Board of County Commissioners Agenda Request

2G
Agenda Item #

Requested Meeting Date: July 23, 2019

Title of Item: Guidelines & Procedures for MN Government Data Practices Act

☐ REGULAR AGENDA	**Action Requested:**	☐ Direction Requested
☑ CONSENT AGENDA	☑ Approve/Deny Motion	☐ Discussion Item
☐ INFORMATION ONLY	☐ Adopt Resolution (attach draft)	☐ Hold Public Hearing*
	**provide copy of hearing notice that was published*	

Submitted by: Jessica Seibert	**Department:** Administration
Presenter (Name and Title):	**Estimated Time Needed:**

Summary of Issue:

Changes to the Data Practices Policy must be made by August 1st of each year. Attached is an updated Aitkin County Guidelines and Procedures for MN Government Data Practices Act for Board approval.

Changes for the Data Practices Act can be found on Pages 1, 34, and, 41. All changes are indicted in red. The changes consist of revising the date on the cover page, and updating the contact information under Responsible Authority, Data Practices Compliance Official and Designees.

Alternatives, Options, Effects on Others/Comments:

Recommended Action/Motion:

Approve the updated Aitkin County Guidelines and Procedures for Minnesota Government Data Practices Act.

Financial Impact:

Is there a cost associated with this request? ☐ *Yes* ☑ *No*

What is the total cost, with tax and shipping? $

Is this budgeted? ☐ *Yes* ☐ *No* *Please Explain:*

Legally binding agreements must have County Attorney approval prior to submission.

AITKIN COUNTY
GUIDELINES AND PROCEDURES

FOR
MINNESOTA
GOVERNMENT DATA PRACTICES ACT

Aitkin
County

Adopted by the Aitkin County Board of Commissioners
~~Approved by the Board November 27, 2018~~ July 23, 2019
~~Effective January 1, 2019~~

To the extent that the Minnesota Government Data Practices Act changes, these guidelines and procedures shall be construed as consistent with those changes.

MINNESOTA GOVERNMENT DATA PRACTICES ACT

Table of Contents

MINNESOTA GOVERNMENT DATA PRACTICES ACT

Introduction

These guidelines and procedures provide direction in complying with those portions of the MGDPA that relate to *public access to government data* and to the *rights of subjects of data*.

The public access requirements are:

- The presumption that all government data are public unless classified as not public by state or federal statute;
- The right of any person to know what kinds of data are collected by the government entity and how that data is classified;
- The right of any person to inspect, at no charge, all public government data at reasonable times and places;
- The right of any person to have public data explained in an understandable way;
- The right of any person to get copies of public government data at a reasonable cost;
- The right of any person to an appropriate and prompt response from the government entity when exercising these rights; and
- The right of any person to be informed of the authority by which an entity can deny access to government data.

A BRIEF OVERVIEW OF THE MINNESOTA GOVERNMENT DATA PRACTICES ACT

The Minnesota Government Data Practices Act regulates the management of all government data that are created, collected, received, or released by a government entity, no matter what form the data are in, or how they are stored or used.

Briefly, the Act regulates:

- what data can be collected;
- who may see or get copies of the data;
- the classification of specific types of government data;
- the duties of government personnel in administering the Act;
- procedures for access to the data;
- procedures for classifying data as not public;
- civil penalties for violation of the Act; and
- the charging of fees for copies of government data.

Government data is either *data on individuals or data not on individuals.* Data on individuals are classified as either public, private, or confidential. Data not on individuals are classified as public, nonpublic, or protected nonpublic. This classification system determines how government data are handled (see chart below).

Data on Individuals	Meaning of Classification	Data *Not* on Individuals
Public	Available to anyone for any reason	Public
Private	Available only to the data subject and to anyone authorized by the data subject or by law to see it	Nonpublic
Confidential	Not available to the public or the data subject	Protected Nonpublic

I. COLLECTION OF GOVERNMENT DATA

What is the Minnesota Government Data Practices Act?
The Minnesota Government Data Practices Act (MGDPA), which is Chapter 13 of Minnesota Statutes, is a state law that controls how government data are collected, created, stored, maintained, used, and disseminated.

What are government data?
Government data are all data maintained in any recorded form by government entities, including counties. As long as data are recorded in some way by a government entity, they are government data, no matter what physical form they are in, or how they are stored or used. Government data may be stored on paper forms/records/files, in electronic form, on audio or video tape, on charts, maps, etc. Government data normally do not include mental impressions.

Persons or entities licensed or funded by, or under contract to, a government entity are subject to the MGDPA to the extent specified in the licensing, contract, or funding agreement.

Official records must be kept. MINN. STAT. § 15.17, subd. 1 requires all officers and agencies of the state, and all officers and agencies of the counties, cities, and towns to make and keep all records necessary for a full and accurate knowledge of their official activities. Requirements for collecting, creating, maintaining, storing, and disseminating data are found in MINN. STAT. CH. 13 AND MINN. R. 1205, the Minnesota Government Data Practices Act and Rules. Links for locating the governing statute and rules are shown below.

Minnesota Statutes
Chapter 13. Government Data Practices
https://www.revisor.mn.gov/statutes/?id=13

Minnesota Administrative Rules, Chapter 1205, Data Practices
https://www.revisor.mn.gov/rules/?id=1205

A. The collection and storage of public, private, and confidential data on individuals are limited to that necessary for the administration and management of programs specifically authorized or mandated by the state, local governing body, or the federal government.

B. DEFINITIONS

1. **Data Inventory** - The public document required by MINN. STAT. § 13.025, subd. 1, containing the name of the responsible authority and the individual designee, title and address, and a description of each category of record, file, or process relating to private or confidential data on individuals maintained by the government entity. The responsible authority shall update the inventory annually and make any changes necessary to maintain the accuracy of the inventory.

2. **Authorized Representative** - The individual, entity, or person authorized to act on behalf of another individual, entity or person. For the purposes of the Act, the authorized representative may include, but is not limited to: (a) in the case of a minor, a parent, or guardian, (see Section IX.B, Notification to Minors); (b) an attorney acting on behalf of an individual when the individual has given written informed consent (see page 30-31); (c) any other individual entity, or person given written authorization by the data subject; or (d) an insurer or its representative, provided that the data subject has given informed consent (see page 30-31) for the release of the information, (e) court appointed guardian/conservator.

3. **Court Order** - The direction of a judge, or other appropriate presiding judicial officer made or entered in writing, or on the record in a legal proceeding.

4. **Data** - All data collected, created, received, maintained, or disseminated by a government entity regardless of its physical form, storage media, or conditions of use, including, but not limited to, paper records and files, microfilm, computer media, or other processes.

5. **Data Subject** - The individual or person about whom the data is created or collected.

6. **Designee** - Any person designated by a responsible authority (a) to be in charge of individual files or systems containing government data and (b) to receive and comply with requests for government data.

7. **Government Entity** – A state agency, statewide system, or political subdivision.

8. **Individual** - A natural person. In the case of a minor or an individual adjudged mentally incompetent, "individual" includes a parent or guardian or an individual acting as a parent or guardian in the absence of a parent or guardian, except that the responsible authority shall withhold data from parents or guardians or individuals acting as parents or guardians in the absence of parents or guardians, upon request by the minor if the responsible authority determines that withholding the data would be in the best interest of the minor.

9. **Informed Consent** (see page 30-31) - The written consent that must be given by a data subject to allow disclosure of private data about the individual.

10. **Person** - Any individual, partnership, corporation, association, business trust, or legal representative of an organization.

11. **Political Subdivision** - Any county, statutory or home rule charter city, school district, special district, any town exercising powers under Minn. Stat. 368 and located in a metropolitan area, and any board, commission, district or authority created pursuant to law, local ordinance, or charter provision. It includes any nonprofit corporation which is a community action agency organized to qualify for public funds, or any nonprofit social service agency which performs services under contract to a government entity to the extent that the nonprofit social service

agency or nonprofit corporation collects, stores, disseminates, and uses data on individuals because of a contractual relationship with a government entity.

