Privacy Policy

The Institute of Machine Learning (i4ml) www.i4ml.com

Effective Date: 05/01/2026 **Last Updated:** 05/21/2026

1. Introduction

The Institute of Machine Learning ("i4ml," "we," "us," or "our") is committed to protecting the privacy of individuals who visit our website at www.i4ml.com, use the HumanicFlow platform at humanicflow.i4ml.com, the CredentialHub platform at credentialhub.i4ml.com, the FlowTower platform at flowtower.i4ml.com (collectively, "i4ml platforms"), enroll in our courses, or otherwise interact with our services (collectively, the "Services").

This Privacy Policy describes what personal information we collect, how we use it, with whom we share it, how we protect it, how long we retain it, and what rights you have with respect to your information. This Privacy Policy is incorporated into and forms part of our Terms and Conditions, which are accessible via the Terms and Conditions menu. In the event of a conflict between this Privacy Policy and the Terms and Conditions with respect to the substance of data privacy practices — including what information is collected, how it is used, how long it is retained, and with whom it is shared — this Privacy Policy shall control. All disputes arising out of or relating to this Privacy Policy, including claims regarding the collection, use, or handling of personal information, are subject to the dispute resolution, governing law, and limitation of liability provisions set forth in the Terms and Conditions (Sections 14, 17, and 18).

By accessing or using the Services, you acknowledge that you have read and understood this Privacy Policy. If you do not agree with our data practices as described herein, you should not access or use the Services.

2. Consent and Notice at Collection

When you create an account on the Services — whether through email registration or social login — you are presented with this Privacy Policy and are required to affirmatively acknowledge it before your account is activated. For email-registered users, this acknowledgment is collected as part of the registration process prior to email verification. For users who register via social login (Google or Microsoft), this acknowledgment is collected on first access to the platform following OAuth authentication.

Your acknowledgment constitutes your informed consent to the data practices described in this Privacy Policy. You may withdraw consent at any time by deleting your account in accordance with Section 8.1; however, withdrawal of consent may result in the inability to access or use the Services.

For users in the European Economic Area (EEA) and United Kingdom (UK), the specific legal bases for our processing activities are detailed in Section 8.2.

3. Information We Collect

We collect information in three ways: information you provide to us directly, information collected automatically when you use the Services, and information received from third-party sources.

3.1 Information You Provide Directly

Account Registration Information. When you create an account, we collect your name, email address, and password. If you register using a social login provider (Google or Microsoft), we receive your name and email address from that provider. Passwords are cryptographically hashed using bcrypt and are never stored in plaintext.

Course Enrollment Information. When you enroll in a course, we collect enrollment details, course selection, and any information you provide through pre-course and post-course assessments, including self-reported confidence ratings and professional background information.

Payment Information. When you purchase course enrollment or credits, your payment is processed by Stripe, our third-party payment processor. We do not collect, process, or store credit card numbers, bank account numbers, or other payment card data on our systems. Stripe processes your payment on its own hosted checkout pages. We receive and store only a Stripe transaction reference identifier, the purchase amount, and the date of the transaction for our financial records.

User Data on the i4ml Platforms. When you use the i4ml platforms, you may upload documents, datasets, files, and other materials ("User Data"). You may also create workflow configurations, agentic designs, prompt sequences, RAG pipeline configurations, and other workflow assets ("User Workflows"). The platforms also generate outputs on your behalf, including AI-generated text, reports, analyses, credentials, and other materials ("User Outputs"). As described in our Terms and Conditions, you retain ownership of your User Data, User Workflows, and User Outputs.

Fine-Tuning Datasets. If you use the HumanicFlow platform's model fine-tuning features, the training datasets you provide are uploaded to our external fine-tuning provider for processing. We store metadata about your fine-tuning jobs (job status, configuration, timestamps) but the training data itself is transmitted to and processed by the external provider.

Communications. If you contact us by email or through our support channels, we collect the content of your communications, your email address, and any other information you choose to provide.

