

Effective Date: 07-31-2025

PRIVACY NOTICE

PURSUANT TO THE MINNESOTA CONSUMER DATA PRIVACY ACT

This Minnesota privacy notice (“Notice”) pursuant to the Minnesota Consumer Data Privacy Act, Minnesota Statutes §13.6505 et seq., (“MCDPA”), supplements the information contained in the Privacy Policy of Rausch Sturm LLP (“Rausch Sturm,” “we,” “us,” or “our”), and applies solely to visitors, users, and others who reside in the State of Minnesota (“consumers” or “you”). Rausch Sturm is a debt collector. This Notice applies to both our online and offline practices. We adopt this Notice to comply with the MCDPA. Any terms defined in the MCDPA have the same meaning when used in this Notice. For questions concerning this Notice or to obtain a copy of this Notice in an alternative format or in Spanish, please call us at 855-517-6279.

A. Consumer Rights

The MCDPA provides consumers with specific rights regarding their personal data. This section describes your rights.

1. Right to Confirm:
You have the right to confirm whether we are processing personal data concerning you, and to access the categories of personal data we are processing.
2. Right to Correct:
You have the right to correct inaccurate personal data concerning you, taking into account the nature of the personal data and the purposes of the processing of the personal data.
3. Right to Deletion:
You have the right to delete personal data concerning you.
4. Right to Obtain:
You have the right to obtain personal data concerning you, which you previously provided to us, in a portable and, to the extent technically feasible, readily usable format that allows you to transmit the data to another controller without hindrance, where the processing is carried out by automated means.
5. Right to Opt Out:
You have the right to opt out of the processing of personal data concerning you for purposes of targeted advertising, the sale of personal data, or profiling in furtherance of automated decisions that produce legal effects concerning you or similarly significant effects concerning you.
6. Right related to Profiling:
If your personal data is profiled in furtherance of decisions that produce legal effects concerning you or similarly significant effects concerning you, you have the right to question the result of the profiling, to be informed of the reason that the profiling resulted in the decision, and, if feasible, to be informed of what actions you might have taken to secure a different decision and the actions that you might take to secure a different decision in the future. You have the right to review your personal data used in the profiling. If the decision is determined to have been based upon inaccurate personal data, taking into account the nature of the personal

data and the purposes of the processing of the personal data, you have the right to have the data corrected and the profiling decision reevaluated based upon the corrected data.

7. Right to obtain list of Third Parties.

You have a right to obtain a list of the specific third parties to which we have disclosed your personal data. If we do not maintain the information in a format specific to you, a list of specific third parties to whom we have disclosed any consumers' personal data may be provided instead.

B. Our Duties

1. Representations:

- i. We will limit the collection of personal data to what is adequate, relevant, and reasonably necessary in relation to the purposes for which that personal data is processed, as disclosed to the consumer; and
- ii. For purposes of protecting the confidentiality, integrity, and accessibility of personal data, we will establish, implement, and maintain reasonable administrative, technical, and physical data security practices that are appropriate to the volume and nature of the personal data at issue.
- iii. We will not, except as otherwise provided in the MCDPA, process the sensitive data of yours without obtaining your consent.

2. The MCDPA requires that we provide you with the following information.

i. Categories of personal data processed by us:

- Personal identifying information, like name, address and account number, as well as other identifying information, which we obtain from the consumer's creditor, credit reports and other skip trace tools, and the consumer;
- Characteristics such as age, gender, etc., which we obtain from the consumer's creditor and consumer's credit report;
- Retail information, which we obtain from the consumer's creditor and the consumer's credit report;
- Commercial information, including records of personal property;
- Internet activity regarding online payments and account updates, which we collect if the consumer visits our website or payment portal;
- Geolocation data, which we obtain from process servers;
- Recordings, which are made when the consumer has a telephone conversation with us;
- Professional and employment related information, which we obtain from the consumer's creditor, credit reporting agencies, the consumer, and other skip trace sources; and
- Educational information, which we obtain from the consumer's creditor, credit reporting agencies, the consumer, and other skip trace sources.

