PRIVACY POLICY

Effective as of December 09, 2025

(Previous Versions)

Ensemble Labs, Inc., (doing business as True Foundry) ("**we**," "**us**," or "**our**") offers an enterprise ready AI gateway and agentic deployment platform offered as a subscription based Software as a Service ("**Services**"). Please refer to our website https://truefoundry.com for more details of our Services.

This privacy policy ("**Privacy Policy**") applies to the collection, use disclosure and protection of personal information processed in connection with, or through the Services including any personal data handled through:

- The platform https://truefoundry.com or any other website operated by us that links to this Privacy Policy;
- Administrative interfaces;
- Application Programming Interfaces (APIs);
- Integrations;
- Support channels;
- Engagement with us in other related ways including any sales, marketing or events; and

We enforce these standards regardless of whether these Services are deployed on-premises, within a virtual private cloud, in a hybrid environment, or on public cloud infrastructure. Some features that we offer are also governed by supplemental privacy policies which will be prompted to you before you use these features. You are encouraged to read and accept this Privacy Policy and any supplemental privacy policies before using our Services.

1. WHAT INFORMATION DO WE COLLECT AND THEIR SOURCES?

The categories of information we receive and collect depend on how you access, configure, and interact with the Services. This includes any specific features you enable, the deployment model you choose, the administrative settings you apply, and the data you decide to transmit, upload, or integrate with the platform.

Personal information you disclose to us and their source

We collect personal information that you voluntarily provide to us when you register for our Services or when you contact us. This information includes:

- **Account Information**: When you or the organisation that you work with creates an account with us, we collection your name, email address, account credentials (such as passwords). Additionally if you are an individual user or sole proprietor of your business, we may collect your payment or credit card information and transaction history.
- **User Content**: When you use our Services, we collect the Personal Data that is included in the models, datasets, code, proprietary algorithms, and workflows that you provide to our Services. User Content is end to end encrypted and is not accessed or visible to us.
- **Communication Information**: If you communicate with us, we collect your name, contact information such as email, and the contents of any messages you send.
- **Social Media Information**: When you interact with us on social media platforms such as LinkedIn, GitHub, Twitter, or Discord, you may provide Personal Data such as your name

and contact details as per your preferences set on these social media websites, and we collect that information. We also receive aggregate analytics and engagement data about our social-media activity from these social media platforms.

- **Marketing Data**: When you participate in our events or surveys, or when you submit details to verify your age or identity including you contract information such as email.

Information automatically collected

System Data: We automatically collect operational and system-generated information when you deploy, access, or use the Services. This information enables core platform functionality, security, observability, and performance. The information we collect may include authentication and access metadata, infrastructure and environment details, integration and configuration settings, deployment and runtime data, and telemetry, trace, and audit logs generated through your use of the platform (collectively "**System Data**"). Most of this information does not identify an individual and does not qualify as Personal Information. However, certain elements may constitute Personal Information in specific contexts for example, account-level details, audit logs that record user actions, or trace data that includes user identifiers or user-generated content transmitted through the Services.

Automatic Tracking and Cookies: We may use cookies and similar tracking technologies (like web beacons and pixels) to gather information when you interact with our Services. Some online tracking technologies help us maintain the security of our Services and your account, prevent crashes, fix bugs, save your preferences, and assist with basic site functions. Specific information about how we use such technologies and how you can refuse certain cookies is set out in our Cookie Notice: http://truefoundry.com/cookie-policy.

Third Party Analytics: We also permit third parties and service providers to use online tracking technologies on our Services for analytics and advertising, including to help manage and display advertisements, to tailor advertisements to your interests. The third parties and service providers use their technology to provide advertising about products and services tailored to your interests which may appear either on our Services or on other websites. To the extent these online tracking technologies are deemed to be a "sale"/"sharing" (which includes targeted advertising, as defined under the applicable laws) under applicable US state laws, you can opt out of these online tracking technologies by submitting a request as described below.

Do Not Track Signals

Most web browsers and some mobile operating systems and mobile applications include a Do-Not-Track ("DNT") feature or setting you can activate to signal your privacy preference not to have data about your online browsing activities monitored and collected. At this stage, no uniform technology standard for recognizing and implementing DNT signals has been finalized. As such, we do not currently respond to DNT browser signals or any other mechanism that automatically communicates your choice not to be tracked online. If a standard for online tracking is adopted that we must follow in the future, we will inform you about that practice in a revised version of this Privacy Notice.

California law requires us to let you know how we respond to web browser DNT signals. Because there currently is not an industry or legal standard for recognizing or honouring DNT signals, we do not respond to them at this time.

Recruitment Data

For recruitment-related interactions, we collect and process certain information to evaluate and manage your job application; however, all data collection, use, and processing activities associated with hiring are governed exclusively by our separate Recruitment Privacy Policy. That policy explains the categories of information we collect during the hiring process, how we use and retain that information, and the rights and choices available to applicants. Any personal information you submit or that we obtain in connection with a job application will be handled solely in accordance with the Recruitment Privacy Policy and not under this Privacy Policy.

Information collected in the past 12 months

The table below shows the categories of personal data that we have collected in the past 12 (twelve) months to provide our Services. The table includes illustrative examples of each category and does not reflect the personal information we collect from you. The inventory of all personal information we process is described in this section above.

Category	Examples	Collected (Yes/No)
A. Identifier	Contact details, such as name, email address, and account credentials	Yes
B. Personal information as defined in the California Customer Records statue	Name, contact information, education, employment, employment history and financial information	Yes
C. Protected classification characteristics under state or federal law	Gender, age, date of birth, race and ethnicity, national origin, marital status, and other demographic data	No
D. Commercial information	Transaction information, purchase history, financial details, and payment information	Yes
E. Biometric information	Fingerprints and voiceprints	No
F. Internet or other similar network activity	Browser history, search history online behaviour, interest data and interactions with our and other websites, applications systems and advertisements	Yes
G. Geolocation data	Device location	Yes
H. Audio, electronic, sensory or similar information	Images and audio, video or call recordings created in connection with our business activities	No
I. Professional or employment related information	Business contact details in order to provide you our services at the business level or job title, work history and professional qualifications if you apply for a job with us.	No
J. Education information	Student records and directory information	No

K. Inferences drawn from collected personal information	Inferences drawn from any of the collected personal information listed above to create a profile or summary about, for example, an individual's preferences and characteristics	No
L. Sensitive personal information	Government and financial identifiers, financial account information, sex life or sexual orientation.	No

2. HOW DO WE PROCESS YOUR INFORMATION AND WHAT LEGAL BASIS DO WE RELY ON TO PROCESS YOUR INFORMATION?

Your interactions (such as when you register for the Services on our website, express an interest in obtaining information about us or our products and Services, or otherwise when you contact us) involve different types of information necessary to operate, secure, and optimize the Services:

- **To facilitate account creation and authentication and otherwise manage user accounts.** We may process your information so you can create and log in to your account, as well as keep your account in working order.
- **To deliver and facilitate delivery of services to the user.** We may process your information to provide you with the requested Service.
- **To request feedback.** We may process your information when necessary to request feedback and to contact you about your use of our Services.
- **To protect our Services.** We may process your information as part of our efforts to keep our Services safe and secure, including fraud monitoring and prevention.
- **To identify usage trends.** We may process information about how you use our Services to better understand how they are being used so we can improve them.
- **To save or protect an individual's vital interest.** We may process your information when necessary to save or protect an individual's vital interest, such as to prevent harm.

If you are located in the European Union or United Kingdom, this section applies to you.

The General Data Protection Regulation (GDPR) and UK GDPR require us to explain the valid legal bases we rely on in order to process your personal information. As such, we may rely on the following legal bases to process your personal information:

Sl. No.	Legitimate Basis	Categories of Personal Information
1.	**Consent**. We process your personal information when you give us permission to use it for a specific purpose. You may withdraw your consent at any time. Learn more about withdrawing your consent.	● Account Information (including Category A - Identifier, Category B - Personal information as defined in the California Customer Records statue, and Category D - Commercial Information) ● User Content ● Communication Information ● Social Media Information ● Marketing Data ● System Data(Including Category G - Geolocation Data, and Category F -

		Internet and other similar network activity) ● Automatic Tracking and Cookies ● Third Party Analytics
2.	**Performance of a Contract**. We process your personal information when doing so is necessary to fulfil our contractual obligations to you. This includes helping you create and manage your user account, enabling your use of the Services, and taking steps you request before we enter into a contract with you.	● Account Information (including Category A - Identifier, Category B - Personal information as defined in the California Customer Records statue, and Category D - Commercial Information) ● User Content ● Communication Information ● System Data(Including Category G - Geolocation Data, and Category F - Internet and other similar network activity) ● Automatic Tracking and Cookies ● Third Party Analytics
3.	**Legitimate Interests**. We process your personal information when doing so is necessary for our legitimate business interests and when those interests do not override your rights and freedoms. For example, we process information to: ● analyse how users engage with our Services so we can improve and retain user engagement; ● diagnose technical issues and prevent fraudulent or harmful activities; ● understand how users interact with our products and services to improve overall user experience.	● Account Information (including Category A - Identifier, Category B - Personal information as defined in the California Customer Records statue, and Category D - Commercial Information) ● Communication Information ● System Data (Including Category G - Geolocation Data, and Category F - Internet and other similar network activity) ● Automatic Tracking and Cookies ● Third Party Analytics
4.	**Legal Obligations**. We process your information when we must comply with applicable laws, such as cooperating with law-enforcement or regulatory authorities, exercising or defending legal claims, or disclosing information as evidence in litigation.	● Account Information (including Category A - Identifier, Category B - Personal information as defined in the California Customer Records statue, and Category D - Commercial Information) ● User Content ● Communication Information ● System Data (Including Category G - Geolocation Data, and Category F - Internet and other similar network activity)

5.	**Vital Interests.** We process your information when doing so is necessary to protect your vital interests or the vital interests of another person, including situations that involve potential threats to an individual's safety.	● Account Information (including Category A - Identifier, Category B - Personal information as defined in the California Customer Records statue, and Category D - Commercial Information) ● User Content ● Communication Information

In legal terms, we are generally the "data controller" under European data protection laws of the personal information described in this Privacy Notice, since we determine the means and/or purposes of the data processing we perform. This Privacy Notice does not apply to the personal information we process as a "data processor" on behalf of our customers including the User Content or any personal information contained in the User Content that we may process. In those situations, the customer that we provide services to and with whom we have entered into a data processing agreement is the "data controller" responsible for your personal information, and we merely process your information on their behalf in accordance with your instructions. If you want to know more about our customers' privacy practices, you should read their privacy policies and direct any questions you have to them.

If you are located in Canada, this section applies to you.

We may process your information if you have given us specific permission (i.e., express consent) to use your personal information for a specific purpose, or in situations where your permission can be inferred (i.e., implied consent). You can withdraw your consent at any time.

In some exceptional cases, we may be legally permitted under applicable law to process your information without your consent, including, for example:

- If collection is clearly in the interests of an individual and consent cannot be obtained in a timely way.
- For investigations and fraud detection and prevention.
- For business transactions provided certain conditions are met.
- If it is contained in a witness statement and the collection is necessary to assess, process, or settle an insurance claim.
- For identifying injured, ill, or deceased persons and communicating with next of kin.
- If we have reasonable grounds to believe an individual has been, is, or may be victim of financial abuse.
- If it is reasonable to expect collection and use with consent would compromise the availability or the accuracy of the information and the collection is reasonable for purposes related to investigating a breach of an agreement or a contravention of the laws of Canada or a province.
- If disclosure is required to comply with a subpoena, warrant, court order, or rules of the court relating to the production of records.
- If it was produced by an individual in the course of their employment, business, or profession and the collection is consistent with the purposes for which the information was produced.
- If the collection is solely for journalistic, artistic, or literary purposes.
- If the information is publicly available and is specified by the regulations.

- We may disclose de-identified information for approved research or statistics projects, subject to ethics oversight and confidentiality commitments.

3. WHEN AND WITH WHOM DO WE SHARE YOUR PERSONAL INFORMATION?

Vendors, Consultants, and Other Third-Party Service Providers. We may share your data with third-party vendors, service providers, contractors, or agents ("**third parties**") who perform services for us or on our behalf and require access to such information to do that work. We have contracts in place with our third parties, which are designed to help safeguard your personal information. This means that they cannot do anything with your personal information unless we have instructed them to do it. They will also not share your personal information with any organization apart from us. They also commit to protect the data they hold on our behalf and to retain it for the period we instruct.

Google Analytics. We may share your information with Google Analytics to track and analyse the use of the Services. To opt out of being tracked by Google Analytics across the Services, visit https://tools.google.com/dlpage/gaoptout. For more information on the privacy practices of Google, please visit the Google Privacy & Terms page.

The categories of third parties we may share personal information with are as follows:

- Data Analytics Services
- Performance Monitoring Tools
- Communication & Collaboration Tools
- Sales & Marketing Tools
- User Account Registration & Authentication Services
- Website Hosting Service Providers

We also may need to share your personal information in the following situations:

- **Business Transfers.** We may share or transfer your information in connection with, or during negotiations of, any merger, sale of company assets, financing, or acquisition of all or a portion of our business to another company.
- **Affiliates.** We may share your information with our affiliates, in which case we will require those affiliates to honor this Privacy Notice. Affiliates include our parent company and any subsidiaries, joint venture partners, or other companies that we control or that are under common control with us.

We may use your personal information for our own business purposes, such as for undertaking internal research for technological development and demonstration. This is not considered to be "selling" of your personal information.

We have not sold or shared any personal information to third parties for a business or commercial purpose in the preceding twelve (12) months. We have disclosed the following categories of personal information to third parties for a business or commercial purpose in the preceding twelve (12) months:

Category A. Identifiers

Category B. Personal information as defined in the California Customer Records statue

Category G. Geolocation data

4. HOW LONG DO WE KEEP YOUR INFORMATION?

Your personal data is maintained as per the Data Management Policy of the company (available here). We will only keep your personal information for as long as it is necessary for the purposes set out in this Privacy Notice, unless a longer retention period is required or permitted by law (such as tax, accounting, or other legal requirements). No purpose in this notice will require us keeping your personal information for longer than the period of time in which users have an account with us.

When we have no ongoing legitimate business need to process your personal information, we will either delete or anonymize such information, or, if this is not possible (for example, because your personal information has been stored in backup archives), then we will securely store your personal information and isolate it from any further processing until deletion is possible.

5. HOW DO WE KEEP YOUR INFORMATION SAFE?

We have implemented appropriate and reasonable technical and organizational security measures designed to protect the security of any personal information we process. However, despite our safeguards and efforts to secure your information, no electronic transmission over the Internet or information storage technology can be guaranteed to be 100% secure, so we cannot promise or guarantee that hackers, cybercriminals, or other unauthorized third parties will not be able to defeat our security and improperly collect, access, steal, or modify your information. Although we will do our best to protect your personal information, transmission of personal information to and from our Services is at your own risk. You should only access the Services within a secure environment. Our information security protocols and certifications maintained in this regard are available here.

6. DO WE COLLECT INFORMATION FROM MINORS?

We do not knowingly collect, solicit data from, or market to children under 18 years of age or the equivalent age as specified by law in your jurisdiction, nor do we knowingly sell such personal information. By using the Services, you represent that you are at least 18 or the equivalent age as specified by law in your jurisdiction or that you are the parent or guardian of such a minor and consent to such minor dependent's use of the Services. If we learn that personal information from users less than 18 years of age or the equivalent age as specified by law in your jurisdiction has been collected, we will deactivate the account and take reasonable measures to promptly delete such data from our records. If you become aware of any data we may have collected from children under age 18 or the equivalent age as specified by law in your jurisdiction, please contact us at dpo@truefoundry.com.

7. WHAT ARE YOUR PRIVACY RIGHTS?

You have rights under certain US state data protection laws. However, these rights are not absolute, and in certain cases, we may decline your request as permitted by law. These rights include:

- Right to know whether or not we are processing your personal data
- Right to access your personal data
- Right to correct inaccuracies in your personal data
- Right to request the deletion of your personal data
- Right to obtain a copy of the personal data you previously shared with us
- Right to non-discrimination for exercising your rights
- Right to opt out of the processing of your personal data if it is used for targeted advertising (or sharing as defined under California's privacy law), the sale of personal data, or profiling in furtherance of decisions that produce legal or similarly significant effects ("profiling")

Depending upon the state where you live, you may also have the following rights:

- Right to obtain a list of the categories of third parties to which we have disclosed personal data (as permitted by applicable law, including the privacy law in California)
- Right to limit use and disclosure of sensitive personal data (as permitted by applicable law, including the privacy law in California)

In some regions (like the EEA, UK, Switzerland, and Canada), you have certain rights under applicable data protection laws. These may include the right

- to request access and obtain a copy of your personal information,
- to request rectification or erasure;
- to restrict the processing of your personal information;
- if applicable, to data portability; and
- not to be subject to automated decision-making. If a decision that produces legal or similarly significant effects is made solely by automated means, we will inform you, explain the main factors, and offer a simple way to request human review.

