

Responding to data requests

General Counsel's Office – Privacy Office

Policy Number: 8236.600
Initial Date: 5/14/2025
Effective Date: 6/10/2025
Issue Date: 6/10/2025

POLICY:

All DHS employees must respond to data requests in compliance with the Minnesota Government Data Practices Act (MGDPA).

AUTHORITY:

[Minnesota Statutes, section 13.025, "MGDPA – Government Entity Obligation"](#)

[Minnesota Statutes, section 13.03, "Access to Government Data"](#)

APPLICABILITY:

DHS-wide excluding Direct Care and Treatment

Staff may be subject to disciplinary action, up to and including termination, for failure to comply with policies.

PURPOSE:

To provide consistent practices for evaluating and responding to data requests within the scope of the MGDPA, and to ensure compliance with Minnesota Statutes and Minnesota Rules regarding data practices.

DEFINITIONS:

Business area designee: an employee within a business area that has no assigned data liaison and that holds the data that the public seeks.

Copy: a photocopy produced by a copy machine, or a printed page produced by a printer. A paper copy is one side of a sheet of standard (letter or legal) paper. A two-sided copy counts as two copies. An electronic copy is data provided to a requesting party in an electronic format or by an electronic media, including data provided on CDs, flash drives or diskettes and data sent via email in response to a request for data.

Data liaison: employee(s) appointed by business areas who are responsible for responding to data requests.

Data on individuals: all government data in which any individual is or can be identified as the subject of that data.

Data request: requests for any government data under the MGDPA. Paper documents, electronic documents, email, videotape, and computer files are all forms of “data.” Data requests do not include requests to answer questions or to create new data. The MGDPA governs two types of data requests:

- requests from individuals seeking their own data; and
- requests from members of the public seeking public data. Requests for public data from legislators and media are considered requests from members of the public.

Data subject: any individual is or can be identified as the subject of that data.

Government data: all data collected, created, received, maintained, or disseminated by any government entity regardless of its physical form, storage media or conditions of use.

Government entity: means a state agency, statewide system, or political subdivision.

Individual: means a natural person. In the case of a minor or an incapacitated person, “individual” also includes a parent or guardian or an individual acting as a parent or guardian. However, DHS must 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 DHS determines that withholding the data would be in the best interest of the minor.

Minnesota Government Data Practices Act (MGDPA): governs access to data that is collected, created, stored, maintained, or disseminated by state agencies.

Private data on individuals: data made by statute or federal law applicable to the data: (a) not public and (b) accessible to the individual subject of those data.

Public data: data accessible to the public.

Preparation of summary data: time spent removing identifying information (private data) to create summary (public) data from private data.

Record custodian: The individual (role) or business unit responsible for managing a record.

Redaction: the process of reviewing and removing not public data. Redaction does not include removing identifying information from private data and replacing the identifying data with a unique identifier to facilitate analysis of a variety of data elements.

Searching and retrieving: time spent identifying and reviewing files, databases, or other storage devices (paper or electronic) to locate data or to determine whether data exists to respond to a request and retrieving the relevant data. Retrieving data also includes creating, specifying, and executing a data warehouse query, reviewing the results for accuracy, and putting the data into a readable format.

Sorting data: time spent organizing the data, removing, or inserting staples, paper clips, placing the data in folders, transporting the data to a location for viewing or inspection and related tasks.

Summary data: statistical records and reports derived from data on individuals but in which individuals are not identified and from which neither their identities nor any other characteristic that could uniquely identify an individual is ascertainable.

PROCEDURES:

A. Data requests

1. Individuals may request to inspect or obtain copies of information or data maintained and stored by DHS by submitting any of the following ways to dhs.datarequest@state.mn.us:
 - a. a written request;
 - b. the [Request for Private Data about Yourself form \(DHS-7338\)](#); or
 - c. the [Request for Public Data form \(DHS-7337\)](#).
2. Media may request to inspect or obtain copies of information or data maintained and stored by DHS by submitting to the [DHS Contacts for reporters](#).

- B. DHS staff who receive a data request under the Minnesota Government Data Practices Act (MGDPA) must forward the request to the DHS centralized data request email inbox at dhs.datarequest@state.mn.us.
- C. DHS staff who receive a data request outside the scope of the MGDPA, including requests from law enforcement, external auditors, the Governor's Office, and requests for data between DHS business areas will forward the request to the specific area/division manager or a general counsel's office contact.
- D. DHS staff who receive requests to answer questions or who are asked to create new data not already collected or maintained by DHS are not required to respond to these as data requests under this policy and the MGDPA. In these situations, staff must consult with the specific area/division manager or a general counsel's office contact before responding or creating data.

E. Roles and responsibilities

1. The data privacy office/designee will:
 - a. log the data request in the [Centralized Data Practices Tracking Log \(agile app\)](#); and
 - b. assign the data request to the designated data liaison(s) or in the case where there are no data liaison(s), to a business area designee(s).
2. Data liaisons must respond to the requester acknowledging that DHS has received the request and include: (as applicable)
 - a. a statement that there is no data responsive to the request;
 - b. an explanation of the requirement for verifying of identification or authorization;
 - c. an estimate of the cost of the data responsive to the request or a description of the process for inspection;
 - d. a request for clarification of data being requested; or
 - e. an update on the status of the request.
3. Record custodians must:
 - a. conduct a reasonable search to locate responsive data; and
 - b. review all data to ensure that the data may be disclosed to the requester.