ii. Purpose for processing personal data:

- Helping to ensure security and integrity to the extent the use of personal data is reasonably necessary and proportionate for these purposes;
- Debugging to identify and repair errors that impair existing intended functionality;

- Short-term, transient use, including, but not limited to, non-personalized advertising shown as part of consumer's current interaction with the business, provided that the consumer's personal data is not disclosed to another third party and is not used to build a profile about the consumer or otherwise alter the consumer's experience outside the current interaction with us.
 - Performing services on our behalf of the business, including maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, providing financing, providing analytic services, providing storage, or providing similar services on behalf of the business.
 - Undertaking internal research for technological development and demonstration.
 - Undertaking activities to verify or maintain the quality or safety of a service or device that is owned, manufactured, manufactured for, or controlled by the business, and to improve, upgrade, or enhance the service or device that is owned, manufactured, manufacture for, or controlled by the business.
 - Other business or business operational purposes as follows:
 - Debt collection.
 - To fulfill or meet the reason for which the information is provided. For example, if you provide us with personal data in order for us to process a payment, we will use that information to process said payment.
 - To provide you with information or services that you request from us.
 - To provide you with email or text alerts and other notices concerning our services.
 - To carry out our obligations and enforce our rights arising from any contracts entered into between you and us, including for collections.
 - To carry out our obligations and enforce our rights arising from any contracts entered into between you and our clients, including for collections.
 - To improve our website and present its contents to you.
 - For testing, research, analysis and service development.
 - As necessary or appropriate to protect the rights, property or safety of us, our clients or others.
 - To respond to law enforcement requests and as required by applicable law, court order, governmental regulations, or comply with a court order or subpoena to provide information.
 - As described to you when collecting your personal data or as otherwise set forth in the Minnesota collection laws.
- iii. How you may exercise your rights, including the process by which you may appeal our decision with regard to your request:
- When you exercise your rights, we will use commercially reasonable methods for authenticating the identity of the person submitting a request to exercise rights.
 - We will notify you if we cannot, using commercially reasonable methods, authenticate your request without additional information from you.
 - When you exercise your rights, we will respond without undue delay, which may not be later than 45 days after the date of the receipt of the request. We may extend

the response period once by an additional 45 days when reasonably necessary, taking into account the complexity and number of the consumer's request, so long as we inform you of the extension within the initial 45-day response period, together with the reason for the extension.

- If we cannot take action regarding your request, we must inform you without undue delay, which may not be later than 45 days after the date of receipt of the request, of the justification for the inability to take action on the request and provide instructions on how to appeal the decision.
- We have established an appeal process by which you may appeal any refusal of ours to take action on a request. We will inform you in writing of any action taken or not taken in response to an appeal within 45 days after the date of receipt of the appeal, including a written explanation of the reason or reasons for the decision. That period may be extended by 60 additional days where reasonably necessary, taking into account the complexity and number of the requests serving as the basis for the appeal. The controller must inform the consumer of any extension within days of receipt of the appeal, together with the reasons for the delay. If we deny the appeal, we will provide or specify information that enables you to contact the Attorney General to submit a complaint.

iv. Categories of personal information that we sell to third parties:

We do not sell your personal information to third parties. If we intend to sell your personal information to third parties, we will provide you with notification of your rights including opt out rights.

v. Categories of personal data that we share with third parties:

- Personal identifying information
- Characteristic information
- Retail information
- Professional or employment related information

vi. Categories of third parties with whom we sell personal data:

We do not sell your personal information to third parties. If we intend to sell your personal information to third parties, we will provide you with notification of your rights including opt out rights.

vii. Categories of third parties with which we share personal data:

- Service providers and contractors.
- Third parties to whom you or your agents authorize us to disclose your personal information in connection with products or services we provide to you.

viii. Description of the methods by which consumers can submit requests to exercise their consumer rights or appeal our refusal to take action:

- Submission: To exercise the rights described above, please submit a verifiable consumer request by either:
 - Calling us at 855-517-6279
 - Submitting the submission form located at:
www.rauschsturm.com/request-MN.

3. We do not sell personal data to third parties or process personal information for targeted advertising. If in the future, we anticipate selling your personal data to third parties or processing your personal data for targeted advertising, we will provide you required information pursuant to the MCDPA, including opt-out rights.

C. Limitations

The above rights and duties may be limited if any of the following apply:

1. We are both a controller and a processor as those terms are defined by the MCDPA. A processor that is a controller shall comply with the MCDPA with regard to any personal data that it collects or maintains outside of its role as a processor. Most of the personal data that we collect or maintain is done in context of our role as a processor. If we deny your verified request pursuant to this notice because all of the information collected or maintained about you has been pursuant to our role as a processor, we will provide you with the contact information of the business on whose behalf we collect or maintain the information.
2. The MCDPA does not apply to the following entities, activities, or types of information:
 - i. a government entity;
 - ii. a federally recognized Indian tribe;
 - iii. information that meets the definition of:
 - (a) protected health information, as defined by and for purposes of the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, and related regulations;
 - (b) health records, as defined in section 144.291, subdivision 2;
 - (c) patient identifying information for purposes of Code of Federal Regulations, title, part 2, established pursuant to United States Code, title 42, section 290dd-2;
 - (d) identifiable private information for purposes of the federal policy for the protection of human subjects, Code of Federal Regulations, title 45, part 46; identifiable private information that is otherwise information collected as part of human subjects research pursuant to the good clinical practice guidelines issued by the International Council for Harmonisation; the protection of human subjects under Code of Federal Regulations, title 21, parts 50 and 56; or personal data used or shared in research conducted in accordance with one or more of the requirements set forth in this paragraph;
 - (e) information and documents created for purposes of the federal Health Care Quality Improvement Act of 1986, Public Law 99-660, and related regulations; or Article 5 Sec. 4. 160
 - (f) patient safety work product for purposes of Code of Federal Regulations, title 42, part 3, established pursuant to United States Code, title 42, sections 299b-21 to 299b-26;
 - iv. information that is derived from any of the health care-related information that has been deidentified in accordance with the requirements for deidentification set forth in Code of Federal Regulations, title 45, part 164;
 - v. information originating from, and intermingled to be indistinguishable with, any of the health care-related information that is maintained by:

- (a) a covered entity or business associate, as defined by the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, and related regulations;
 - (b) a health care provider, as defined in section 144.291, subdivision 2; or
 - (c) a program or a qualified service organization, as defined by Code of Federal Regulations, title 42, part 2, established pursuant to United States Code, title 42, section 290dd-2;
- vi. information that is:
 - (a) maintained by an entity that meets the definition of health care provider under Code of Federal Regulations, title 45, section 160.103, to the extent that the entity maintains the information in the manner required of covered entities with respect to protected health information for purposes of the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, and related regulations;
 - (b) included in a limited data set, as described under Code of Federal Regulations, title 45, part 164.514(e), to the extent that the information is used, disclosed, and maintained in the manner specified by that part;
 - (c) maintained by, or maintained to comply with the rules or orders of, a self-regulatory organization as defined by United States Code, title 15, section 78c(a)(26);
 - (d) originated from, or intermingled with, information that a licensed residential mortgage originator, as defined under section 58.02, subdivision 19, or residential mortgage servicer, as defined under section 58.02, subdivision 20, collects, processes, uses, or maintains; or
 - (e) originated from, or intermingled with, information that a nonbank financial institution, as defined by section 46A.01, subdivision 12, collects, processes, uses, or maintains;
- vii. information used only for public health activities and purposes, as described under Code of Federal Regulations, title 45, part 164.512;
- viii. an activity involving the collection, maintenance, disclosure, sale, communication, or use of any personal data bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living by a consumer reporting agency, as defined in United States Code, title 15, section 1681a(f), by a furnisher of information, as set forth in United States Code, title 15, section 1681s-2, who provides information for use in a consumer report, as defined in United States Code, title 15, section 1681a(d), and by a user of a consumer report, as set forth in United States Code, title 15, section 1681b, except that information is only excluded under this paragraph to the extent that the activity involving the collection, maintenance, disclosure, sale, communication, or use of the information by the agency, furnisher, or user is subject to regulation under the federal Fair Credit Reporting Act, United States Code, title 15, sections 1681 to 1681x, and the information is not collected, maintained, used, communicated, disclosed, or sold except as authorized by the Fair Credit Reporting Act;

