Worksheet for Developing Data Practices Policies & Procedures

This worksheet is intended to assist government entities in developing their required data practices policies and procedures under Minnesota Statutes, sections 13.025 and 13.03.

See: https://mn.gov/admin/data-practices/data/rules/policies/

Decision points, responsibilities, and Data Practices Office (DPO) recommendations are described in this italicized format.

Part 1: Identify Staff with Data Practices Responsibilities

Each government entity must designate or appoint an individual to be the responsible authority (RA) under Minnesota Statutes, section 13.02, subdivision 16, and Minnesota Rules 1205.1000.

- Entities seeking guidance in selecting an RA should look to language in Minnesota Rules 1205.0200, subparts 12 – 15, and Minnesota Statutes, section 13.46, subdivision 10.
- More information: https://mn.gov/admin/data-practices/data/contacts/. Sample forms to use for appointing an RA are in Minnesota Rules 1205.2000.

Who is your responsible authority?

Minnesota Statutes, section 13.05, subdivision 13, requires all RAs to appoint or designate a data practices compliance official (DPCO).

- The RA and DPCO may be the same person.
- The DPCO must be a government entity employee who assists with data practices related issues.

Who is your DPCO?

Minnesota Statutes, section 13.03, subdivision 2, allows RAs to appoint one or more designees. The definition of designee is in Minnesota Statutes, section 13.02, subdivision 6.

Has your RA appointed/designated any staff to be data practices designees?

Who are they?

If listed in your policy, you can require data requesters to make requests to specific designees. The RA may appoint the DPCO as the designee for all data requests.

Do you want to direct requesters to specific designees depending on what data are requested?

If yes, list name and type of data for which designee is responsible. If no, all requests should be directed to the RA.

By law, all data requests must be made to the RA or designee; however, you need to make decisions about how your specific entity will handle requests in a way that ensures you respond within the statutory time frames. For example, once a data request is made to the RA, will the RA handle the request, or will the RA give all requests to the DPCO or another staff person to coordinate responses? Regardless of which staff person actually manages a data request, the RA ultimately is responsible.

Name and contact information for these staff members should be listed in the Data Practices Contacts page in your policies.

Part 2: Set Parameters for Data Requests

The Data Practices Act does not require that individuals make data requests in writing; however, DPO recommends that government entities make this their policy. If you decide to require written requests, you must include it in your Data Practices Policy (see Advisory Opinion 01-014).

Do you want to require requesters to make their data requests in writing?

If you decide not to require written requests, you should still have some system of documenting data requests made verbally.

If you require that data requests be made in writing, will you allow requests by mail, fax, and/or email?

If you allow for data requests to be made by email, do you have a central location where email messages are sent that can be accessed by more than one staff person?

Minnesota Statutes, section 13.05, subdivision 5, requires that all government entities establish appropriate security safeguards for all records containing data on individuals.

When an individual requests data about him/herself, you must verify that the requester is the data subject or the data subject's parent or guardian.

You should know how you verify someone's identity and it is good practice to document how you made the verification.

Part 3: Respond to Data Requests

Timeframes

The Data Practices Act provides the timeframes for responding to data requests.

- Entities must respond to members of the public seeking public data in an appropriate and prompt manner (section 13.03), and within a reasonable time (Minnesota Rules 1205.0300).
- Entities must respond to data subjects seeking access to data about them within ten business days (section 13.04).
    - In other words, entities must either provide the data to the data subject or inform the data subject there are no data available within ten business days.
    - This does not mean that an entity cannot arrange for a longer period of the time to respond, as long as the data subject agrees.

DPO recommends that entities respond to all data requests in writing.

Charging for copies of data

The Data Practices Act allows, but does not require, government entities to charge for copies of data.

Some entities choose an amount below which it is not cost effective to charge for copies. Check with your entity's financial department to find out if there is such an amount.

Do you have a dollar figure below which you will not charge for copies? If yes, what is the amount?

