

Last Updated: July 9, 2024

Privacy Policy

This Privacy Policy (“**Policy**”) describes how InscribeAI, Inc. (“**Inscribe**”, “**InscribeAI**”, “**We**”, “**Us**”) collects, uses, and discloses personally identifiable information (as defined by applicable law, “**Personal Information**”). This Policy applies to the websites that we control, including <https://inscribe.ai/> (the “**Websites**”) and our InscribeAI web application service and API, which we make available to our clients for document analysis and detection of document fraud (the “**Platform**” and together with our Websites, the “**Services**”). The privacy of our users is of great importance to us. By using the Services, including by visiting the Website or logging in to the Platform, or by providing Personal Information to InscribeAI, you acknowledge and agree to the practices and policies outlined in this Policy.

Our Services are not directed at individuals under 18 and we do not knowingly collect data from individuals under the age of 18.

With respect to our Platform, we enter into agreements with our customers that define our obligations to our customers with respect to the Personal Information they provide to us. In this Privacy Policy, we describe where we collect information on our own behalf, for our business purposes and on our customers’ behalf as a service provider or data processor. You should refer to our customers’ privacy policies for information about how our customers collect, use and share information including through their use of our Services.

1. Application of this Policy

This Policy covers our collection, use and disclosure of information Personal Information, including individuals who use our Services (“**Users**”), as well as our clients (“**Clients**”) and individuals who visit our Website.

This Policy does not apply to the practices of companies that we do not own or control, including those practices of our Clients, third party service providers, or other third-party organizations.

2. How We Collect Personal Information We Collect

We provide a comprehensive table of the categories of Personal Information we collect and the categories of third parties we share information with [here](#).

We collect personal information in the following ways:

- When you provide Personal Information to us by filling out forms, uploading documents, emailing us, sending messages in the Platform, registering to use the Services, or in other ways;
- Directly from our Clients and Users when they input Personal Information to our Platform, including documents that they analyze using our Platform;
- Directly from third party service providers or other publicly available sources when our Clients and Users request information from third party sources through our Platform;
- Directly from third party marketing, social media and analytics providers, or from our referral partners;
- Automatically about your interaction with the Service through automatic tracking technologies (e.g., cookies) that may or may not personally identify you (this information may be combined with information that does personally identify you). This includes information like IP address, Internet connection, network activity, the device or equipment you use, geolocation, your activity or interaction with the Site or Service, our social media accounts, email marketing campaigns, or marketing materials;

3. Categories of Personal Information We Collect

We provide a comprehensive table of the categories of Personal Information we collect and the categories of third parties we share information with [here](#).

We collect the following categories of Personal Information:

- **Identifiers:** we collect name, email address, phone number which we collect from Clients, Users and prospective clients when they provided it to us or when we receive it from a referral partner.
- **Account information:** Users are required to create an account in order to use our Platform. In connection with registration, we collect name, email address, phone number and business address, as well as other business information.
- **Documents our Clients Upload:** our Users upload documents, including invoices, billing statements, account statements, loan applications, credit card statements, payroll documents, pay stubs, tax documents, education records and other information about individuals for their fraud detection and compliance purposes.

- **Government issued ID:** our Users may upload government issued IDs, like driver's license for fraud detection and compliance purposes.
- **Data we receive from other sources:** as part of our Service to our Clients, we may receive information from third party sources (whether service provider, third party or publicly available).
- **Inferences:** we use information that we receive from our Clients and information that we receive from third party service providers and other sources to create inferences about individuals.
- **Usage and Analytics Information:** we collect device data and usage information like IP address, login information, webpages visited, referring and exiting webpages, time zone, setting and location, device location, hardware model and operating system, browser data, network data, and other technical data.
- **Demographic information:** we may receive demographic information from our third party marketing and analytics service providers. These providers may link your Personal Information (including information collected from our Website) with other information they collect.

3. How We Use the Personal Information We Collect

We provide a comprehensive table of that includes the business purpose for the collection and use of Personal Information [here](#).

We use Personal Information for the following business and commercial purposes:

- **Provide Services:** we use Personal Information to operate, provide, secure, support, maintain, enhance, and modify our Services. This includes for research and development purposes, to develop new services or features, or to determine how our Clients or other users use our Services.
- **To Help our Clients Prevent Fraud and Verify Identities:** we use the Personal Information that our Clients upload to help our Clients identify fraud and verify the identity of individuals. This includes analyzing documents, verifying information, and creating inferences based on the information we collect and receive. We also use the Personal Information that we collect to protect our Services and others from fraud, malicious activity, and for other privacy and security-related concerns.
- **Develop Insights:** We use Personal Information to develop insights based on the documents we receive from Users and third party sources (including publicly

available information). This is part of the Service we provide to our Clients. We also may develop insights about our Users or Website visitors using marketing and analytics service providers.

- **Communicate With You:** we use Personal Information to communicate with you and send you things like technical notices, updates, security alerts, marketing communications, support communications and other messages.
- **For Marketing Purposes:** we use Personal Information that we collect or receive from third parties to market our services. This may include marketing on social media or third party websites, to invite you to our events, or keep you updated on product offerings.
- **Investigate Misuse and Misconduct:** we use Personal Information to investigate any misuse of our Service, criminal activity, or other unauthorized access to our Services.
- **For Legal Purposes:** we use Personal Information to comply with contractual and legal obligations under applicable law and for other legal purposes such as to establish and defend against claims.
- **With Your Consent:** we may use Personal Information for other notified purposes with your consent or at your direction.
- **Change of Control:** if we (or substantially all of our assets) are acquired, or if we go out of business, enter bankruptcy, or go through some other change of control, Personal Information may be made available or otherwise transferred to the new controlling entity, or other third party.

We collect, use, and share data that has been aggregated or anonymized in a manner that does not identify you personally for any purpose permitted under applicable law. This includes creating or using aggregated or anonymized data to develop new services, or to facilitate research, and for analytics purposes to help assess the speed, accuracy, and/or security of our services.

4. Categories of Third Parties we Disclose Personal Information to

We provide a comprehensive table of the categories of third parties with whom we share Personal Information [here](#).

We share Personal Information with the following categories of third parties:

- **Service Providers:** We use third party service providers to deliver our Services, and share Personal Information with in order to deliver our Services. We may share Personal Information with cloud and infrastructure service providers, support desk service providers, information security detection service providers, payment service providers, data analytics providers, fraud detection and prevention service providers, search engine service providers, third party data sources. We also use service providers to support our business operations, including email service providers, chat service providers, marketing service providers, or analytics service providers. For a current list of our third-party sub-processors, please see <https://inscribe.ai/subprocessors>.
- **Clients and Users:** we share information that we receive from third party service providers and provide that information to our Clients and Users for their fraud detection purposes, including the inferences that we create.
- **Professional Advisors and Consultants:** we may use professional services and consultants to provide advice, develop software, provide data analysis and research, support our sales and marketing teams, or for other similar consulting services.
- **Business Partners and Referral Partners:** we may share Personal Information with our business partners, including integration partners, resellers and referral partners, or event sponsors.
- **Marketing, Social Media and Analytics Providers:** we may share Personal Information that we collect using Automatic Tracking Technologies with data analytics, marketing and social media providers. This includes information like IP address, demographic and other technical or usage information. These third parties may combine the Personal Information that we provide them with Personal Information they receive from other sources.
- **Third Parties in Connection with a Change of Control:** we may share Personal information to an acquirer or major investor in connection with sale of our business, or a trustee or other third parties in connection with bankruptcy proceedings.
- **Third Parties in Connection with our Legal Obligations:** we may disclose Personal information if we are under a duty to disclose or share your Personal Information in order to comply with any legal obligation, or in order to enforce or apply our Client contracts and other agreements; or to protect our rights, property, or safety, our customers, or others. This includes exchanging information with other companies and organizations for the purposes of fraud protection and credit risk reduction. All disclosures will be made in accordance with applicable laws.

- **With our Affiliated Entities.** We may share Personal Information with our affiliated entities.
- **Other Third Parties with Notice:** we may share Personal Information with other third parties for any other purpose that we notify you of, or where you direct us to do so.

5. Automatic Tracking Technology

We use cookies, pixels and other automatic tracking technology on our Website and on the Platform. We use both session-based and persistent cookies.

Cookies are small text files sent by us to your computer and from your computer or mobile device to us each time you use our Services. They are unique to your account or your browser. Session-based cookies last only while your browser is open and are automatically deleted when you close your browser. Persistent cookies last until you or your browser delete them or until they expire.

Some cookies are associated with a user account. We use session cookies containing encrypted information to allow the system to uniquely identify a User Account while the User is logged in. This information allows us to process your online transactions and requests. Session cookies help us make sure you are who you say you are after you've logged in and are required in order to use the Services.

Other cookies are not tied to a user account but are unique and allow us to carry out site analytics and customization, among other similar things. We use persistent cookies to identify the fact that you are a user and track the webpages you view and use. If you access Services through your browser, you can manage your cookie settings there but if you disable some or all cookies you may not be able to use Services.

Finally, we use third parties like Google Analytics for website analytics, including who visit the Websites, such as the date and time, the search engine where the visitor comes from, the number of visits, etc. You may opt-out of third party cookies from Google Analytics on its website. Our third-party partners also employ clear gifs, images, and scripts that help them better manage content on our site.

You may be able to instruct your browser to refuse all cookies or to indicate when a cookie is being sent. Review your browser settings to set how to accept cookies, disable cookies or to notify you when receiving a new cookie. If you do not accept cookies, you may not be able to use some features of our Services and we recommend that you leave them turned on.

6. Security

The security of your Personal Information is important to us. We use commercially reasonable efforts to store and maintain your Personal Information. We take technical, contractual, administrative, and physical security steps designed to protect Personal Information that you provide to us.

7. Retention

We will keep your Personal Information for as long as we determine that it is necessary for the identified purpose, or as required by law or as necessary for compliance purposes, which may extend beyond the termination of our relationship with you.

Where we are processing Personal Information on behalf of our Clients, we will retain the Personal Information for as long as we are contractually obliged to do so, and for a period of time thereafter. All retained Personal Information will remain subject to the terms of this Privacy Policy.

We use the following criteria to determine appropriate retention periods for Personal Information:

- The amount, nature, and sensitivity of the Personal Information.
- The purpose(s) for which the Personal Information was collected and used.
- Whether we have a legal or compliance obligation to retain Personal Information.
- Whether retaining Personal Information is necessary to resolve disputes, including the establishment, exercise, or defense of legal claims.

8. EEA, UK, & Swiss Data Privacy Rights

We operate internationally, and so we transfer the data we collect about you across international borders for processing and storage.

8.1 Rights of EEA and UK Residents

If you are a resident of the European Economic Area (“**EEA**”), the United Kingdom (“**UK**”), or Switzerland, you are entitled to certain rights. These rights include:

- **Right of Access and/or Portability:** You have the right to access any Personal Information that we hold about you and, in some circumstances, have that data provided to you so that you can provide or “port” that data to another provider.
- **Right of Erasure:** In certain circumstances, you have the right to the erasure of Personal Information that we hold about you (for example, if it is no longer necessary for the purposes for which it was originally collected).

- **Right to Object to Processing:** In certain circumstances, you have the right to request that we stop processing your Personal Information and/or stop sending you marketing communications.
- **Right to Rectification:** You have the right to require us to correct any inaccurate or incomplete Personal Information.
- **Right to restrict processing:** You have the right to request that we restrict processing of your Personal Information in certain circumstances (for example, where you believe that the Personal Information we hold about you is not accurate or lawfully held).

To submit a request to exercise your rights, please contact us at dpo@inscribe.ai. If you submit a request related to a Client's use of the Services, we will direct you to submit a request to exercise your rights directly with our Client. We may have a reason under the law why we do not have to comply with your request or may comply with it in a more limited way than you anticipated. If we do, we will explain that to you in our response.

We process Personal Information, or "Personal Data" as that term is defined in the EU General Data Protection Regulation, on the following legal bases: (1) with your consent; (2) as necessary to perform our agreement to provide Services; and (3) as necessary for our legitimate interests where those interests do not override your fundamental rights and freedom related to data privacy. We may also process Personal Information as necessary to comply with legal obligations.