12. **Representative of the Decedent** - The personal representative of the estate of the decedent during the period of administration, or if no personal representative has been appointed, or after discharge, the surviving spouse, any child of the decedent, or, if there are no surviving spouse or children, the parents of the decedent.

13. **Requestor** - The individual, entity, or person requesting access and/or copies of the government data.

14. **Responsible Authority - Counties** - Each elected official of the county shall be the responsible authority of the respective office. An individual who is an employee of the county shall be appointed by the County Board to be the responsible authority for any data administered outside the departments of elected officials. For a statewide system, the responsible authority is the commissioner of any state department, or any executive officer designated by statute or executive order as responsible for such system.

15. **Rules** - "The Rules Governing the Enforcement of the Minnesota Government Data Practices Act." Minn. R., Chap. 1205. .

16. **State Agency** - The state, the University of Minnesota, and any office, officer, department, division, bureau, board, commission, authority, district, or agency of the state.

17. **Statewide System** - Any recordkeeping system in which government data is collected, stored, disseminated, and used by means of a system common to one or more state agencies or more than one of its political subdivisions or any combination of state agencies and political subdivisions.

18. **Temporary Classification** - An application by a state agency, statewide system, or political subdivision, pursuant to MINN. STAT. § 13.06 which has been approved by the Commissioner of Administration to classify government data not classified by state statute or federal law as either private or confidential for data on individuals, or nonpublic or protected nonpublic for data not on individuals.

19. **Tennessen Warning (see page 28-29)** - Those rights, as contained in Section IX.A, communicated to an individual asked to supply private or confidential data concerning himself or herself.

II. CLASSIFICATION OF GOVERNMENT DATA

For the purposes of these guidelines, government data is divided into four types; (a) data on individuals, which is classified as either public, private, or confidential; (b) data not on individuals, which is classified as either public, nonpublic, or protected nonpublic; (c) statistical or summary data derived from data on individuals in which individuals are not identified; and (d) data on decedents. These classifications, the criteria for classification, and the description of who has access are as follows:

A. DATA ON INDIVIDUALS

1. Public Data on Individuals

a. Definition: All data on individuals is public, unless classified as private or confidential.

b. Data on Individuals is Public if:

1) A statute or federal law requires or allows the collection of the data and does not classify the data as private or confidential.

2) An application for Temporary Classification for private or confidential data on individuals is disapproved by the Commissioner of Administration.

3) The data is summary or statistical data derived from data on individuals.

4) Private or confidential data becomes public in order to comply with either judicial or administrative rules pertaining to the conduct of legal action. (For example: Private or confidential data which is presented in court and made public by the court.)

c. Access: All public data on individuals is accessible by any person regardless of their interest in that data.

2. Private Data on Individuals

a. Definition: Private data on individuals is data which is not accessible to the public, but is accessible to the individual subject of the data.

b. Tennessen Warning (see page 28-29): Except for law enforcement investigations, a Tennessen Warning must be given when private data is collected from the subject of the data (Section IX.A describes the Tennessen Warning.)

A Tennessen Warning need not be given when private data is collected from someone other than the subject of the data.

c. **Data on Individuals is Private if:**

1) A state statute or federal law expressly classifies the data as not accessible to the public, but accessible to the subject of the data.

2) A Temporary Classification of private has been approved by the Commissioner of Administration and has not expired.

3) If data is classified as both private and confidential by state or federal law, the data is private.

d. **Access:** Private data on individuals is accessible to:

1) The individual subject of the data or the representative as authorized in writing (if the subject is a minor, usually by the subject's parent or guardian).

2) Individuals, entities, or persons who have been given express written permission by the data subject. (Section IX.C describes Informed Consent.)

3) Personnel within the entity whose work assignment requires access as determined by the responsible authority or designee.

4) Individuals, entities, or persons who used, stored, and disseminated government data collected prior to August 1, 1975, with the condition that use, storage, and dissemination was not accessible to the public, but accessible to the data subject. Use, storage, and dissemination of this data is limited to the purposes for which it was originally collected.

5) Individuals, entities, or persons for which a state, local, or federal law authorizes new use or new dissemination of the data.

6) Individuals, entities, or persons subsequent to the collection of the data and subsequent to the communication of the Tennessen Warning, when specifically approved by the Commissioner of Administration, as necessary, to carry out a function assigned by law.

7) Pursuant to a court order.

8) Individuals, entities, or persons as otherwise provided by law.

3. **Confidential Data on Individuals**

a. **Definition:** Data on individuals is confidential if it is made by statute or federal law not accessible by the public and <u>not</u> accessible to the individual subject of the data.

b. **Tennessen Warning (see page 28-29):** Except for law enforcement

investigations, a Tennessen Warning must be given when confidential data is collected from the subject of the data.

A Tennessen Warning is not given when confidential data is collected from someone other than the subject of the data.

c. Data on Individuals is Confidential if:

1) A state or federal statute expressly provides that: (a) the data shall not be available to either the public or to the data subject, or (b) the data shall not be available to anyone except those agencies which need the data for agency purposes.

2) A Temporary Classification of confidential has been approved by the Commissioner of Administration and has not expired.

d. Access: Confidential data on individuals is accessible to:

1) Individuals, entities, or persons who are authorized by state, local, or federal law to gain access.

2) Personnel within the entity whose work assignment requires access as determined by the responsible authority, or the designee.

3) Individuals, entities, or persons who used, stored, and disseminated government data collected prior to August 1, 1975, with the condition that the data was not accessible to the individual subject of the data.

4) Individuals, entities, or persons for which a state or federal law authorizes a new use or new dissemination of the data.

5) Individuals, entities, or persons subsequent to the collection of the data and communication of the Tennessen Warning when specifically approved by the Commissioner of Administration, as necessary, to carry out a function assigned by law.

6) Pursuant to a court order.

7) Individuals, entities, or persons as otherwise provided for by law.

B. PUBLIC, NONPUBLIC, OR PROTECTED NONPUBLIC DATA NOT ON INDIVIDUALS

1. Public Data Not on Individuals

a. Definition: Public data not on individuals means data not on individuals which is accessible to the public.

b. Data Not on Individuals is Public if:

1) A statute or federal law does not expressly classify the data as not public.

2) An application for Temporary Classification for data as nonpublic or protected nonpublic is not approved by the Commissioner of Administration.

3) A statute requires the data to be made available to the public.

c. Access: Public data not on individuals is accessible to any person regardless of their interest in the data.

2. Nonpublic Data Not on Individuals

a. Definition: 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 a person as defined in Section I.C., paragraph 10.

b. Data Not on Individuals is Nonpublic if:

1) A state statute or federal law classifies the data as not public, but accessible to the subject of the data, if any.

2) A Temporary Classification of data as nonpublic has been approved by the Commissioner of Administration.

c. Access: Nonpublic data not on individuals is accessible to:

1) The subject of the data, if any.

2) Personnel within the entity whose work assignment requires access as determined by the responsible authority or designee.

3) Individuals, entities, or persons authorized by statute or federal statute to gain access.

4) It is reasonable to conclude that access to the data should be limited to entities or persons who have the legal authority to do so, and to entity staff on a need-to-know basis, that a representative of the organization which is the subject of the data may access the nonpublic data and may consent to its release.

5) Pursuant to court order.

6) Individuals, entities, or persons as otherwise provided by law.

3. Protected Nonpublic Data Not on Individuals

a. Definition: Protected nonpublic data not on individuals means data which is

not public and not accessible to the subject of the data, if any. As used here, the subject data means a person as defined in Section I.C., paragraph 10.

b. Data Not on Individuals is Protected Nonpublic if:

1) A state statute or federal law classifies the data as not accessible to the public and not accessible to the data subject.

