

What do I need to know?

This section provides general guidelines for managing and handling private and public data. For more specific information on data privacy laws and requirements, consult with your HR Generalist Team.

The **Minnesota Government Data Practices Act** regulates the collection, creation, storage, maintenance, dissemination, and access to government data. It establishes a presumption that government data are public and are accessible by the public for both inspection and copying unless there is a federal law, a state statute, or a temporary classification of data that provides that certain data are not public.

One exception to the presumption that government data are public involves personnel data. Most personnel data is private data and can only be made available to individuals within the City of Minneapolis whose work assignments reasonably require access to the data.

Some examples of public and private data are as follows:

Public Data:

Name and Employee Identification #
Department and funding source
Job description, duties and responsibilities
Dates of appointment and separation
Job classification & range of pay
Gross salary, rate of pay and pay frequency
Time Worked
City paid fringe benefits
Retirement plan

Private Data:

Social Security Number
Marital status, tax exemptions and taxes withheld
Voluntary and involuntary deductions
Net pay
Home address and phone number
Ethnicity and gender data
Performance evaluation details
Medical history
Designee for final paycheck

IMPORTANT: All personnel data maintained on an undercover law enforcement officer is private.

What is my responsibility?

As a City of Minneapolis employee with access to both public and private personnel data, you accept responsibility for handling personnel data with sensitivity and in accordance with the Minnesota Government Data Practices Act. Improper or unauthorized use of private personnel data could result in disciplinary action and liability to the City. Following are some general guidelines to follow:

- It is the responsibility of all personnel to protect against the unauthorized disclosure of private personnel data
- Only authorized users may have access to private personnel data and that access is based upon a legitimate “need to know”
- Private personnel data could be disclosed in electronic form, on paper or verbally. All personnel shall protect the integrity and security private personnel data from unlawful disclosures. (e.g., private data should not be left unattended in meeting rooms or in open view on an individual’s desk if someone who does not have a need to know the information could view the data)
- Managers who identify a proxy to perform HR related activities on their behalf have not relinquished any responsibility for protecting private personnel data. Managers accept responsibility of the actions taken by their proxies.