Community Participation. If you participate in community features hosted on third-party platforms (such as Slack), your interactions on those platforms are governed by those platforms' respective privacy policies. We do not independently collect or store your community discussion content.

3.2 Information Collected Automatically

Platform Usage Data. When you use the i4ml platforms, we automatically collect usage data for the purposes of operating the platforms, administering the credit system, and improving the Services. This includes credit consumption records (which operations you performed and the credits consumed), feature utilization metrics, and timestamps of platform activity.

Interaction Logs. The i4ml platforms record interaction logs — including prompts submitted, tools invoked, and workflow executions — which serve two distinct purposes. First, these logs support platform operation, including credit metering, debugging, and security monitoring, in i4ml's capacity as a data controller. Second, these logs serve as a project-level audit trail visible to the project owner and authorized project participants (organizational administrators, collaborators, and viewers) for governance purposes. In this second capacity, interaction logs form part of the user's project data and are subject to the ownership and data export rights described in the Terms and Conditions.

Session Data. We use server-side sessions to maintain your authenticated state. Session data is stored in our database (not in client-side cookies beyond a session identifier). Sessions expire after 24 hours of inactivity. The session cookie is configured as secure, httpOnly, and sameSite=lax.

Log Data. Our servers automatically record information when you access the Services, including your IP address, browser type, referring URL, pages visited, and the date and time of your visit.

Device and Browser Information. We collect technical information about the device and browser you use to access the Services, including device type, operating system, browser version, and screen resolution.

3.3 Information from Third-Party Sources

Social Login Providers. If you register or log in using Google OAuth or Microsoft OpenID Connect, we receive your name and email address from the provider. We do not receive or store your social login passwords. OAuth access tokens and refresh tokens are not stored in the browser or in persistent client-side storage; only the platform session cookie is present after authentication.

Payment Processor. Stripe provides us with transaction confirmation data, including transaction identifiers and payment status, so that we can credit your account and maintain financial records.

4. How We Use Your Information

We use the information we collect for the following purposes:

To Provide and Operate the Services. We use your account information to authenticate you, your enrollment information to deliver courses, and your User Data to operate the i4ml platforms.

We transmit your prompts, documents, and other inputs to third-party AI providers (including OpenAI and Anthropic) as necessary to process your requests and generate outputs.

To Administer the Credit System. We use credit transaction records to track your credit balance, process credit purchases, meter usage of platform features, and prevent abuse.

To Process Payments. We use Stripe transaction references to reconcile purchases, issue credits, and maintain financial records.

To Communicate with You. We use your email address to send transactional communications, including account verification emails, password reset emails, purchase confirmations, account deactivation notices, and notifications required by our Terms and Conditions (such as material changes to the Terms or data deletion notices). We may also send you educational and product communications; you may opt out of non-transactional emails at any time using the unsubscribe mechanism provided in those emails.

To Improve the Services. We use anonymized and aggregated usage data — such as aggregate feature utilization, credit consumption patterns, and error rates — to analyze, improve, and develop the Services. This anonymized data does not identify individual users and does not include your User Data, User Workflows, or User Outputs in identifiable form.

To Measure Learning Outcomes. We use pre-course and post-course assessment data in aggregated, anonymized form to measure educational effectiveness and improve course design.

To Ensure Security and Prevent Abuse. We use log data, IP addresses, and session data to detect and prevent unauthorized access, enforce rate limits (including registration rate limiting and per-user API rate limiting), investigate security incidents, and enforce our Terms and Conditions.

To Comply with Legal Obligations. We use and retain information as necessary to comply with applicable laws, respond to lawful requests from public authorities, and establish, exercise, or defend legal claims.

5. How We Share Your Information

We do not sell your personal information. We do not disclose personal information to third parties for their direct marketing purposes. We share your information only in the following circumstances:

5.1 Third-Party AI Providers

When you use the i4ml platforms, your prompts, documents, and other inputs are transmitted to third-party AI providers (currently OpenAI and Anthropic) for processing. These transmissions are necessary to generate AI outputs on your behalf. The handling of your data by these providers is subject to their respective privacy policies and terms of service.