2) A Temporary Classification of government data as protected nonpublic has been approved by the Commissioner of Administration.

c. Access: Protected nonpublic data not on individuals is accessible to:

1) Personnel within the entity whose work assignment requires access as determined by the responsible authority or the designee.

2) Individuals, entities, or persons authorized by statute or federal law to gain access.

3) Pursuant to a court order.

4) Individuals, entities, or persons as otherwise provided by law.

C. SUMMARY DATA

1. Definition: Summary data means statistical records and reports derived from data on individuals, but in which the individuals are not identified and neither their identities nor other characteristics that could uniquely identify the individual is ascertainable.

2. Data is Summary Data if:

a. All data elements that could link the data to a specific individual have been removed; AND,

b. Any list of numbers or other data which could uniquely identify an individual is separated from the summary data and is not available to persons who gain access to or possess summary data.

3. Access: Unless classified by a Temporary Classification, summary data is public and may be requested by and made available to any individual or person, including a governmental entity.

D. DATA ON DECEDENTS

1. Private Data on Decedents

a. Definition. Upon death, private and confidential data on an individual shall become, respectively, private data on decedents and confidential data on decedents.

b. Access:

1) Access is available to the personal representative of the estate during the administration or if no personal representative, the surviving spouse, any child of the decedent, or if no spouse or children, to the parent of the decedent.

2) A trustee appointed in a wrongful death action also has access to appropriate private data on decedents concerning the data subject.

2. Confidential Data on Decedents.

a. Definition. Confidential data on decedents means data which, prior to the death of the data subject, was classified by statute, federal law, or temporary classification as confidential data.

b. Access. Access to the data is the same as access to confidential data on individuals.

c. The representative of the decedent may exercise all rights which are conferred by the Act on individuals who are the subjects of confidential data, in the case of confidential data on decedents.

3. Release of private data on a decedent or confidential data on a decedent may also be obtained from a court following the procedure outlined in the statute. Any person may bring an action in the district court located in the county where the data is being maintained or, in the case of data maintained by state agency, in any county, to authorize release of private data on decedents or confidential data on decedents. The court must examine the data and consider whether the harm to the surviving spouse, children, or next-of-kin of the decedent, the harm to any other individual identified in the data, or the harm to the public outweighs the benefit to the person bringing the action or the benefit of the public.

4. Private data on decedents and confidential data on decedents shall become public when ten years have elapsed from the actual or presumed death of the individual and 30 years have elapsed from the creation of the data. For purposes of this determination, an individual is presumed to be dead if either 90 years elapsed since the creation of the data, or 90 years have elapsed since the individual's birth,

whichever is earlier, except that an individual is not presumed to be dead if readily available data indicates that the individual is still living.

III. REQUEST FOR GOVERNMENT DATA

Refer to Section V, the Public Data Request form (see page 33-37), and/or Data Request by Subject of Data form (see page 38-43) when copies are requested. No fee shall be charged for the actual costs of retrieving data or for viewing data.

A. REQUEST FOR DATA - GENERAL - Upon request to the responsible authority or designee, an authorized person shall be permitted to inspect government data at reasonable times and places, and if the party requests, they shall be informed of the meaning of the data. If the data requested is public data, no form is necessary. Upon request, public data may be disclosed over the telephone.

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.

The Public Data Request form (see page 33-37) or Request by Subject of Data form (see page 38-43) shall be completed for all requests by the public for government data which is classified as other than public.

B. REQUESTS FOR DATA ON INDIVIDUALS BY THE DATA SUBJECT

1. Upon request and when access or copies are authorized, the designee shall provide copies of the private or public data on an individual to the subject of the data or authorized representative. See Minn. R. 1205.0500 if data subject is a minor.

2. The designee shall comply immediately, if reasonably possible, or within ten (10) working days of the date of request, if immediate compliance is not reasonably possible.

3. After an individual has been shown the private data and informed of its meaning, the data need not be disclosed to that individual for six (6) months, unless a dispute or action is pending (concerning accuracy of data), or additional information has been obtained on that individual.

C. REQUESTS FOR SUMMARY DATA

1. Unless classified by a Temporary Classification, summary data derived from private or confidential data on individuals is public and the responsible authority or designee shall provide the summary data upon the written request of any individual or person.

2. Within ten (10) days of receipt of such request, the responsible authority or designee shall inform the requestor of the costs of preparing the summary data, if any.

3. The responsible authority or the designee shall:

   a. Provide the summary data requested **OR**

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

   c. Provide access to the requestor to the private or confidential data so that the requestor can compile the summary data. Such access will be provided only when the requestor signs a non-disclosure agreement (see page 27); **OR**

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

4. A non-disclosure agreement (see page 27) is used to protect the confidentiality of government data when the requestor of the summary data prepares the summary by accessing private or confidential data on individuals. A non-disclosure agreement shall contain at least the following:

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

   b. The purpose for which the summary data is being prepared.

   c. A statement that the requestor understands that the requestor may be subject to the civil or criminal penalty provisions of the Act.

   d. The signature of the requestor and the responsible authority, designee, or representative.

D. REQUESTS FOR GOVERNMENT DATA BY OTHER GOVERNMENT AGENCIES.

1. A responsible authority shall allow another responsible authority access to data classified as private, confidential, nonpublic, or protected nonpublic only when the access is authorized or required by state or federal statute.

2. An agency that supplies government data under this section 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 statute.

3. In most cases, 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.

4. When practical and necessary, the requesting agency not listed on the Tennessen Warning (see page 28-29) shall obtain the informed consent (see page 30-31) from the data subject(s) for information classified as private or confidential.

E. HOW DATA PRACTICES APPLIES TO CONTRACTUAL LICENSING AND FUNDING RELATIONSHIP WITH GOVERNMENT ENTITIES.

1. Pursuant to MINN. STAT. § 13.05, subd. 6, if a person **receives not public data on individuals from a government entity because that person has a contract with that entity,** the person must administer the data in a manner that is consistent with the MGDPA.

2. Pursuant to MINN. STAT. § 13.05, subd. 11, if a private person **collects, receives, stores, uses, maintains or disseminates data because the person has a contract with a government entity to perform any of the entity's functions,** all of the data are subject to the requirements of the MGDPA and the contractor must comply with the MGDPA requirements. The contractor may be sued under Sec. 13.08, civil remedies. The contract must clearly inform the contractor of these responsibilities.

3. Pursuant to Minn. Stat. § 13.02, subd. 11, if the data is **collected by a nonprofit social services entity which performs services under contract to a government entity,** and the data is collected and used because of that contract, access to the data is regulated by the MGDPA.

4. If a third party is **licensed by a government entity and the licensure is conditioned upon compliance with the MGDPA, or if the party has another type of contract with a government entity,** the party is subject to the MGDPA to the extent specified in the contract or the licensing agreement.

IV. DATA REQUEST FORM (see page 33-37) AND DATA REQUEST FORM FOR SUBJECT OF DATA (see page 38-43)

A. DATA REQUEST FORM (see page 33-37) AND DATA REQUEST FORM FOR SUBJECT OF DATA (see page 38-43).

These forms provide a record of the requestor identification information and the government data requested, as well as the action taken by the responsible authority, or the designee, and any financial transaction which occurs.

B. WHEN COMPLETED. The Data Request form or Data Request form for Subject of Data should be completed for all

requests by the public for government data classified as private, confidential, nonpublic, and protected nonpublic and for all requests by other government agencies for which the not public data is not routinely shared or provided in the normal course of business.

V. FEES FOR COPIES OF GOVERNMENT DATA.

Pursuant to the Minnesota Government Data Practices Act and Aitkin County Board

resolution and unless otherwise provided for by federal law, state statute or rule, fees for copies of government data shall be determined by departments based on the costs of providing such service as set forth in Section V.E. Fees shall be reasonable and consistent. If the fee for fulfilling the request is greater than $5.00, pre-payment shall be required.

NOTE: FEES SHALL NOT BE CHARGED TO THOSE INDIVIDUALS WHO ONLY WISH TO VIEW DATA.

NOTE: FEES MAY NOT BE CHARGED FOR SEPARATING PUBLIC FROM NONPUBLIC DATA.

A. COPIES PROVIDED AT NO CHARGE. When access is authorized, copies may be provided at no charge:

1. When another government agency or responsible authority requires or requests the record/document copies as part of the administration and management of an authorized program and the copies are usually provided as part of the normal course of business.

2. When records, documents, brochures, pamphlets, books, reports, or other similar publications are produced for free distribution to the public. A charge may be assessed if an individual request exceeds normal distribution.

3. When the court orders the requesting party to proceed in forma pauperis.

B. COPIES PROVIDED WITH CHARGE. When access is authorized, copies shall be provided at the applicable rate in the following circumstances:

1. Other government agencies or responsible authorities who require or request record documents or publication copies which are not usually provided or reproduced as part of the normal course of business.

2. Records, documents, brochures, pamphlets, books, reports, or other similar publications that are not normally provided or reproduced for distribution to the public.

3. Public data on individuals and public data <u>not</u> on individuals, particularly when the requestor is not the subject of the data.

C. COPYING FEES. Copying fees shall be charged in accordance with the Fee Schedule for those records, documents, and publications covered in Section B above.

1. When copies are mailed, postage costs shall be added to the rates listed in Appendix C, unless alternative arrangements have been made.

D. COLLECTION OF COPYING FEES. Fees shall be collected before releasing copies unless prior arrangements have been made.

E. FEE SCHEDULE.

See Appendix C

F. DISPOSITION OF FEES. Copying fees collected shall be deposited in the appropriate account with the county treasurer.

VI. ASSIGNMENT OF DESIGNEE.

The responsible authority may assign, in writing, one or more designees. The designee is the person in charge of individual files or systems containing government data and who receives and complies with the requests for government data. Additionally, the designee shall implement the provisions of the Act, the rules, and these guidelines and procedures as directed by the responsible authority. All duties outlined as duties of the responsible authority may be delegated to the designee.

VII. DUTIES OF THE RESPONSIBLE AUTHORITY OR DESIGNEE.

A. DATA INVENTORY

1. The responsible authority shall prepare an inventory containing the authority's name, title, address, and a description of each category of record, file, or process relating to private or confidential data on individuals maintained by the authority's government entity. Forms used to collect private and confidential data may be included in the inventory.

2. The responsible authority shall update the inventory annually and make any changes necessary to maintain the accuracy of the inventory..

3. The responsible authority shall supply the document to the Commissioner of Administration, State of Minnesota, if requested by the Commissioner.

B. PROCEDURES FOR DISSEMINATION OF DATA.

1. The responsible authority shall ensure that each department establishes procedures to manage the dissemination of data. Collection, storage, use, and dissemination of private and confidential data shall be limited to what is necessary for the administration and management of programs authorized or mandated by the state, local governmental body, or the federal government.

2. Data cannot be collected, stored, used, or disseminated for any purpose other than the purpose stated to the individual when the data was originally collected unless:

   a. The data was collected prior to 1975, in which case the data can be used for the original purpose for which it was collected or for an additional purpose approved by the Commissioner of Administration.

b. There is specific authorization for the use in state, local, or federal law.

c. The additional use has been approved by the Commissioner of Administration, as necessary, to carry out a function designated by law.

d. The individual data subject has given an informed consent for the additional use of the data (see Informed Consent, Section IX., subd. C).

C. DATA PROTECTION.

The responsible authority shall establish procedures to assure that all data on individuals is accurate, complete, and current for the purpose for which it was collected, and establish appropriate security safeguards for all records containing data on individuals.

VIII. ACCESS TO GOVERNMENT DATA

A. WHO CAN MAKE A DATA REQUEST?

Anyone may exercise the right to access public government data by making a data request.

B. TO WHOM MUST A DATA REQUEST BE MADE?

1. A data request must be made to the responsible authority or to the appropriate designee(s).

2. The responsible authority for an entity must prepare summary data upon the request of any person if the request is in writing and the requestor pays for the cost to prepare the data.

3. The responsible authority may delegate the preparation of summary data to anyone outside of the entity, including the requestor, if

a. That person's purpose is set forth in writing and the person agrees not to release any of the private or confidential data used to prepare the summary data; and

b. If the entity reasonably determines that the access will not compromise private or confidential data on individuals.

4. The entity may require the requestor to prepay the cost of preparing summary data.

IX. RIGHTS OF DATA SUBJECT

A. TENNESSEN WARNING - Rights of Subjects of Data (see page 28-29)

1. Except for law enforcement investigations, every department that collects private and confidential data from an individual concerning that individual shall, prior to collecting the data, inform the individual of their rights as a subject of data. The notice must be given whenever:

   a. A government *entity requests* data;
   b. The data is requested from an *individual*;

   c. The data requested are *private or confidential*; **and**,

   d. The data is *about the individual* from whom it is requested.

   All four of these conditions must be present before a Tennessen warning notice (see page 28-29) must be given. These rights are referred to as the Tennessen Warning.

   A Tennessen Warning is not required when private and confidential data is collected from an individual who is not the subject of the data.

2. The Tennessen Warning consists of the following information that must be communicated to the individual from whom private or confidential data concerning the individual is collected.

   a. The purpose and intended use of the data. This is why the data are requested and how they will be used within the collecting entity.

   b. Whether the individual may refuse, or is legally required to supply the data. The subject has the right to know whether or not she/he is required by law to provide the data requested.

   c. Any consequences to the individual of either supplying or refusing to supply the data. The entity is required to state the consequences known to the entity at the time when the notice is given; **and**

   d. The identity of other persons or entities that are authorized by law to receive the data. The notice must specifically identify recipients that are known to the entity at the time the notice is given.

   NOTE: In accordance with the Federal Privacy Act of 1974, any federal, state, or local agency which requests an individual to disclose their social security account number shall inform that individual whether that disclosure is mandatory or voluntary, by what statutory or other authority such number is

solicited, and what uses will be made of it.

3. Tennessen Warnings may be either oral or written.

   a. An oral communication. This is not the preferred method of communicating the Tennessen Warning. However, it may be necessary under some circumstances. If an oral communication is necessary, the specific language communicated must be in written form and contained in the departmental data practices procedures and the situation documented.
   b. A written communication requiring the signature of the data subject (i.e., a signature attesting that the individual from whom private or confidential data is collected has read and understands their rights pertaining to the requested data). The Tennessen Warning may be included on the form that collects the private or confidential data.

4. A sample format for a Notice of Rights Tennessen Warning is on page 29.

B. NOTIFICATION TO MINORS

A minor has the right to request that the entity withhold private data about her/him from the parent or guardian. The entity may require that the request be in writing. A written request must include the reasons for withholding the data from the parents and must be signed by the minor.

Upon receipt of the request, the responsible authority must determine whether honoring the request is in the best interests of the minor. The responsible authority must consider, at a minimum:

1. Whether the minor is old and mature enough to explain the reasons for the request and to understand the consequences of making the request;

2. Whether denying access to the data may protect the minor from physical or emotional harm;

3. Whether there is a reason to believe that the minor's reasons for denying access to the parent(s) are reasonably accurate; and

4. Whether the nature of the data is such that disclosing the data to the parents could lead to physical or emotional harm to the minor. Minn. Rule 1205.0500 contains the procedures for the release of data about minors.

C. INFORMED CONSENT (see page 30-31)

1. Private data on individuals may be used by and disseminated to any individual or person by the responsible authority, or the designee, if the individual subject or subjects of the data have given their informed consent.

NOTE: Informed consent cannot authorize a new purpose or a new use of confidential data on individuals.

2. Private data may be used by and disseminated to any entity (e.g., political subdivision, government agency, etc.) if the individual subject or subjects have given their informed consent.