Government entities may require pre-payment for copies of data if documented in the Data Practices Policy (see Advisory Opinion 04-068).

Will you require pre-payment for copies?

If you decide to charge for copies of data, the allowable amount depends upon whether the person requesting the data is the data subject or a member of the public**.**

Members of the public

- For 100 or fewer black and white paper copies, the maximum amount government entities can charge is 25¢ per page.
- For more than 100 black and white paper copies and most other types of copies (photographs, audiotapes, data on a CD or DVD, data stored electronically, etc.) government entities can charge only the actual cost of employee time to: (1) search for and retrieve the data and (2) make the copies (see also Minnesota Rules 1205.0300).
    - When a requester asks that the data be sent electronically (e.g., via email), the copy charge may include the actual cost of sending the data.
    - When calculating employee time for making the copies, you should use the hourly wage of the lowest-paid employee who is able to search for, retrieve, and make the copies. (Note: Your actual cost could be less than 25¢ per page.)

If you charge members of the public for copies, DPO recommends re-calculating actual costs on an annual basis and documenting this calculation.

More information about charging members of the public for copies: https://mn.gov/admin/data-practices/data/rules/copy-costs/.

Are there statutes, other than Minnesota Statutes, section 13.03, that set specific copy charges for your data? If yes, cite the statute and corresponding fee(s).

For example, under Minnesota Statutes, section 144.226, subdivisions 1, 3, and 4, the Minnesota Department of Health charges $16 for a certified copy of a birth certificate. Under Minnesota Statutes, section 169.09, the Commissioner of Public Safety charges certain persons $5 for a copy of an accident report.

Data subjects

When a data subject asks for copies, a government entity may charge the actual cost for an employee to make paper copies or to provide copies of electronically stored data (see also Minnesota Rules 1205.0300 and 1205.0400). When calculating employee time for making the copies, you should use the hourly wage of the lowest-paid employee who is able to make the copies. (Note: government entities may not charge for search and retrieval time if a data subject requests copies.)

Part 4: Creating New Data

Requests to create new data not already collected or maintained by a government entity fall outside the requirements of the Data Practices Act. So, you are not required to create data to respond to a data request. If you choose to create data, DPO recommends working with the requester on a case-by-case basis.

Part 5: Summary Data

This section applies only to the Model Policy for the Public.

Definitions

Minnesota Statutes, section 13.02, subdivision 19, defines summary data and Minnesota Statutes, section 13.05, subdivision 7, discusses the preparation of summary data. Section 13.05 requires an RA to prepare summary data if the request is made in writing and the cost of preparing the summary data is paid for by the requester. Section 13.05 also allows the RA to delegate the preparation of summary data.

Responding to summary data requests

Minnesota Rules 1205.0700 discusses requirements for responding to summary data requests and preparing summary data. Subpart 3 requires RAs to prepare and implement summary data access procedures. Subpart 4 requires government entities to respond to summary data requests within ten days.

Nondisclosure agreements

Minnesota Rules 1205.0700, subpart 5, discusses the requirements of a nondisclosure agreement.

Part 6: Parent Access to Private Data about Minor Children

This section applies only to the Model Policy for Data Subjects.

Based on the definition of "individual" in Minnesota Statutes, section 13.02, subdivision 8, parents and guardians generally are entitled to the same data practices rights as their minor children. However, Minnesota Rules 1205.0500 discusses that a minor has the right to ask that his/her private data not be released to his/her parent or guardian. The rules provide guidance to government entities about responding to a minor's request to limit access to data about him/her. (Note: government entities may not deny parents/guardians access to educational data that are maintained by an educational agency or institution.)

Document your policy or practice for notifying minors that they have a right to request that you not release their private data to their parent or guardian. For each situation where you receive a request from a minor, document how/why you made the determination to withhold or release.

Part 7: Tennessen Warning Notices

This section applies only to the Model Policy for Data Subjects.

Minnesota Statutes, section 13.04, subdivision 2, discusses the notice that government entities must provide to an individual when collecting private and/or confidential data about that individual from that individual. This notice is commonly referred to as a Tennessen warning.

With limited exceptions, you may not collect, store, use or disseminate private or confidential data for any purpose other than those you specified in the Tennessen warning notice. Because the consequences of not giving a proper notice are so severe, you must tailor your notices to your entity's specific programs.

DPO suggests you seek legal advice when developing your notices.

More information about Tennessen warning notices: https://mn.gov/admin/data-practices/data/warnings/tennessen/.

Part 8: Informed Consent

Minnesota Statutes section 13.05, subdivision 4, and Minnesota Rules 1205.1400, discuss informed consent. You must create legally-valid consent forms.

More information about informed consent requirements: https://mn.gov/admin/data-practices/data/warnings/consent/.

Will you require data subjects to use only the consent forms your entity has created or will you release data pursuant to a consent form created by another entity?

Part 9: Keep Data Secure

This section applies only to the Model Policy for Data Subjects.

Minnesota Statutes, section 13.05, subdivision 5, requires that all government entities:

- Establish procedures to assure that all data on individuals are accurate, complete, and current for the purposes for which the data were collected.
- Establish appropriate security safeguards for all records containing data on individuals, including procedures for ensuring that data that are not public are accessible only to persons whose work assignment reasonably requires access to the data, and are accessed only by those persons for purposes described in the procedure.
- Develop a policy incorporating these procedures, which may include a model policy governing access to the data if sharing of the data with other government entities is authorized by law.

Minnesota Rules 1205.0400 states that private data are accessible to individuals within a government entity whose work assignments reasonably require access.

DPO has guidance on its website that discusses how entities can meet these requirements.

Minnesota Statutes, section 13.055, requires government entities to notify data subjects when a "breach of the security of the data" has occurred and an unauthorized person has gained access to data.

DPO recommends documenting your policy or practice for meeting the requirements in section 13.055 and has guidance on its website about those requirements.

Part 10: Create, Update, and Post Policies

Minnesota Statutes, section 13.025, requires government entities to create policies that describe the processes members of the public and data subjects need to follow when requesting data.

Government entities should update their policies yearly. Particularly, entities should update the data practices contact information (to be consistent with staff changes) and make sure the hourly wage rates they use for determining actual copy charge costs are current.

Have you updated your access documents within the last year?

Minnesota Statutes, section 13.025, subdivision 4, requires that government entities make their policies easily available to the public by distributing free copies, or by posting a copy on the government entity's website.

Do you have free copies available for the public, or have them posted at your website?

Government Entity Decision Checklist

To complete the Model Policy for the Public and Model Policy for Data Subjects, your entity must make the following decisions. *Indicates a specific obligation under Chapter 13.

Decision Point
Do we have an RA? *
Do we have any designees?
Do we have our policies available for distribution, or have them posted within our entity? *
Do we direct data requesters to staff, other than the RA, for response to data requests?
Do we require written requests?
If requests must be in writing, do we allow requests by mail, fax, and/or email?
Do we have a policy to verify a data subject's identity? *
Do we respond to data requests in writing?
Are there statutory provisions outside of Chapter 13 that give us authority to charge specific costs for copies of data?
If we charge for copies of data, do we have a minimum amount before we charge?
If we charge for copies of data, do we require pre-payment?
Do we have a policy for creating new data?
Do we have a written policy describing our policy/practice for notifying minors that they have the right to ask us to withhold their private data from their parents/guardians? *
Do we have a written policy describing our policy/practice for evaluating a minor's request? *
Each time we evaluate a minor's request, do we document how we make our decision? *
Do we require that individuals use our consent forms?
Do we have a written policy/practice on how we keep data on individuals secure?*
Do we have a written policy/practice detailing which staff has access to private and/or confidential data?*
Have we documented our policy/practice on how we will handle a breach in security of private or confidential data?
When did we last update our access documents? *