If you use model fine-tuning features, your training datasets are transmitted to our external fine-tuning provider. The provider's data handling policy governs the retention and use of your fine-tuning data.

We do not control the data practices of third-party AI providers. We encourage you to review their privacy policies. For this reason, as stated in our Terms and Conditions, you agree not to upload highly confidential data, protected health information (PHI), personally identifiable information of third parties, or data you are legally or contractually prohibited from disclosing to third-party services.

5.2 Payment Processor

Payment transactions are processed by Stripe. When you initiate a purchase, you are directed to Stripe's hosted checkout pages, where you provide your payment information directly to Stripe. Stripe's handling of your payment data is governed by Stripe's privacy policy. No payment card data is transmitted to, processed by, or stored on our systems.

5.3 Hosting and Infrastructure Providers

The Services are hosted on managed infrastructure provided by Replit (application hosting) and Neon (PostgreSQL database hosting). These providers have access to data stored on their infrastructure as necessary to provide their hosting services. Data at rest is encrypted using AES-256 encryption provided by the hosting infrastructure.

5.4 Platform Administrator Access

i4ml's designated platform administrator has access to account information (name, email, account type, credit balance, last active date) and the ability to manage accounts (including adjusting credit balances, deactivating accounts, and removing accounts) for the purposes of platform operation, user support, credit management, and enforcement of the Terms and Conditions. Platform administrator access is restricted to a single designated individual whose account is protected by mandatory two-factor authentication (TOTP).

5.5 Project Sharing (User-Initiated)

The i4ml platforms allow you to share your projects with other users. When you share a project, the recipient gains access to the project's contents — including artifacts, documents, RAG knowledge base data, and interaction logs — at the permission level you grant (viewer: read-only; collaborator: read and write). This is not i4ml sharing your data with a third party; it is you choosing to share your own data with another platform user through a platform feature under your control. You may revoke sharing access at any time.

5.6 Organizational Administrators

If you access the Services through an organizational account, the organization's designated administrator has viewer-level access to all organizational projects by default, including the ability

to view project activity and aggregate credit consumption within the organization. Organizational administrators do not have access to your personal account, personal projects, or personal credit balance.

5.7 Legal Requirements and Protection of Rights

We may disclose your information if we believe in good faith that disclosure is necessary to (a) comply with applicable law, regulation, legal process, or governmental request; (b) enforce our Terms and Conditions; (c) detect, prevent, or address fraud, security, or technical issues; or (d) protect the rights, property, or safety of i4ml, our users, or the public.

5.8 Business Transfers

In the event of a merger, acquisition, reorganization, bankruptcy, or other sale of all or a portion of our assets, your personal information may be transferred as part of the transaction. We will notify you via email or a prominent notice on the Services of any change in ownership or uses of your personal information, as well as any choices you may have regarding your personal information.

5.9 With Your Consent

We may share your information for purposes not described in this Privacy Policy with your explicit consent.

6. Data Security

We implement technical and organizational measures designed to protect your personal information against unauthorized access, alteration, disclosure, or destruction. These measures include:

Encryption. All data in transit is protected by HTTPS with HTTP Strict Transport Security (HSTS) enforced. Data at rest is encrypted using AES-256 encryption provided by our infrastructure providers. Passwords are hashed using bcrypt with a cost factor of 12.

Access Control. Access to user data is enforced through project-level isolation. Each project's data is scoped through database-level access controls, ensuring that users can only access projects they own, that belong to their organization, or that have been explicitly shared with them. RAG knowledge base embeddings are stored in project-scoped namespaces to prevent cross-project data retrieval.

Authentication Security. Platform administrator accounts require time-based one-time password (TOTP) two-factor authentication. Sessions expire after 24 hours of inactivity. Session cookies are configured as secure, httpOnly, and sameSite=lax.