3. All informed consents shall be in writing. (See page 30-31)

4. Informed consent shall not be deemed to have been given by an individual subject of the data by the signing of any statement authorizing any person or agency to disclose information about the individual to an insurer or its authorized representative, unless the statement is:

   a. In plain language;

   b. Dated;

   c. Specific in designating the particular persons or agencies the data subject is authorizing to disclose information about the data subject;

   d. Specific as to the nature of the information the subject is authorizing to be disclosed;

   e. Specific as to the persons or agencies to whom the subject is authorizing information to be disclosed;

   f. Specific as to the purpose or purposes for which the information may be used by any of the parties named in clause (e), both at the time of the disclosure and at any time in the future; and

   g. Specific as to its expiration date which should be within a reasonable period of time, not to exceed one year, except in the case of authorizations given in connection with applications for life insurance or noncancellable or guaranteed renewable health insurance and identified as such, two years after the date of the policy.

5. The informed consent for the disclosure of alcohol and drug abuse patient records may be made only if the consent is in writing and expressly states the fact that the request is for alcohol or drug abuse patient records. It should contain the following:

   a. The name of the program which is to make the disclosure;

   b. The name or title of the person or organization to which disclosure is to be made;

   c. The name of the patient;

d. The purpose or nature of information to be disclosed;

e. The extent or nature of information to be disclosed;

f. A statement that the consent is subject to revocation at any time, except to the extent that action has been taken in reliance thereon, and a specification of the data, event, or condition upon which it will expire without express revocation;

g. The date on which the consent is signed; and

h. The signature of the patient and, when required, of a person authorized to give consent.

6. A sample format is on page 31.

D. PROCEDURES FOR COMPLYING WITH DATA REQUESTS FROM AN INDIVIDUAL

The responsible authority shall ensure that each department establishes procedures to comply with requests for government data in an appropriate and prompt manner.

1. Upon request to the responsible authority, an individual shall be informed whether they are the subject of stored data on individuals, and whether it is classified as public, private, or confidential.

a. The responsible authority shall provide access to the private or public data upon request by the individual subject of the data.

b. An individual may contest the accuracy, current status, or completeness of public or private data. If the individual notifies the responsible authority in writing as to the nature of the disagreement with the data, the responsible authority shall, within 30 days, either correct the data and attempt to notify past recipients of inaccurate, incomplete, or out of date data, including recipients named by the individual, or notify the individual that the responsible authority believes the data to be correct. Subsequently, data in dispute shall be disclosed only if the individual's statement of disagreement is included with the disclosed data.

2. The responsible authority shall prepare a public document, setting forth in writing the rights of the data subject and specific procedures in effect in the county for access by the data subject to public or private data on individuals.

a. When a request is denied, the responsible authority must inform the requestor orally at the time of the request, and in writing, as soon thereafter as possible, and shall cite the statute, temporary classification, or federal law on which the determination is based.

b. The responsible authority shall require the requestor to pay the actual costs of making and certifying copies of the data requested, except those exempted in Section V., subd. A. The requestor may not be charged for separating private or confidential data from public data.

c. The responsible authority shall inform the requestor of the data's meaning, if asked to do so.

E. IF AN ENTITY DETERMINES THAT CHALLENGED DATA ARE ACCURATE AND/OR COMPLETE, AND THE DATA SUBJECT DISAGREES WITH THAT DETERMINATION, THE SUBJECT HAS THE RIGHT TO APPEAL THE ENTITY'S DETERMINATION TO THE COMMISSIONER OF ADMINISTRATION.

1. The subject has the right to take this step *only* after both the subject and the entity have properly completed all the steps in the data challenge process. The subject may appeal only the entity's determination about the accuracy and/or completeness of data.

2. The requirements for filing an appeal are set out at Minnesota Rules Section 1205.1600.

3. Procedure when data is not accurate or complete.

a. An individual subject of the data may contest the accuracy or completeness of public or private data. To exercise this right, an individual shall notify, in writing, the responsible authority describing the nature of the disagreement. The responsible authority shall, within 30 days, 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. Data in dispute shall be disclosed only if the individual's statement of disagreement is included with the disclosed data.

4. The determination of the responsible authority may be appealed pursuant to the provisions of the Administrative Procedure Act, MINN. STAT. § 14.57 to 14.62 and Minn. R. 1205.1600, relating to contested cases. Upon receipt of an appeal by an individual, the commissioner of administration shall, before issuing the order and notice of a contested case hearing required by Chapter 14, try to resolve the dispute through education, conference, conciliation, or persuasion. If the parties consent, the commissioner may refer the matter to mediation. Following these efforts, the commissioner shall dismiss the appeal or issue the order and notice of hearing.

a. Data on individuals that have been successfully challenged by an individual must be completed, corrected, or destroyed by a state government entity without regard to the requirements of Section 138.17.

b. After completing, correcting, or destroying successfully challenged data, a state agency, political subdivision, or statewide system may retain a copy of the Commissioner of Administration's order issued under Chapter 14 or, if no order were issued, a summary of the dispute between the parties that does not contain any particulars of the successfully challenged data.

X. ROLE OF THE COMMISSIONER OF ADMINISTRATION.

A. Pursuant to Section 13.06, subdivision 6a, the Commissioner of the Minnesota Department of Administration is given the authority to approve new uses and disseminations of private and confidential data on individuals.

B. Section 13.06 of the Minnesota Government Data Practices Act (MGDPA) gives to the Commissioner certain powers with regard to approving temporary classifications of data.

C. Section 13.072 of the MGDPA gives the Commissioner authority to issue advisory opinions concerning the rights-of-data-subjects and the classification of government data. Commissioner's opinions may be found on the World Wide Web at www.ipad.state.mn.us

XI. CONSEQUENCES FOR NOT COMPLYING WITH THE MGDPA.

A. Pursuant to Section 13.08 of the MGDPA, a government entity may be sued for violating any of the Act's provisions.

B. Section 13.09 provides criminal penalties and disciplinary action as extreme as dismissal from public employment, for anyone who willfully (knowingly) violates a provision of the MGDPA.

XII. WHERE MORE INFORMATION CAN BE FOUND.

A. *Government entities always must look to their legal advisor(s) for guidance and legal advice on data practices issues.* Only the legal advisor for an entity has the authority and responsibility to provide specific legal advice about the provisions of the MGDPA, and other laws, as they relate to that entity.

1. Minnesota Statutes Chapter 13 (the MGDPA) may be found on the website of the Revisor of Statutes at: www.leg.state.mn.us/leg/statutes.asp.

2. Minnesota Rules, Chapter 1205, The Rules Governing Data Practices, promulgated by the Minnesota Department of Administration, also may be found at the website of the Revisor of Statutes at: www.revisor.leg.state.mn.us/arule/1205.

AITKIN COUNTY

Non-Disclosure Agreement

1. General description of the private or confidential data which is being used to prepare summary data:

2. Purpose for which summary data is being prepared:

3. I,_____,representing _____

have requested the data described above and for the purposes stated and fully understand that I may be subject to the civil or criminal penalty provision of the Minnesota Data Practices Act in the event that the private or confidential data is disclosed.

> Minn. Stat. § 13.09. *Any person who willfully violates the provisions of* Minnesota Statutes Chapter 13, *or any rules adopted or regulation promulgated there under is guilty of a misdemeanor. Any willful violation of* Minnesota Statutes Chapter 13 *by any public employee constitutes just cause for suspension without pay or dismissal of the public employee.*

_____ _____

Requestor of Data Date

_____ _____

Responsible Authority/Designee Date

THE NOTICE OF RIGHTS TENNESSEN WARNING INSTRUCTION GUIDE

Minnesota Statutes Section 13.04, subdivision 2

The notice must be given when:	1. An individual 2. Is asked to supply 3. Private or confidential data 4. Concerning self All four conditions must be present to trigger the notice requirement.
Statements must be included from the individual that inform the individual:	• Why the data is being collected and how the entity intends to use the data; • Whether the individual may refuse or is legally required to supply the data; • Any consequences to the individual of either supplying or refusing to supply the data; and • The identity of other persons or entities authorized by law to receive the data.
Consequences of giving the notice are:	Private or confidential data on individuals may be collected, stored, used, and released as described in the notice without liability to the entity.
Consequences on *not* giving the notice are:	Private or confidential data on individuals cannot be collected, stored, used, or released for any purposes other than those stated in the notice unless: • The individual subject of the data gives informed consent; • The Commissioner of Administration gives approval; or • A state or federal law subsequently authorizes or requires the new use or release.

