



Data Practices Policy: Your Rights as a Data Subject

This policy is required by Minnesota Statutes, sections 13.025 and 13.03 (2017), and was adopted by the Minnesota Board of Cosmetology on October 16, 2017. The intent of this policy is to provide the public with an agency-specific guide related to data practices and is not intended to provide specific or general legal advice.

1000 University Avenue W, Suite 100
Saint Paul, MN 55104
651-201-2742
cosmetology@state.mn.us
mn.gov/boards/cosmetology

What is a “Data Subject”?

When government has information recorded in any form (paper, hard drive, voicemail, video, email, etc.), that information is called “government data” under the Government Data Practices Act (Minnesota Statutes, Chapter 13). When we can identify you in government data, you are the “data subject” of that data. The Data Practices Act gives you, as a data subject, certain rights. This policy explains your rights as a data subject, and tells you how to request data about you, your minor child, or someone for whom you are the legal guardian.

When the Board Has Data about You

The Minnesota Board of Cosmetology has data on many people, such as licensees, registrants, applicants, salons, schools, continuing education providers, and more. We can collect and keep data about you only when we have a legal purpose to have the data. The Board must also keep all government data in a way that makes it easy for you to access data about you.

Government data about an individual have one of three “classifications.” These classifications determine who is legally allowed to see the data. Data about you are classified by state law as public, private, or confidential. Here are some examples:

Public Data

The Data Practices Act presumes that all government data are public unless a state or federal law says that the data are not public. We must give public data to anyone who asks. It does not matter who is asking for the data or why the person wants the data. The following are examples of public data about you that we might have:

- Your name and contact information, if you are a licensee, registrant, or applicant.
- Your license history, including various license types, issue dates, and expiration dates, including executed orders from formal discipline or inspection penalties and fines.
- The professional liability and workers compensation insurance policy information for your salon.
- Inspection reports for your salon, including designated licensed salon manager name and any rule violations or citations.

Private data

We cannot give private data to the general public. We can share your private data with you, with someone who has your permission, with our government entity staff whose job requires or permits them to see the data, and with others as permitted by law or court order. The following are examples of private data about you that we might have:

- Your social security number.
- Your application information prior to licensure.
- Any information pertaining to a complaint on you, if an executed order has not been signed.

Confidential Data

Confidential data have the most protection. Neither the public nor you can access confidential data even when the confidential data are about you. We can share confidential data about you with our government entity staff who have a work assignment to see the data, and to others as permitted by law or court order. The following is an example of confidential data about you:

- Active investigative data relating to the investigation of complaints against you.

To view the board's inventory of not public data, visit mn.gov/boards/cosmetology.

Your Rights Under the Government Data Practices Act

Access to Your Data

You have the right to look at or obtain copies of public and private data that we keep about you. The Data Practices Act allows us to charge for copies and compilation of data. You have the right to look at data, free of charge, before deciding to request copies. Also, 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 or legally appointed guardian, you have the right to look at and get copies of public and private data about your minor children (under the age of 18) or an individual for whom you are appointed guardian.

Minors have the right to ask us not to give data about them to their parent 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 that we should deny your parents or legal guardians access to the data. We will make the final decision about your request based on your best interests.

When We Collect Data From You

When we ask you to provide data about yourself that are not public, we must give you a notice called a Tennessee Warning. The 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. This permission is called informed consent.

Protecting Your Data

The Data Practices Act requires us to protect your data. We have established appropriate safeguards to ensure that your data are safe. In the unfortunate event that we determine a security breach has occurred and an unauthorized person has gained access to your data, we will notify you as required by law.

When Your Data are Inaccurate 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 data about you.

How to Make a Request For Your Data

You can ask to look at data at our offices, or ask for copies of data that we have about you, your minor child, or an individual for whom you have been appointed legal guardian.

All requests must be made in writing. We recommend using the sample **Data Request Form – Data Subjects** on page 7.

If you do not choose to use the data request form, your request should:

- Say that you are making a request as a data subject, for data about you (or your child, or person for whom you are the legal guardian), under the Government Data Practices Act (Minnesota Statutes, Chapter 13).
- Include whether you would like to review the data, have copies of the data, or both.
- Provide a clear description of the data you would like to review or have copied.
- Provide proof that you are the data subject or data subject's parent/legal guardian.