Users that reside in the EEA, UK, or Switzerland have the right to lodge a complaint about our data collection and processing actions with the supervisory authority concerned. Contact details for data protection authorities are available [here](#).

8.2 Cross-border Transfer of Data

If you use our Services outside of the United States, you understand that we may collect, process, and store your information in the United States and other countries. The laws in the U.S. regarding information may be different from the laws of your state or country. Any such transfers will comply with safeguards as required by relevant law.

To facilitate data transfers from the EU to other countries, we make use of the European Commission-approved standard contractual data protection clauses, the Data Privacy Framework, or other appropriate legal mechanisms to safeguard the transfer. Please contact us at dpo@inscribe.ai to receive a copy of our standard contractual data protection clauses.

8.3 Data Privacy Framework Notice

We comply with the EU-U.S. Data Privacy Framework (“**EU-U.S. DPF**”), the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework (“**Swiss-U.S. DPF**”), as set forth by the U.S. Department of Commerce. We have certified to the U.S. Department of Commerce that we adhere to the EU-U.S. Data Privacy Framework Principles (“**EU-U.S. DPF Principles**”) with regard to the processing of Personal Information received from the European Union in reliance on the EU-U.S. DPF and from the United Kingdom (and Gibraltar) in reliance on the UK Extension to the EU-U.S. DPF. We have certified to the U.S. Department of Commerce that it adheres to the Swiss-U.S. Data Privacy Framework Principles (“**Swiss-U.S. DPF Principles**”) with regard to the processing of Personal Information received from Switzerland in reliance on the Swiss-U.S. DPF. If there is any conflict between the terms in this Data Privacy Framework Notice and the EU-U.S. DPF Principles and/or the Swiss-U.S. DPF Principles, the Principles shall govern. To learn more about the Data Privacy Framework (“DPF”) program, and to view our certification, please visit <https://www.dataprivacyframework.gov/>.

We are responsible for the processing of Personal Information we receive under the DPF and subsequently transfers to a third party acting as an agent on its behalf. We comply with the DPF Principles for all onward transfers of Personal Information from the EU, UK, and Switzerland, including the onward transfer liability provisions.

The Federal Trade Commission has jurisdiction over our compliance with the EU-U.S. DPF, the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. DPF. In certain situations, we may be required to disclose Personal Information in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.

In compliance with the EU-U.S. DPF, the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. DPF, we commit to refer unresolved complaints concerning our handling of Non-HR Personal Information received in reliance on the EU-U.S. DPF, the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. DPF to JAMS, an alternative dispute resolution provider based in the United States. For clarity, Non-HR data includes all Personal Information processed by us on behalf of its customers. If you do not receive timely acknowledgment of your DPF Principles-related complaint from us, or if we have not addressed your DPF Principles-related complaint to your satisfaction, please visit <https://www.jamsadr.com/DPF-Dispute-Resolution> for more information or to file a complaint. The services of JAMS are provided at no cost to you.

For complaints regarding DPF compliance not resolved by any of the other DPF mechanisms, you have the possibility, under certain conditions, to invoke binding arbitration. Further information can be found on the official DPF website.

9. U.S. State Privacy Rights

If you are a resident of California, Colorado, Connecticut, Delaware, Indiana, Montana, New Hampshire, New Jersey, Oregon, Tennessee, Texas, Utah, Virginia, or any other

state that has passed data protection legislation, you may have additional rights regarding our use of your Personal Information. The rights outlined in this section do not apply to information exempted under applicable state privacy law. Further, the rights described in this Section are not absolute, are subject to exceptions and limitations, and may not be afforded to residents of all states. In certain cases, we may decline requests to exercise these rights, where permitted by law.

Persons with disabilities may obtain this notice in alternative format upon request by contacting us at dpo@inscribe.ai.

