

Guide for TRA Members Regarding Their Personal TRA Data and Information

This guide describes the rights of TRA members, retirees, survivors, disabilitants and former members with respect to their personal data and information which TRA collects and maintains. This guide also describes how TRA protects the privacy of the personal member data it collects and manages. TRA's practices with respect to the treatment of member data are governed by the Minnesota Government Data Practices Act.

TRA Data Classification

The Minnesota Government Data Practices Act (Chapter 13) regulates the collection, creation, storage, maintenance, dissemination, and public access to government data. That state law establishes a presumption that government data are public and are accessible to the public for both inspection and copying unless there is federal or state law that classifies the data differently.

In the case of TRA, the Data Practices Act narrows considerably the TRA data that are considered public and available to the public. Minnesota Statutes 13.43, Subd. 2a, states: "with respect to data collected and maintained on members, survivors, and beneficiaries by statewide retirement systems that is classified as public data in accordance with subdivision 2, those retirement systems may be only required to disclose name, gross pension, and type of benefit awarded." Additional sections of the Data Practices Act (13.63 and 13.355) further specify that social security numbers are considered private as are certain data on beneficiaries and survivors of TRA members to include: address, birth date, direct deposit account number, and tax withholding data.

TRA Protection of Member Data

Based on these state statutes, TRA takes steps to protect and restrict access to all personally identifiable member data and information other than name, gross pension amount (once awarded) and type of benefit (e.g., pension, survivor, disability or refund benefit). Examples of private member data which TRA protects from unauthorized access and improper disclosure include: social security number, address, birth date, bank account information, tax withholding information, medical records, and benefit applications. The steps TRA takes to protect member data include:

- Having a comprehensive Data Privacy Policy designed to protect the privacy of member data
- Training and requiring all TRA staff, consultants or outside contractors to follow certain operational procedures in working with member data and auditing compliance with those procedures
- Designating a TRA Data Compliance Official who is responsible for classifying data, maintaining a Data Inventory and periodically assessing data security
- Following procedures for verifying the identity of requesters of member data
- Establishing a data security breach policy and procedures

Rights of TRA Members under Data Practices Act

As subjects of TRA data, TRA members have the following rights:

- The right to look at (inspect), free of charge, the member's own personal data that TRA maintains in its data records and systems. Members can acquire copies of this data and TRA is permitted to charge for copies.
- If TRA asks members to provide private or confidential data, TRA will inform the member of the purpose for requesting the data, how it will be used, the member's right to refuse to provide the data, the consequences of refusing to provide the data, and the identity of anyone authorized by law to receive the data.
- TRA will ask written permission of the member before it uses or releases personal private data to an outside party or to another person whom the member designates as a personal representative. See attached consent form.
- The Data Practices Act requires TRA to protect member data. In accordance with that law, TRA has implemented safeguards to ensure member data are safe from unauthorized access and improper disclosure. In the unfortunate event, that a data security breach occurs and an unauthorized person gains access to member data, TRA will notify the subject of the data breach and provide a report that describes the data breach, the name of TRA employee associated with the breach and any disciplinary action taken.
- TRA members have the right to contest the accuracy or completeness of data about them by notifying TRA in writing. TRA will take action within 30 days to correct the data or notify the member that TRA believes the data are accurate. The member has a right to appeal that TRA decision to the TRA Board of Trustees.

Member Requests for Personal Data

TRA members may make a written request to look at or have copies of their own personal data that TRA keeps about the member or about the member's minor children. Individuals who have been appointed legal guardian or who serve as a personal representative of the member may also make such a request for data to TRA's Data Compliance Official: Jay Stoffel, TRA Deputy Executive Director, TRA, 60 Empire Drive, Suite 400, St. Paul, MN 55103; info@minnesotatra.org. A written request may be made by mail or email. The data request form attached to this guide is provided for the data requester's convenience. If the data request form is not used, the written request should contain a clear description of the data requested and whether inspection or copies of the data or both inspection and copies are being requested. The request form must include identifying information that proves the member is the data subject or the data subject's parent/guardian/personal representative.

TRA requires proof of identity before responding to requests for personal data. If a member is requesting data about a minor child, the member must show proof that member is the minor's parent. If a member's guardian or personal representative seeks data, legal documentation must be provided.

How TRA Responds to a Member Request for Personal Data

Upon receiving a written request from a member to look at or have copies of their own personal data that TRA keeps about the member, TRA will process the request and may ask for clarifying information if necessary.

- If TRA does not have the data, TRA will notify the requester in writing within 10 business days.
- If TRA has the data, but the data about you are confidential (meaning neither the public nor the member can have access due to statute or federal law), then TRA will notify the member in writing within 10 business days and state what specific law prevents disclosure of the data.

- If TRA has the data, TRA will respond to the request within 10 business days by doing one of the following:
 - Arrange a date, time and place for inspection of the data or
 - Provide the member with copies of the data within 10 business days. The member may choose to pick up the copies or receive them by mail or fax or in electronic form.

After providing the member access to the data and explaining its content, TRA does not have to provide the data again for six months unless there is a dispute or new data about the member is collected by TRA.

The Data Practices Act does not require TRA to create or collect new data in response to a data request if TRA does not already have the data nor does the Act require TRA to provide data in a specific form or arrangement if TRA does not keep the data in the form or arrangement.

TRA Data Request Form – For Members (Data Subjects)

Date of request:

To request data as a data subject, you must show valid ID, such as a driver's license, military ID, or passport as proof of identity.

I am requesting access to data in the following way:

Inspection

Copies

Both inspection and copies

Describe the data being requested in as much detail as possible. (If more space is needed, use the back of this form.)

Contact Information for the Data Request

Data Subject Name:

Parent/Guardian Name (if applicable):

Address:

Phone Number or Email:

Signature of Data Subject or Parent/Guardian:

Staff Verification

Identification provided:

Signature of TRA Employee who processed this request: