiable. Summary data is public data unless otherwise classified by state or federal law or temporary classification.

C. Data Not On Individuals

Public data not on individuals is data accessible to the public unless otherwise classified by state or federal law or temporary classification.

Nonpublic data not on individuals means data which is not public but is accessible to the subject of the data, if any. As used here, the "subject of the data" means an individual, partnership, corporation, etc. Data not on individuals is nonpublic if so classified by state or federal law or temporary classification. Nonpublic data is accessible to the subject of the data, if any, individuals, entities or persons authorized by state or federal law, personnel within the entity whose work assignments reasonably require access, and pursuant to a court order. However, nonpublic data "may be discussed at a meeting open to the public to the extent provided in section 471.705, subdivision 1d." Minn. Stat. § 13.03, subd. 11 (1998).

Except for security information, nonpublic data shall become public ten years after the data was created, collected or received by the governmental agency. Access may be denied if release of the data will result in a harm to the public or data subject which outweighs the benefit to the public.

Protected nonpublic data not on individuals means data which is not public and not accessible to the subject of the data. Data not on individuals is protected nonpublic if so classified by state or federal law or temporary classification. Protected nonpublic data is accessible to individuals, entities or persons authorized by state or federal law, personnel within the entity whose work assignments reasonably require access, and pursuant to a court order.

Except for security information, protected nonpublic data shall become public ten years after the data was created, collected or received by the governmental agency. Access may be denied if release of the data will result in a harm to the public or data subject which outweighs the benefit to the public.

D. Juvenile Records.

The following applies to private (not confidential) data about people under the age of 18.

Parental Access. In addition to the people listed above who may have access to private data, a parent may have access to private information about a juvenile data subject. "Parent" means the parent or guardian of a juvenile data subject, or individual acting as a parent or guardian in the absence of a parent or guardian. The parent is presumed to have this right unless the responsible authority or designee has been given evidence that there is a state law, court order, or other legally binding document which prohibits this right.

Notice to Juvenile. Before requesting private data from juveniles, city personnel must notify the juveniles that they may request that the information not be given to their parent(s).

Denial of Parental Access. The responsible authority or designee may deny parental access to private data when the juvenile requests this denial and the responsible authority or designee determines that withholding the data would be in the best interest of the juvenile. The request from the juvenile must be in writing stating the reasons for the request. In determining the best interest of the juvenile, the responsible authority or designee will consider:

- Whether the juvenile is of sufficient age and maturity to explain the reasons and understand the consequences,
- Whether denying access may protect the juvenile from physical or emotional harm,
- Whether there is reasonable grounds to support the juvenile's reasons, and
- Whether the data concerns medical, dental, or other health services provided under Minnesota Statutes Sections 144.341 to 144.347. If so, the data may be released only if failure to inform the parent would seriously jeopardize the health of the minor.

The responsible authority or designee may also deny parental access without a request from the juvenile under Minnesota Statutes Section 144.335.

IV. TEMPORARY CLASSIFICATION

Unless a state or federal law expressly classifies government data as not public (i.e., private, confidential, nonpublic or protected nonpublic), the data is public and accessible to anyone. The temporary classification system was established to reclassify data when a governmental agency has a compelling reason to protect otherwise unprotected data. Minn. Stat. § 13.06, subd. 7 (1998) provides that "On or before January 15 of each year, the commissioner shall submit all temporary classifications in effect on January 1 in bill form to the legislature. The temporary classification expires June 1 of the year following its submission to the legislature." Note that "unless otherwise 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 to the data is made, regardless of the data's classification at the time it was collected, created, or received." Minn. Stat. § 13.03, subd. 9 (1998).

Temporary classification forms may be obtained from the Data Privacy Division of the State Department of Administration.

V. REQUESTS FOR GOVERNMENT DATA

A. Requests For Data – General

Upon request to the responsible authority or the designee, an authorized individual, entity or person shall be permitted to inspect and copy government data at reasonable times and places and if the party requests, s/he shall be informed of the data's meaning.

"If a person requests copies or electronic transmittal of the data to the person, the responsible authority may require the requesting person to pay the actual costs of searching for and retrieving governmental data, including the cost of employee time, and for making, certifying, compiling, and electronically transmitting the copies of the data or the data, but may not charge for separating public from not public data." Minn. Stat. § 13.03, subd. 3 (1998). See also Minn. Stat. § 13.05, subd. 4(d)(7).

The responsible authority may also charge an additional fee if the copies have commercial value and are a substantial and discrete portion of a formula, compilation, program, process, or system developed with significant expenditure of public funds. This additional fee must relate to the actual development costs of the information.

If the request is unclear or for many documents or for a variety of information or the data is not easily retrievable and involves the collating of data from a number of sources, you may require the request to be put in writing.

Regardless of where the data originates, if it is in your possession, it is government data and subject to the access provisions of the law. "Unless otherwise 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 to the data is made, regardless of the data's classification at the time it was collected, created, or received." Minn. Stat. § 13.03, subd. 9 (1998).

Requested information is to be released as promptly as circumstances allow and in an impartial, courteous and objective manner. Data may not be withheld, delayed or selectively released to favor any person, agency or media. Specific independent inquiries, especially from the media, are to be honored in the order received.

B. Requests For Data On Individuals By The Data Subject

Any individual may request verbally or in writing if the City has stored data about that individual and whether the data is classified as public, private, or confidential.

Upon request and when access/copies are authorized, the designee shall provide copies of the private or public data on individuals to the subject of the data or the subject's authorized representative.

The designee shall comply immediately, if possible, or within five working days of the date of the request if immediate compliance is not possible. If the responsible authority or designee cannot comply with the request within that time, s/he shall inform the requestor, and may have an additional five working days within which to comply with the request.

The responsible authority or designee must verify the identity of the requesting party as a person entitled to access. This can be through personal knowledge, presentation of written identification, comparison of the data subject's signature on a consent form with the person's signature in City records, or other reasonable means.

If access is authorized, the responsible authority or designee **must** supply the requested data within ten working days.

C. Requests For Summary Data

Unless classified by a state statute, federal law or temporary classification, summary data derived from private or confidential data on individuals is public and the responsible authority or designee shall inform the requestor of the estimated costs of preparing the summary data, if any.

The responsible authority or the designee shall:

1. Provide the summary data requested as soon as reasonably possible; OR

2. Provide a written statement to the requestor, giving a time schedule for preparing the requested data, including reasons for any delays; OR

3. Provide access to the requestor to the private or confidential data so that the requestor can compile the summary. Such access will be provided only when the requestor signs a non-disclosure agreement; OR

4. Provide a written statement to the requestor stating reasons why the requestor's access would compromise the private or confidential data.

A NON-DISCLOSURE AGREEMENT is used to protect the confidentiality of government data when the requestor of the summary data will prepare the summary by accessing private or confidential data on individuals. A non-disclosure agreement shall contain at least the following:

1. A general description of the private or confidential data which is being used to prepare summary data;

2. The purpose for which the summary data is being prepared;

3. A statement that the preparer (requestor) understands s/he may be subject to the civil or criminal penalty provisions of the Act in the event that the private or confidential data is disclosed;

4. A section in which the preparer (requestor), in consideration for being given access to private or confidential data, agrees not to disclose data in any form that would identify or tend to identify an individual and that s/he also agrees to defend and indemnify the City of Winona and any of its employees in any legal actions brought as a result of his/her having access to private or confidential data.

5. A description of the civil and criminal penalty provisions of the Act.

6. The signature of the requestor and the responsible authority, designee or his/her representative.

D. Requests For Government Data By Other Government Agencies

A responsible authority may allow another responsible authority access to data classified as other than public ONLY when the access is authorized or required by state statute or federal law.

An agency that supplies government data may require the requesting agency to pay the actual cost of supplying the data when the requested data is NOT provided in the normal course of business and NOT required by state or federal law.

Data shall have the same classification in the hands of the agency receiving it as it had in the agency providing it unless the classification is required to change to meet judicial or administrative requirements. When practical and necessary, the agency providing the requested information shall indicate the classification of the information if the data is classified as "not public." "If a state agency, statewide system, or political subdivision disseminates data to another state agency, statewide system, or political subdivision, a classification provided for by law in the hands of the entity receiving the data does not affect the classification of the data in the hands of the entity that disseminates the data." Minn. Stat. § 13.03, subd. 4(d) (1998).

When necessary, the requesting agency, if not listed on the "Tennessen Warning," should obtain informed consent from the data subject(s) for information classified

as private or confidential. Minnesota Statutes Section 13.04, Subd. 2.

E. Requests For All Other Government Data

For requests from parties other than individual data subjects or government agencies or persons, when access is authorized, the responsible authority or designee should provide data on request.

If access is authorized and the responsible authority or designee is not able to provide copies at the time the request is made, s/he shall supply copies as soon as reasonably possible.

F. Denying Requests For Access To Government Data

Access to government data may be denied when the data is classified by state statute or federal law as not accessible to the requestor.

Any person denied access to government data shall be informed orally at the time of the request or in writing as soon after that time as possible of the specific state statute, federal law or temporary classification upon which the denial is based.

Further, upon the request of any person denied access, the responsible authority or designee shall certify in writing that the request for access has been denied and cite the specific state statute, federal law or temporary classification upon which the denial was based.

VI. ANNUAL INVENTORY

By August 1 of each calendar year, each department shall file copies of its updated inventory with the Offices of the City Attorney and of the City Clerk. If the department determines that the data listings are complete and the classifications unchanged, then a letter stating these facts may be filed in lieu of an updated inventory.

VII. VIOLATION OF THE ACT

A non-willful violation may be punished by assessment against the City of damages suffered by the person aggrieved. In the case of a willful violation, the City may, in addition, be liable to exemplary damages of not less than $100 nor more than $10,000 for each violation. Minnesota Statutes Section 13.08, Subd. 1.

A person who willfully violates the Act is guilty of a misdemeanor. Willful violation constitutes just cause for suspension without pay or dismissal. Minnesota Statutes Section 13.09.