9.1 U.S. Privacy Rights

To the extent you are provided additional privacy rights in the state you reside, you have the following rights with respect to the information that we collect (in each case, subject to applicable law):

- **Right to Know:** To know the categories and specific Personal Information we have collected, the categories and sources from which we collected the Personal Information, the categories of third parties with whom we share Personal Information, and the business or commercial purpose for collecting or selling (if applicable) Personal Information, and the right to request information about and opt out of automated decision making (if applicable).
- **Right to Access:** To request a copy of the Personal Information that we have collected about you during the past 12 months.
- **Right to Opt-Out of Sales or Sharing:** To opt out of sales of Personal Information (if applicable) or sharing Personal Information for Cross-Contextual Behavioral Advertising.
- **Right to Delete:** To request that we delete the Personal Information that we have collected from you.
- **Right to Correct:** To correct inaccurate information that we maintain about you.
- **Right to Limit Disclosure of Sensitive Information:** To limit the disclosure of sensitive Personal Information, if we use or disclose sensitive Personal Information.
- **Freedom from Discrimination:** To exercise the rights described above free from discrimination or retaliation as prohibited under applicable law.

9.2 Exercising Your State Privacy Rights

If you reside in a state that provides specific data privacy rights, you may contact us using the **Contact Us** section below.

Your rights may only be exercised by you or by your designated agent. You may submit a request to know twice within a 12-month period unless applicable data privacy law grants you additional rights.

Your request must include enough information to allow us to reasonably verify that you are the person about whom we collected Personal Information or an authorized representative, which may include: (1) verifying your account information if you have an account with us; or (2) requesting two forms of identification that are reliable for verification purposes, unless the request includes sensitive information and, in which case, we may require additional verification. The information included in your request must allow us to properly understand, evaluate, and respond to it.

We cannot respond to your request if we cannot verify your identity or authority to make the request and confirm that the Personal Information relates to you. If we cannot verify your identity or authority, we will not fulfill your request. We will only use Personal Information provided in the request to verify the requestor's identity or authority to make it.

You may submit a request through a designated agent. You must instruct that agent that they will need to state that they are acting on your behalf when making the request, have reasonably necessary documentation, and be prepared to provide the necessary Personal Information to properly verify your request.

We will acknowledge receipt of your request. We will provide a substantive response within 45 calendar days or inform you of the reason and extension period (up to a total of 90 days) in writing.

You may appeal our decision with respect to a request you have submitted by contact us using the **Contact Us** section below.

9.3 Special Information for Nevada Residents

Residents of the State of Nevada have the right to opt-out of the sale of certain pieces of their information to other companies who will sell or license their information to others. At this time, we do not engage in such sales. If you are a Nevada resident and would like more information about our data-sharing practices, please email dpo@inscribe.ai.

9.4 California Shine the Light

Residents of the State of California have the right to request information from us regarding other companies to whom the company has disclosed certain categories of information during the preceding year for those companies' direct marketing purposes. If you are a California resident and would like to make such a request, please email dpo@inscribe.ai or write to us at InscribeAI, Inc, WeWork, 2 Dublin Landings, N Wall Quay, D01V4A3, Dublin, Ireland.

10. Your Choices

We offer the following choices for updating your Personal information or opting out of other uses of your Personal Information:

- **Users:** If you are an authorized user of our Services, you can sign into your account to update your contact information and payment method.
- **Our Emails:** If at any time you would like to unsubscribe from receiving future emails, you can click the unsubscribe link at the bottom of any email, or email us at dpo@inscribe.ai and we will promptly remove you from all correspondence.
- **Web Browser Settings:** Most web browsers automatically accept cookies but, if you prefer, you can usually modify your browser setting to disable or reject cookies. If you delete your cookies or if you set your browser to decline cookies, some features of the Services may not be available, work, or work as designed. You may also be able to opt out of or block tracking by interacting directly with the other companies who conduct tracking through our Services.
- **Google Analytics:** You may manage the information that Google Analytics receives by downloading and installing the browser plugin available [here](#).

11. Changes to this policy

We may amend this Policy from time to time. The use of Personal Information we collect is subject to the Policy in effect at the time such information is collected, used, or disclosed. If we make material changes or changes in the way we use Personal Information, we will notify you by posting an announcement on our Website or Platform, or by sending you an email or notification prior to the change becoming effective. You are bound by any changes to the Policy when you use the Services after such changes have been first posted.

12. Contact Us

For questions about our privacy practices, contact us via:

Data Protection Officer: dpo@inscribe.ai.

Phone Number: +1 844 735 4250