"NOTICE OF RIGHTS"
SAMPLE FORMAT FOR TENNESSEN WARNING

In accordance with the Minnesota Government Data Practices Act, Aitkin County is required to inform you of your rights as they pertain to the private information collected from you. Your personal information we collect from you is private. Access to this information is available only to you and the agency collecting the information and other statutorily authorized agencies, unless you or a court authorize its release.

The Minnesota Government Data Practices Act requires that you be informed that the following information, which you are asked to provide, is considered private.

_____

The purpose and intended use of the requested information is:

_____

Authorized persons or agencies with whom this information may be shared include:

_____

Furnishing the above information is voluntary, but refusal to supply the requested information will mean:

_____

_____
Name

_____
Date

MINN. STAT. § 13.04(2)

INFORMED CONSENT INSTRUCTION GUIDE

A. Enter the complete name and address of the entity that maintains the information. Include any relevant program names, staff names, titles and telephone numbers.

B. Identify, as specifically as possible, the reports, record names, or types of information or records that will be released.

C. Identify the entity or agencies to which the information will be released. Include the name and address of the entity. Include relevant staff names and titles. Be specific.

D. Describe specifically and completely the purpose(s) for seeking the client's informed consent and the new use(s) to which the information will be put.

E. Describe specifically and completely the known consequences of releasing the information.

Describe specifically and completely the known consequences of *not* releasing the information.

G. Instruct the person to sign the consent and enter the date on which the consent is signed.

H. As a general rule, a parent or guardian's signature should be obtained when the subject is under the age of 18 or has a legally appointed guardian; however, specific requirements for obtaining consent to release data in these circumstances vary. **Instructions for completing this portion of the form within your particular entity should be developed in consultation with the County Attorney's office.**

INFORMED CONSENT FOR THE RELEASE OF INFORMATION

I, _____

(Name of individual authorizing release)

authorize _____

(Name of individual, entity, or person holding record)

to disclose to _____

(Name of individual, entity, or person to receive the information)

the following information:

_____

for the purpose of:

_____

I understand that my records are protected under state and/or federal privacy laws and cannot be disclosed without my written consent unless otherwise provided for by state or federal law. I understand that once this data is released that it may be subject to further disclosure without my written consent. I also understand that I may revoke this consent at any time except to the extent that action has been taken in reliance on it and that in any event, this consent expires automatically in one year or as described below, whichever is earlier.

Specification of the date or condition upon which this consent expires:

_____

Executed this _____ day of _____ ,20 _____ .

_____

(Signature of individual authorizing release)

_____

(Signature of witness)

_____

(Signature of parent, guardian, or authorized representative, when required)

DATA PRACTICES NOTICE

I have been subpoenaed to testify before this court. I have been advised by the Office of the Aitkin County Attorney to provide the following information to the Court.

> "The data I have been requested to provide includes data which is classified as private data as defined by Minn. Statute Chapter 13, the Minnesota Government Data Practices Act. Pursuant to Minnesota Statute 13.03 and Minnesota Rule 1205.0100, Subp. 5, the Court's attention is called to this classification. The Data Practices Act requires that I may disclose this data only if the data subject has given written consent, a statute allows disclosure, or a court orders disclosure. If this court orders me to provide this private data, I will do so."

AITKIN COUNTY

PUBLIC DATA REQUEST FORM (APPENDIX A)

Right to Access Public Data
According to the Data Practices Act (Minnesota Statutes, Chapter 13), all government data are presumed to be public unless a state or federal law says otherwise. Government data is a term that means all the recorded information a government entity has, including paper, email, CDROMs, photographs, etc.

The Data Practices Act also provides that Aitkin County must keep all government data in a way that makes it easy for you, as a member of the public, to access. You have the right to look at all public data that we keep, free of charge; to get copies of public data, for which the Data Practices Act allows us to charge; and to look at the data, free of charge, before deciding to request copies.

How to Make a Data Request
To look at data or request copies of data that Aitkin County keeps, you must make a request directly to the department that maintains the data you are requesting. You may make your request by phone; or by mail, fax, or email using the Data Request Form (attached).

If you choose not to use the data request form, your request should include the following:
- State that you, as a member of the public, are making a request for data under the Data Practices Act, Minnesota Statutes, Chapter 13;
- Indicate whether you would like to look at the data, get copies of the data, or both; and
- Provide a clear description of the data you would like to inspect or have copied.

Aitkin County cannot require you, as a member of the public, to identify yourself or explain the reason for your data request. However, depending on how you want us to process your request (if, for example, you want us to mail you copies of data), we may need some information about you, such as your name and address. If you choose not to give us any identifying information, we will provide you with contact information so you may check on the status of your request. However, please keep in mind that if we do not understand your request and have no way to contact you, we will not be able to begin processing your request.

How We Respond to a Data Request
Upon receiving your request, we will begin to process it.
- If we do not have the data, we will notify you as soon as reasonably possible.
- If we have the data, but the data are not public, we will notify you as soon as reasonably possible, and state which specific law says the data are not public.
- If we have the data, and the data are public, we will respond to your request appropriately and within a reasonable amount of time, by doing one of the following:
  - arrange a date, time, and place for you to inspect data, at no charge, if your request is to look at the data, or
  - provide you with copies of the data as soon as reasonably possible. You may choose to pick up your copies, or we will mail or fax them to you. If you want us to send you the copies, you will need to provide us with an address or fax number. We will provide electronic copies (such as email or CD-ROM), upon request, if we keep the data in electronic format. Information about copy charges can be found in the County's current fee schedule, located on the County website. If the fee for fulfilling the request is greater than $5.00, pre-payment shall be required.

If you do not understand some of the data (technical terminology, abbreviations, or acronyms), please contact the person who provided it, so that he/she can explain it.

The Data Practices Act does not require us to create or collect new data in response to a data request, or to provide data in a specific form or arrangement if we do not keep the data in that form or arrangement. (For example, if the data you request are on paper only, we are not required to create electronic documents in response to your request.) If we do agree to create data for you, we will work with you on the details of your request, including cost and response time.

Requests for Summary Data

Summary data are statistical records or reports that are prepared by removing all identifying information from private or confidential data on individuals. The preparation of summary data is not a means to gain access to private or confidential data. Aitkin County will prepare summary data if you make your request in writing – you may use the Data Request Form attached – and pay for the cost of creating the data. We will respond within ten business days of receiving your written request with details of when the data will be ready, and how much we will charge for the data.

Data Practices Contacts

The following table provides contact information for the individuals who are responsible for responding to requests for data. The Responsible Authority is the individual responsible for establishing and overseeing data access processes. The Data Practices Compliance Official is the individual to whom questions about, or problems related to, data practices should be directed.

Office	**Responsible Authority, Data Practices Compliance Official and Designees**
County Attorney	Jim Ratz, County Attorney *Designee: Lisa Rakotz, Sr. Assistant County Attorney* 217 2nd Street NW, Room 231, Aitkin, MN 56431 218-927-7347; Fax 218-927-7365 jratz@co.aitkin.mn.us
County Auditor	Kirk Peysar, County Auditor *Designee: ~~Jonathan Knutson, Financial Assistant~~ Vacant* 209 2nd Street NW, Room 202, Aitkin, MN 56431 218-927-7354; Fax 218-927-7324 kpeysar@co.aitkin.mn.us
County Recorder	Michael Moriarty, County Recorder *Designee: Roxy Hoppe, Chief Deputy Recorder* 209 2nd Street NW, Room 205, Aitkin, MN 56431 218-927-7336; Fax 218-927-7324 mick.moriarty@co.aitkin.mn.us
County Treasurer	Lori Grams, County Treasurer *Designee: Julie Hughes, Chief Deputy Treasurer* 209 2nd Street NW, Room 203, Aitkin, MN 56431 218-927-7325; Fax 218-927-7357 lgrams@co.aitkin.mn.us
Sheriff	Dan Guida, County Sheriff *Designee: ~~John Drahota~~ Heidi Lenk, Undersheriff* 217 2nd Street NW, Room 185, Aitkin, MN 56431 218-927-7435; Fax 218-927-7359 dguida@co.aitkin.mn.us
All other County offices	*Responsible Authority and Data Practices Compliance Official:* Jessica Seibert, County Administrator 217 2nd Street NW, Room 130, Aitkin, MN 56431 218-927-3093; Fax 218-927-7374 jessica.seibert@co.aitkin.mn.us

All other County offices, cont.	*Designees:* Assessor's Office Mike Dangers, County Assessor 209 2nd Street NW, Room 111, Aitkin, MN 56431 218-927-7327, Fax 218-927-7379 mike.dangers@co.aitkin.mn.us Community Corrections Kami Genz, Director 204 1st Street NW, Aitkin, MN 56431 218-927-7281, Fax 218-927-2142 kami.genz@co.aitkin.mn.us Environmental Services / Planning & Zoning Department Terry Neff, Environmental Services Director 209 2nd Street NW, Room 100, Aitkin, MN 56431 218-927-7342; Fax 218-927-4372 tneff@co.aitkin.mn.us Economic Development Ross Wagner, Economic Development/Forestry Industry Coord. 217 2nd Street NW, Room 131, Aitkin, MN 56431 218-927-7305; Fax 218-927-7374 rwagner@co.aitkin.mn.us Health and Human Services Department Cynthia Bennett, HHS Director 204 1st Street NW, Aitkin, MN 56431 218-927-7200; Fax 218-927-7461 cynthia.bennett@co.aitkin.mn.us Highway Department John Welle, County Engineer 1211 Air Park Drive, Aitkin, MN 56431 218-927-3741; Fax 218-927-2356 jwelle@co.aitkin.mn.us Human Resources Department Bobbie Danielson, HR Director 217 2nd Street NW, Room 134, Aitkin, MN 56431 218-927-7306; Fax 218-927-7374 bobbie.danielson@co.aitkin.mn.us Information Technology Steve Bennett, IT Director 209 2nd Street NW, Room 118, Aitkin, MN 56431 218-927-7345; Fax 218-927-7369 sbennett@co.aitkin.mn.us

All other County offices, cont.	Land & Parks Department and Long Lake Conservation Center Rich Courtemanche, Land Commissioner 502 Minnesota Avenue North, Aitkin, MN 56431 218-927-7364; Fax 218-927-7249 rich.courtemanche@co.aitkin.mn.us Veterans Services Office Penny Harms, Veterans Services Officer 217 2nd Street NW, Room 130, Aitkin, MN 56431 218-927-7320; Fax 218-927-7309 penny.harms@co.aitkin.mn.us

AITKIN COUNTY

DATA REQUEST FORM
Members of the Public

Date of request: _____

I am requesting access to data in the following way:

☐Inspection ☐Copies ☐Both inspection and copies

Note: Inspection is free, but there is a charge for copies. If the fee for fulfilling the request is greater than $5.00, pre-payment shall be required.

These are the data I am requesting:

_____
_____
_____

Note: Describe the data you are requesting as specifically as possible. If you need more space, please use the back of this form.

Contact Information:

Name: _____

Address: _____

City: _____ State: _____ Zip: _____

Phone number: _____ Email: _____

Note: You do not have to provide any of the above contact information. However, if you want us to mail your requested data, we will need some type of contact information. In addition, if we do not understand your request and need to get clarification from you, without contact information, we will be unable to begin processing your request.

Aitkin County will respond to your request as soon as reasonably possible.

(For office use)	
Department /Division:	***Request handled by / Ext.:***
Method of response:	
Charges:	
Amt Due:	***Received by / Ext.:***

Additional Information:

_____
_____
_____

AITKIN COUNTY

DATA REQUEST BY SUBJECT OF DATA (APPENDIX B)

Data about You

According to the Data Practices Act (Minnesota Statutes, Chapter 13), data subjects have certain rights related to a government entity collecting, creating, and keeping government data about them. You are the subject of data when you can be identified from the data. Government data is a term that means all recorded information a government entity has, including paper, email, CDROMs, photographs, etc.

Classifications of Data about You

The Data Practices Act presumes that all government data are public, unless a state or federal law says otherwise. Data that is about you may be classified by state law as public, private, or confidential.

Public data: We must give public data to anyone who asks for it (e.g., the assessed value of your home is public data).

Private data: We cannot give private data to the general public, but you may have access when the data is about you (e.g., your Social Security number is private data). We may share your private data with you, with someone who has your written permission, with Aitkin County staff who need the data to perform an official function or duties, and as otherwise permitted by law or required by court order.

Confidential data: Confidential data have the most protection. Neither the public nor you can get access even when the confidential data are about you (e.g., if you register a complaint with a government entity concerning violations of state laws or local ordinances concerning the use of real property, your identity is confidential). We may share confidential data about you with Aitkin County staff who need the data to perform an official function or duty, and with others as permitted by law or court order. We cannot give you access to confidential data about you.

Your Rights under the Data Practices Act

Aitkin County must keep all government data about you in a way that makes it easy for you to access. We can collect and keep only that data about you that we need for administering and managing programs that are permitted by law.

As a data subject, you have the right to look at the public and private data that we keep about you, free of charge; the right to get copies of public and private data about you, for which the Data Practices Act allows us to charge an appropriate fee; and the right to look at data, free of charge, before deciding to request copies. If you ask, we will tell you whether we keep data about you and whether the data are public, private, or confidential.

As a parent, you have the right to look at and get copies of public and private data about your minor children (under the age of 18). As a legally appointed guardian, you have the right to look at and get copies of public and private data about an individual for whom you are appointed guardian. Minors have the right to ask Aitkin County not to give data about them to their parent(s) or guardian. If you are a minor, we will tell you that you have this right. We will ask you to put your request in writing and to include the reasons why we should deny your parents/guardian access to the data. Aitkin County will make the final decision about your request based on your best interests.

The Data Practices Act requires us to protect your data. We have established appropriate safeguards to ensure that your data are safe.

When we ask you to provide data about yourself that are not public, we must give you a data privacy notice (sometimes referred to as a Tennessen warning). This notice controls what we do with the data that we collect from you. Usually, we can use and release the data only in the ways described in the notice.

We will ask for your written permission if we need to use or release private data about you in a different way, or if you ask us to release the data to another person. If you want us to release data to another person, written authorization to do so must be provided to us.

When your data are inaccurate and/or incomplete, you have the right to challenge the accuracy and/or completeness of public and private data about you. You also have the right to appeal our decision. If you are a minor, your parent or guardian has the right to challenge the accuracy or completeness of data about you.

How to Make a Data Request

To look at data or request copies of data that Aitkin County keeps, you must make a written request directly to the department who maintains the data you are requesting. You may make your written request for data by mail, fax, or email, using the Data Request Form (copy attached).

If you choose not to use the Data Request Form, your written request must include:

- A statement that you are making a request for data under the Data Practices Act, Minnesota Statutes, Chapter 13, as a data subject, or as the parent/guardian of the data subject;
- Whether you would like to look at the data, get copies of the data, or both;
- A clear description of the data you would like to inspect or have copied; and
- Identifying information that proves you are the data subject, or the data subject's parent/guardian, as listed below.