- ix. personal data collected, processed, sold, or disclosed pursuant to the federal Gramm-Leach-Bliley Act, Public Law 106-102, and implementing regulations, if the collection, processing, sale, or disclosure is in compliance with that law;
- x. personal data collected, processed, sold, or disclosed pursuant to the federal Driver's Privacy Protection Act of 1994, United States Code, title 18, sections 2721 to 2725, if the collection, processing, sale, or disclosure is in compliance with that law;
- xi. personal data regulated by the federal Family Educational Rights and Privacy Act, United States Code, title 20, section 1232g, and implementing regulations;
- xii. personal data collected, processed, sold, or disclosed pursuant to the federal Farm Credit Act of 1971, as amended, United States Code, title 12, sections 2001 to 2279cc, and implementing regulations, Code of Federal Regulations, title 12, part 600, if the collection, processing, sale, or disclosure is in compliance with that law;
- xiii. data collected or maintained:
 - (a) in the course of an individual acting as a job applicant to or an employee, owner, director, officer, medical staff member, or contractor of a business if the data is collected and used solely within the context of the role;
 - (b) as the emergency contact information of an individual if used solely for emergency contact purposes; or
 - (c) that is necessary for the business to retain to administer benefits for another individual relating to the individual if used solely for the purposes of administering those benefits;
- xiv. personal data collected, processed, sold, or disclosed pursuant to the Minnesota Insurance Fair Information Reporting Act in sections 72A.49 to 72A.505;
- xv. data collected, processed, sold, or disclosed as part of a payment-only credit, check, or cash transaction where no data about consumers are retained;
- xvi. a state or federally chartered bank or credit union, or an affiliate or subsidiary that is principally engaged in financial activities, as described in United States Code, title 12, section 1843(k);
- xvii. information that originates from, or is intermingled so as to be indistinguishable from, information that a person licensed under chapter 56 collects, processes, uses, or maintains;
- xviii. an insurance company, as defined in section 60A.02, subdivision 4, an insurance producer, as defined in section 60K.31, subdivision 6, a third-party administrator of self-insurance, or an affiliate or subsidiary of any entity identified in this clause that is principally engaged in financial activities, as described in United States Code, title 12, section 1843(k), except that this clause does not apply to a person that, alone or in combination with another person, establishes and maintains a self-insurance program that does not otherwise engage in the business of entering into policies of insurance;
- xix. a small business, as defined by the United States Small Business Administration under Code of Federal Regulations, title 13, part 121, except that a small business identified in this clause is subject to section 325O.075;
- xx. a nonprofit organization that is established to detect and prevent fraudulent acts in connection with insurance; and

- xxi. an air carrier subject to the federal Airline Deregulation Act, Public Law 95-504, only to the extent that an air carrier collects personal data related to prices, routes, or services and only to the extent that the provisions of the Airline Deregulation Act preempt the requirements of this chapter.
3. Compliance would require a controller, processor, third party, or consumer to disclose trade secrets.
 4. Compliance would restrict our ability to:
 - i. comply with federal, state, or local laws, rules, or regulations, including but not limited to data retention requirements in state or federal law notwithstanding a consumer's request to delete personal data;
 - ii. comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, local, or other governmental authorities;
 - iii. cooperate with law enforcement agencies concerning conduct or activity that the controller or processor reasonably and in good faith believes may violate federal, state, or local laws, rules, or regulations;
 - iv. investigate, establish, exercise, prepare for, or defend legal claims;
 - v. provide a product or service specifically requested by a consumer; perform a contract to which the consumer is a party, including fulfilling the terms of a written warranty; or take steps at the request of the consumer prior to entering into a contract;
 - vi. take immediate steps to protect an interest that is essential for the life or physical safety of the consumer or of another natural person, and where the processing cannot be manifestly based on another legal basis;
 - vii. prevent, detect, protect against, or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities, or any illegal activity; preserve the integrity or security of systems; or investigate, report, or prosecute those responsible for any such action;
 - viii. assist another controller, processor, or third party with any of the obligations under this paragraph;
 - ix. engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws and is approved, monitored, and governed by an institutional review board, human subjects research ethics review board, or a similar independent oversight entity that has determined: (i) the research is likely to provide substantial benefits that do not exclusively accrue to the controller; (ii) the expected benefits of the research outweigh the privacy risks; and (iii) the controller has implemented reasonable safeguards to mitigate privacy risks associated with research, including any risks associated with reidentification; or
 - x. process personal data for the benefit of the public in the areas of public health, community health, or population health, but only to the extent that the processing is: (i) subject to suitable and specific measures to safeguard the rights of the consumer whose personal data is being processed; and (ii) under the responsibility of a professional individual who is subject to confidentiality obligations under federal, state, or local law.

5. The obligations imposed on controllers or processors do not restrict a controller's or processor's ability to collect, use, or retain data to:
 - i. effectuate a product recall or identify and repair technical errors that impair existing or intended functionality;
 - ii. perform internal operations that are reasonably aligned with the expectations of the consumer based on the consumer's existing relationship with the controller, or are otherwise compatible with processing in furtherance of the provision of a product or service specifically requested by a consumer or the performance of a contract to which the consumer is a party; or
 - iii. conduct internal research to develop, improve, or repair products, services, or technology.
6. The obligations imposed on controllers or processors do not apply where compliance by the controller or processor would violate an evidentiary privilege under Minnesota law and do not prevent a controller or processor from providing personal data concerning a consumer to a person covered by an evidentiary privilege under Minnesota law as part of a privileged communication.
7. Obligations imposed on controllers and processors under this chapter shall not:
 - i. adversely affect the rights or freedoms of any persons, including exercising the right of free speech pursuant to the First Amendment of the United States Constitution; or
 - ii. apply to the processing of personal data by a natural person in the course of a purely personal or household activity.
8. Compliance would require us to do any of the following:
 - i. reidentify deidentified data or pseudonymous data; or
 - ii. maintain data in identifiable form or collect, obtain, retain or access data or technology in order to be capable of associating an authenticated consumer request with personal information; or
 - iii. comply with an authenticated consumer request to exercise a right if: (a) we cannot reasonably associate the request with personal information or it would be unreasonably burdensome for us to associate the request with the personal information; (b) we do not use personal information to recognize or respond to the specific consumer who is the subject of the personal information or associate the personal information with any other personal information about you; and (c) we do not sell or otherwise voluntarily disclose personal information to a third party other than a processor; or
 - iv. delete information that we maintain or use as aggregate or de-identified data, provided that such data in the possession of us is not linked to a specific consumer.

D. Changes To Our Privacy Notice

This Notice was last updated on 7-31-2025. We reserve the right to amend this Notice at our discretion and at any time. When we make changes to this Notice, we will notify you by updating the “last updated” date on this notice.

This communication is from a debt collector.