- 1) For requests from a person seeking their own data, review the data to ensure that it does not contain private data on any other person or any other data that may not be legally disclosed.
 - 2) For requests from a member of the public seeking public data, review the data to ensure that it only contains data that is classified as public under state and federal law.
4. The data liaison/business area designee(s) will:
- a. in collaboration with the record custodian, review, redact or remove data that may not be disclosed to the requester pursuant to state or federal law, utilizing:
 - 1) [Guide to reviewing documents for public data requests \(DHS-7280\)](#);
 - 2) [DHS policy 4200.525, "Protecting Not Public Data"](#);
 - 3) [DHS policy 4200.630, "Safeguarding Federal Tax Information \(FTI\)"](#); and
 - 4) [DHS policies, "Health Insurance Portability and Accountability Act."](#)
 - b. send the releasable data to the requester:
 - 1) If there is a cost, provide the data upon receiving the payment; or
 - 2) If there is no cost, provide the data when available.
 - c. log the information regarding the data request in the Centralized Data Practices Tracking Log (agile app).

F. Processing Not public data requests

1. Data liaison and business area staff determines the requester's authority to access the data.
 - a. If the requester is not authorized to receive the requested data, provide the statute that explains why the requested data cannot be disclosed.
 - b. For requests from third parties to access data on an individual, the requester must provide proper written authorization or consent to access their information. If the requester does not provide an authorization, direct the third-party requester to complete the [General Consent/Authorization to Release Information \(DHS-3549\)](#)
2. Verification of identity
 - a. For people seeking private data, data liaison and business area staff verifies the person is who they say they are. To verify the requester's identity, direct the requester to complete and return the [Verification of Identity and Request for Information form, DHS-4259-ENG \(PDF\)](#). Other ways to verify identity are discussed in the [Guide for Requesting Data About You \(PDF\)](#).
 - b. A person seeking their own data may have authorized representatives, guardians or others who may exercise the same rights as the person. The relationship to the person and authority of the requester to access the person's data must be verified before any private data is provided.
 - c. If a person refuses or cannot verify their identity, data liaison denies the data request.

3. Timeline

a. DHS must either:

- 1) provide the data to the data subject or inform the data subject there is no data available within ten business days; or
- 2) arrange for a longer period of the time to respond, if the data subject agrees.

b. DHS will promptly respond to data requests for private data about others if the requester provides proper written authorization or consent.

4. Estimation of Cost: Refer to [Guide to Responding to Data Requests](#).

G. Responding to Requests for Public

1. Data liaison and business area staff do not need to verify the identity of or the authority for a requester seeking public data.
2. Timeline: DHS will respond to data requests seeking public data within a reasonable amount of time.
3. Estimation of Cost: Refer to Guide to Responding to Data Requests.

H. Summary Data

1. Assigned DHS employees will prepare summary data if the request is made in writing and the cost of preparing the summary data is paid for by the requester.
2. Timeline: Within ten days of the receipt of a request, the data liaison will either:
 - a. inform the requester of the estimated costs: (Refer to Guide to Responding to Data Requests);
 - b. provide a written statement to the requester describing a timeline for preparing the requested summary data including reasons for any delays;
 - c. provide a written statement to the requester stating reasons why the requester's access would compromise the private or confidential data; or
 - d. provide access to the private or confidential data for the purpose of the requester's preparation of summary data under an agreement or contract (Refer to Minnesota Statutes, section 13.05, subdivision 7, and Administrative Rule 1205, subpart 5).
3. The data liaison will provide the compiled summary data
 - a. If there is a cost, provide the data upon receiving the payment; or
 - b. If there is no cost, provide the data when available.

I. Inspection

1. DHS may not charge anyone to inspect data responsive to a data request.
2. The DHS data liaison will arrange for the inspection at a date, time during business hours and place within DHS with the requester.

3. The data requester may not take the DHS copies without first paying the costs to make copies. (Refer to Guide to Responding to Data Requests).

REVIEW:

Annual

REFERENCES:

[Information privacy \(InfoLink\)](#)

[DHS policy 4200.525, "Protecting Not Public Data" \(PDF\)](#)

[DHS policy 4200.630, "Safeguarding Federal Tax Information \(FTI\)" \(PDF\)](#)

[DHS policies, "Health Insurance Portability and Accountability Act" \(Webpage\)](#)

[Minnesota Government Data Practices Act \(MGDPA\), Minnesota Statutes, Chapter 13](#)

[Minnesota Administrative Rules, Chapter 1205, "Data Practices"](#)

ATTACHMENTS:

[Centralized Data Practices Tracking Log \(AgileApp\)](#)

[General Consent/Authorization to Release Information DHS-3549 \(PDF\)](#)

[Guide for members of the public requesting public data DHS-6554 \(PDF\)](#)

[Guide for Requesting Data About You DHS-6553 \(PDF\)](#)

[Guide to Responding to Data Requests DHS-7408 \(PDF\)](#)

[Guide to reviewing documents for public data requests DHS-7280 \(PDF\)](#)

[Request for Private Data about Yourself form DHS-7338 \(PDF\)](#)

[Request for Public Data form DHS-7737 \(PDF\)](#)

[Verification of Identity and Request for Information form DHS-4259 \(PDF\)](#)

SUPERSESION:

Any memos, or other communications whether verbal, written, or transmitted by electronic means regarding this topic.



Amy Akbay, General Counsel
Department of Human Services
General Counsel's Office