We require proof of your identity before we can respond to your request for data. If you are requesting data about your minor child, you must show proof that you are the minor's parent. If you are a legal guardian, you must show legal documentation of your guardianship. Please see the Standards for Verifying Identity on page 8. If you do not provide proof that you are the data subject, we cannot respond to your request.

Copy and Compilation Costs When You Request Public Data

Minnesota Statutes, section 13.03, subdivision 3(c) allows us to charge for copies. All payments must be received prior to release of the data.

The charge for most other types of copies and data requests, when a charge is not set by statute or rule, is the actual cost of searching for and retrieving the data, and making the copies or electronically sending the data.

In determining the actual cost of making copies, we include employee time, the cost of the materials onto which we are copying the data (paper, CD, DVD, etc.), and mailing costs (if any). If your request is for copies of data that we cannot copy ourselves, such as photographs, we will charge you the actual cost we must pay an outside vendor for the copies. The cost is \$29.25 per hour with a minimum cost of \$29.25.

If, based on your request, we find it necessary for a higher-paid employee to search for and retrieve the data, we will calculate search and retrieval charges at the higher salary/wage.

How We Respond to a Data Request

Upon receiving your request, we will review it.

- We may ask you to clarify what data you are requesting.
- We will ask you to confirm your identity as the data subject.
- If you are requesting data about you and we do not have the data, we will notify you in writing within 10 business days.
- If you are requesting data about you and we have the data, but the data are either confidential or not public data about someone else, we will notify you within 10 business days and identify the law that prevents us from providing the data.

- If you are requesting data about you and we have the data, and the data are public or private data about you, we will respond to your request within 10 business days by doing one of the following:
 - Arrange a date, time, and place to review data in our offices; or
 - We will inform you about our requirement to prepay for the data or copies. You may choose to pick up the printed or copied data, or we will mail or email them to you. We will provide electronic copies (such as email) upon request, if we keep the data electronically and if we can reasonably make a copy.
- After we have provided you with your requested data, we do not have to show you the same data again for 6 months unless there is a dispute about the data or we collect or create new data about you.

Response time may be impacted by the size or complexity of your request and by the number of requests you make in a given period of time. Following our response, if you do not make arrangements within 15 business days to review or pay for the data, we will conclude that you no longer want the data and will consider your request closed.

If you do not understand some of the data (technical terminology, abbreviations, or acronyms), please tell the person who provided the data to you. We will give you an explanation if you ask.

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 to respond to your request. If we agree to create data in response to your request, we will work with you on the details of your request, including cost and response time.

In addition, we are not required to respond to questions that are not about your data requests, or that are not requests for government data.

Data Practices Contacts

Responsible Authority

Gina Fast, Executive Director

Phone: 651-201-2744

Email: Gina.Fast@state.mn.us

Data Practices Compliance Official

Catrina Mairose, Chief of Staff

Phone: 612-548-2176

Email: Catrina.Mairose@state.mn.us

Data Practices Designee

Jenna Bohl, Licensing Division Manager

Phone: 651-201-2750

Email: Jenna.Bohl@state.mn.us

Data Request Form – Data Subject

Request date:

Contact information:

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.

Data Subject Name:

Parent/Guardian Name (if applicable):

Phone number/email address:

The data I am requesting:

Describe the data you are requesting as specifically as possible.

I am requesting access to data in the following way:

- Review
- Copies
- Both review and copies

We will respond to your request within 10 business days

To Be Completed By Staff Member Responding to Data Request:

Identity Confirmed:

Date:

Staff Name:

Standards For Verifying Identity

The following constitute proof of identity:

- An adult individual must provide a valid photo ID, such as
 - a driver's license
 - a state-issued ID
 - a tribal ID
 - a military ID
 - a passport
 - the foreign equivalent of any of the above
- A minor individual must provide a valid photo ID, such as
 - a driver's license
 - a state-issued ID (including a school/student ID)
 - a tribal ID
 - a military ID
 - a passport
 - the foreign equivalent of any of the above
- 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, foster care
 - a foster care contract
 - 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)
 - valid power of attorney

Note: Individuals who do not review data or pick up copies of data in person may be required to provide either notarized or certified copies of the documents that are required or an affidavit of ID.