Security Headers. The platforms implement security headers including X-Frame-Options (DENY), X-Content-Type-Options (nosniff), Strict-Transport-Security, Referrer-Policy, and Content-Security-Policy to protect against common web vulnerabilities.

Rate Limiting. Registration and API requests are rate-limited to prevent abuse and protect platform integrity.

Payment Security. All payment processing occurs on Stripe's PCI-DSS-compliant hosted checkout pages. No payment card data is transmitted to, processed by, or stored on our systems. Stripe webhook signatures are validated to prevent unauthorized transaction manipulation.

Incident Response. We maintain an incident response procedure to detect, investigate, contain, and remediate security incidents in a timely manner. In the event of a data breach, notification procedures are described in Section 9.

While we implement these measures to protect your data, no method of transmission over the Internet or electronic storage is completely secure. We cannot guarantee the absolute security of your information.

7. Data Retention

We retain your information for the following periods:

Account Information. Your account information is retained for the lifetime of your account. Following account deletion, your data is retained for ninety (90) days to allow for recovery. You are notified fourteen (14) days before permanent deletion. After the 90-day retention period, your data is permanently deleted from production systems, subject to the backup retention provisions described below.

User Data, User Workflows, and User Outputs. Retained for the lifetime of the associated project. When a project is deleted, it enters a 30-day soft-delete window during which it can be recovered. After the soft-delete period, project data is permanently deleted from production systems. When your account is deleted, the retention schedule described in the preceding paragraph applies.

Vector Embeddings (RAG). Stored in project-scoped namespaces and retained for the lifetime of the associated project. Deleted when the project is deleted.

Credit Transaction Records and Payment Records. Retained as necessary to comply with applicable tax, accounting, and financial reporting obligations, including U.S. federal tax record-keeping requirements. i4ml reviews financial record retention periodically and will delete records when no legal obligation requires their continued retention.

Fine-Tuned Model Adapters. Metadata is retained for the project lifetime. The adapters themselves are stored by the external fine-tuning provider and are subject to the provider's

retention policy. Adapters are included in pre-deletion data exports and removed on the same schedule as the associated account or project.

Interaction Logs. Platform interaction logs (prompts, tool invocations, workflow executions) are retained for the project lifetime to support platform functionality, governance, and your ability to review past interactions.

Server Logs. Standard server access logs (IP addresses, request metadata) are retained for ninety (90) days and then deleted.

7.1 Backup Retention

The platforms maintain database backups for disaster recovery purposes. These backups include continuous point-in-time recovery (retained for the duration of our hosting plan's recovery window, currently up to 30 days) and daily compressed database exports (retained for 14 days). As a result, data that has been deleted at the application level may persist in encrypted backups for up to 30 days following its deletion from production systems. Backup data is encrypted at rest, subject to the same access controls as production data, and is not used for any purpose other than disaster recovery. Backups are overwritten on a rolling schedule, and no data is extracted from backups except in the event of a disaster recovery operation. i4ml does not restore individual user data from backups upon request after the application-level retention period described in this section has expired.

8. Your Rights and Choices

8.1 All Users

Regardless of your location, you have the following rights:

Access and Export. You may access and export your User Data, User Workflows, and User Outputs at any time using the platforms' built-in export functionality or by contacting us at info@i4ml.com, subject to platform availability. We will make commercially reasonable efforts to maintain export functionality and to provide your data in a standard, portable format. Before account deletion, the platform provides a downloadable archive of all personal data, including projects, artifacts, transaction history, and fine-tuned model adapters.

Correction. You may update your account information, including your display name and email address (with re-verification), through the platforms' self-service account management features.

Deletion. You may request deletion of your account and all associated data by following the account deletion procedure in the platform or by contacting us at info@i4ml.com. Deletion follows the retention schedule described in Section 7, including the backup retention provisions in Section 7.1.

Communication Preferences. You may opt out of non-transactional emails at any time using the unsubscribe mechanism provided in those emails. You cannot opt out of transactional

communications necessary for account operation (such as verification emails, security notices, and deletion notifications).