Standards for Verifying Identity

- An **adult individual** must provide a valid photo ID, such as a state driver's license, a military ID, a passport, a state ID, or a state tribal ID
- A **minor individual** must provide a valid photo ID, such as a state driver's license, a military ID, a passport, a state ID, a state tribal ID, or a state school ID
- The **parent or guardian of a minor** must provide a valid photo ID *and either* a certified copy of the minor's birth certificate *or* a certified copy of documents that establish the parent or guardian's relationship to the child, such as: a court order relating to divorce, separation, custody, or foster care; a foster care contract; or an affidavit of parentage
- The **legal guardian for an individual** must provide a valid photo ID *and* a certified copy of appropriate documentation of formal or informal appointment as guardian, such as court order(s) or valid power of attorney
- An **attorney** requesting information on your behalf must send a request on his/her letterhead along with your express written consent; the request should be signed by both you and the attorney

Note: Individuals who do not exercise their data practices rights in person must provide *either* notarized or certified copies of the documents that are required *or* an affidavit of ID. (*This requirement does not apply to attorneys requesting data on your behalf.*)

How We Respond to a Data Request

Upon receiving your written request, we will begin to process it. If it is not clear what data you are requesting, we will ask you for clarification. If we do not have the data, we will notify you within 10 business days. If we have the data but the data are confidential, we will notify you within 10

business days, and state which specific law says you cannot access the data. If we have the data, and the data are public or private data about you, we will respond to your request within 10 business days. If your request is to look at the data, we will arrange a date, time, and place to inspect data.

After we have provided you with access to data about you, we do not have to show you the same data again for 6 months, unless there is a dispute or we collect or create new data about you. If you do not understand some of the data (technical terminology, abbreviations, or acronyms), please contact the person who provided it, so that he/she can explain it.

The Data Practices Act does not require us to create or collect new data in response to a data request, or to provide data in a specific form or arrangement if we do not keep the data in that form or arrangement. (For example, if the data you request are on paper only, we are not required to create electronic documents in response to your request.) If we do agree to create data for you, we will work with you on the details of your request, including cost and response time.

Charges for Copies of Data

We may only charge you the actual cost of making copies of data about you. This charge may include the following: employee time* to prepare and make copies (i.e. removing staples and paper clips, sorting data, labeling data, taking data to a copier and actually producing copies); actual cost of media used (e.g., paper, CD ROMs, DVDs, etc.); and mailing costs if you request the copies be mailed to you. We *may not* charge you the cost of searching for and retrieving the data, redacting confidential data or private data about others from your data, or sorting of data that is not necessary for copying of your data. The amount that is charged will be the same regardless of whether the request is made by you as the data subject, your parent/guardian, or by a representative to whom you have granted authorization to access your data.

* Employee time is calculated based upon the average wage of the lowest-paid Aitkin County employee who could complete the tasks necessary, plus the base cost of insurance benefits for that employee.

Data Practices Contacts

The following table provides contact information for the individuals who are responsible for responding to requests for data. The Responsible Authority is the individual responsible for establishing and overseeing data access processes. The Data Practices Compliance Official is the individual to whom questions about, or problems related to, data practices should be directed.

Office	Responsible Authority, Data Practices Compliance Official and Designees
County Attorney	Jim Ratz, County Attorney *Designee: Lisa Rakotz, Sr. Assistant County Attorney* 217 2nd Street NW, Room 231, Aitkin, MN 56431 218-927-7347; Fax 218-927-7365 jratz@co.aitkin.mn.us
County Auditor	Kirk Peysar, County Auditor *Designee: ~~Jonathan Knutson, Financial Assistant~~ Vacant* 209 2nd Street NW, Room 202, Aitkin, MN 56431 218-927-7354; Fax 218-927-7324 kpeysar@co.aitkin.mn.us
County Recorder	Michael Moriarty, County Recorder *Designee: Roxy Hoppe, Chief Deputy Recorder* 209 2nd Street NW, Room 205, Aitkin, MN 56431 218-927-7336; Fax 218-927-7324 mick.moriarty@co.aitkin.mn.us
County Treasurer	Lori Grams, County Treasurer *Designee: Julie Hughes, Chief Deputy Treasurer* 209 2nd Street NW, Room 203, Aitkin, MN 56431 218-927-7325; Fax 218-927-7357 lgrams@co.aitkin.mn.us
Sheriff	Dan Guida, County Sheriff *Designee: ~~John Drahota~~ Heidi Lenk, Undersheriff* 217 2nd Street NW, Room 185, Aitkin, MN 56431 218-927-7435; Fax 218-927-7359 dguida@co.aitkin.mn.us
All other County offices	*Responsible Authority and Data Practices Compliance Official:* Jessica Seibert, County Administrator 217 2nd Street NW, Room 130, Aitkin, MN 56431 218-927-3093; Fax 218-927-7374 jessica.seibert@co.aitkin.mn.us *Designees:* Assessor's Office Mike Dangers, County Assessor 209 2nd Street NW, Room 111, Aitkin, MN 56431 218-927-7327, Fax 218-927-7379 mike.dangers@co.aitkin.mn.us Community Corrections Kami Genz, Director 204 1st Street NW, Aitkin, MN 56431 218-927-7281, Fax 218-927-2142 kami.genz@co.aitkin.mn.us

All other County offices, cont.	Environmental Services / Planning & Zoning Department Terry Neff, Environmental Services Director 209 2nd Street NW, Room 100, Aitkin, MN 56431 218-927-7342; Fax 218-927-4372 tneff@co.aitkin.mn.us Economic Development Ross Wagner, Economic Development/Forestry Industry Coord. 217 2nd Street NW, Room 131, Aitkin, MN 56431 218-927-7305; Fax 218-927-7374 rwagner@co.aitkin.mn.us Health and Human Services Department Cynthia Bennett, HHS Director 204 1st Street NW, Aitkin, MN 56431 218-927-7200; Fax 218-927-7461 cynthia.bennett@co.aitkin.mn.us Highway Department John Welle, County Engineer 1211 Air Park Drive, Aitkin, MN 56431 218-927-3741; Fax 218-927-2356 jwelle@co.aitkin.mn.us Human Resources Department Bobbie Danielson, HR Director 217 2nd Street NW, Room 134, Aitkin, MN 56431 218-927-7306; Fax 218-927-7374 bobbie.danielson@co.aitkin.mn.us Information Technology Steve Bennett, IT Director 209 2nd Street NW, Room 118, Aitkin, MN 56431 218-927-7345; Fax 218-927-7369 sbennett@co.aitkin.mn.us Land & Parks Department and Long Lake Conservation Center Rich Courtemanche, Land Commissioner 502 Minnesota Avenue North, Aitkin, MN 56431 218-927-7364; Fax 218-927-7249 rich.courtemanche@co.aitkin.mn.us Veterans Services Office Penny Harms, Veterans Services Officer 217 2nd Street NW, Room 130, Aitkin, MN 56431 218-927-7320; Fax 218-927-7309 penny.harms@co.aitkin.mn.us

AITKIN COUNTY

DATA REQUEST FORM
Subject of Data

Date of request: _____

I am requesting access to data in the following way:

☐Inspection ☐Copies ☐Both inspection and copies

Note: Inspection is free, but there is a charge for copies. If the fee for fulfilling the request is greater than $5.00, pre-payment shall be required.

These are the data I am requesting:

_____

_____

_____

Note: Describe the data you are requesting as specifically as possible. If you need more space, please use the back of this form.

To request data as a data subject, you must show a valid state ID, such as a driver's license, military ID, or passport as proof of identity. To request data on behalf of the data subject, you must present proper written permission granting you such access.

Data Subject Name: _____

Address: _____

Phone number: _____ Email: _____

Parent/Guardian Name (if applicable): _____

Signature of Data Subject or Parent/Guardian: _____

Aitkin County will respond to your request within 10 days.

(For office use)	
ID provided:	
Department name:	***Request handled by:***
Method of response:	
Charges:	
Amt Due:	***Received by:***
Notes	