In certain circumstances, you may also have the right to object to the processing of your personal information. You can make such a request by contacting us by using the contact details provided in the section below.

We will consider and act upon any request in accordance with applicable data protection laws.

If you are located in the EEA or UK and you believe we are unlawfully processing your personal information, you also have the right to complain to your Member State data protection authority or UK data protection authority.

If you are located in Switzerland, you may contact the Federal Data Protection and Information Commissioner.

Withdrawing your consent: If we are relying on your consent to process your personal information, which may be express and/or implied consent depending on the applicable law, you have the right to withdraw your consent at any time. You can withdraw your consent at any time by contacting us by using the contact details provided in the section below or updating your preferences.

However, please note that this will not affect the lawfulness of the processing before its withdrawal nor, when applicable law allows, will it affect the processing of your personal information conducted in reliance on lawful processing grounds other than consent

How to Exercise Your Rights

To exercise these rights, you can contact us by emailing us at security@truefoundry.com, or by referring to the contact details at the bottom of this document.

We will honor your opt-out preferences if you enact the Global Privacy Control (GPC) opt-out signal on your browser.

Under certain US state data protection laws, you can designate an authorized agent to make a request on your behalf. We may deny a request from an authorized agent that does not submit proof that they have been validly authorized to act on your behalf in accordance with applicable laws.

Request Verification

Upon receiving your request, we will need to verify your identity to determine you are the same person about whom we have the information in our system. We will only use personal information provided in your request to verify your identity or authority to make the request. However, if we cannot verify your identity from the information already maintained by us, we may request that you provide additional information for the purposes of verifying your identity and for security or fraud-prevention purposes.

If you submit the request through an authorized agent, we may need to collect additional information to verify your identity before processing your request and the agent will need to provide a written and signed permission from you to submit such request on your behalf.

California "Shine The Light" Law

California Civil Code Section 1798.83, also known as the "Shine The Light" law, permits our users who are California residents to request and obtain from us, once a year and free of charge, information about categories of personal information (if any) we disclosed to third parties for direct marketing purposes and the names and addresses of all third parties with which we shared personal information in the immediately preceding calendar year. If you are a California resident and would like to make such a request, please submit your request in writing to us by using the contact details provided in the section below.

8. DO WE MAKE UPDATES TO THIS NOTICE?

We may update this Privacy Notice from time to time. The updated version will be indicated by an updated "Revised" date at the top of this Privacy Notice. If we make material changes to this Privacy Notice, we may notify you either by prominently posting a notice of such changes or by directly sending you a notification. We encourage you to review this Privacy Notice frequently to be informed of how we are protecting your information.

9. HOW CAN YOU CONTACT US ABOUT THIS NOTICE?

If you have questions or comments about this notice, you may contact our Data Protection Officer (DPO) by email at dpo@truefoundry.com, by phone at +91 9871534339, or contact us by post at:

Ensemble Labs Inc
Data Protection Officer
355 Bryant St, Unit 403
San Francisco, , CA 94107
United States

Based on the applicable laws of your country or state of residence in the US, you may have the right to request access to the personal information we collect from you, details about how we have processed it, correct inaccuracies, or delete your personal information. You may also have the right to withdraw your consent to our processing of your personal information. These rights may be limited in some circumstances by applicable law. To request to review, update, or delete your personal information, please email us at security@truefoundry.com.

If you are a resident in the European Economic Area or Switzerland, we are the "data controller" of your personal information. We have appointed Adam Brogden to be our representative in the EEA and Switzerland. You can contact them directly regarding our processing of your information, by email at contact@gdprlocal.com, by phone at +35315549700, or by post to:

INSTANT EU GDPR REPRESENTATIVE LTD, Office 2
12A Lower Main Street, Lucan Co
Dublin K78 X5P8
Ireland

If you are a resident in the United Kingdom, we are the "data controller" of your personal information. We have appointed Adam Brogden to be our representative in the UK. You can contact them directly regarding our processing of your information, by email at contact@gdprlocal.com, by phone at +44 1772 217800, or by post to:

1st Floor Front Suite
27-29 North Street, Brighton
_____ _____
England