8.2 Residents of the European Economic Area (EEA) and the United Kingdom (UK)

If you are a resident of the EEA or UK, the General Data Protection Regulation (GDPR) and the UK GDPR provide you with additional rights. The legal bases for our processing of your personal data are as follows:

Performance of a Contract. We process your account information, enrollment data, payment data, and User Data as necessary to perform our contractual obligations to you under the Terms and Conditions — that is, to provide you with the Services you have requested.

Legitimate Interests. We process usage data, log data, and anonymized analytics data on the basis of our legitimate interests in operating, securing, and improving the Services, provided that these interests are not overridden by your data protection rights.

Legal Obligation. We process and retain certain information (such as financial records) as necessary to comply with applicable legal obligations.

Consent. Where we send you non-transactional marketing or educational communications, we do so on the basis of your consent. You may withdraw consent at any time by unsubscribing.

In addition to the rights described in Section 8.1, you have the following rights under the GDPR:

Right to Restriction of Processing. You may request that we restrict the processing of your personal data in certain circumstances, such as when you contest the accuracy of your data or when you have objected to processing pending verification of our legitimate grounds.

Right to Object. You may object to the processing of your personal data where we rely on legitimate interests as the legal basis. We will cease processing unless we demonstrate compelling legitimate grounds that override your interests, rights, and freedoms.

Right to Data Portability. You have the right to receive your personal data in a structured, commonly used, and machine-readable format and to transmit that data to another controller. The platforms' data export functionality is designed to facilitate this right.

Right to Lodge a Complaint. You have the right to lodge a complaint with a supervisory authority in the EEA member state or UK country of your habitual residence, place of work, or place of the alleged infringement.

International Data Transfers. Your personal data is processed and stored in the United States. If you are located in the EEA or UK, we implement Standard Contractual Clauses (SCCs) adopted by the European Commission or other appropriate transfer mechanisms as required by applicable law, supplemented by the technical safeguards described in Section 6 of this Privacy Policy. Where

the transfer is necessary for the performance of our contract with you, we additionally rely on Article 49(1)(b) GDPR as a basis for the transfer.

Data Protection Officer. Given the nature and scale of our current data processing activities, i4ml has not appointed a Data Protection Officer (DPO). If you have questions or concerns about our data practices, please contact us using the information provided in Section 15. We will review the need for a DPO appointment as the scope of our processing activities evolves.

8.3 Residents of California

If you are a resident of California, the California Consumer Privacy Act (CCPA), as amended by the California Privacy Rights Act (CPRA), provides you with additional rights.

Right to Know. You have the right to request that we disclose the categories and specific pieces of personal information we have collected about you, the categories of sources from which the information was collected, the business or commercial purposes for collection, and the categories of third parties with whom we share your personal information.

Right to Delete. You have the right to request the deletion of personal information we have collected from you, subject to certain exceptions.

Right to Correct. You have the right to request correction of inaccurate personal information.

Right to Opt-Out of Sale or Sharing. We do not sell your personal information, nor do we share your personal information for cross-context behavioral advertising purposes, as those terms are defined under the CCPA/CPRA.

Right to Non-Discrimination. We will not discriminate against you for exercising your CCPA/CPRA rights.

Categories of Personal Information Collected. For CCPA purposes, the categories of personal information we collect include: identifiers (name, email address, IP address); commercial information (purchase records, credit transactions); internet or other electronic network activity information (usage data, log data, interaction logs); and professional or employment-related information (to the extent you provide it in course enrollment or assessments).

Shine the Light (California Civil Code §1798.83). We do not disclose personal information to third parties for their direct marketing purposes. If you are a California resident and have questions about this practice, you may contact us at info@i4ml.com.

To exercise your rights under the CCPA/CPRA, contact us at info@i4ml.com or at the mailing address provided in Section 15. We will verify your identity before processing your request.

8.4 Residents of Other Jurisdictions

If you reside in a jurisdiction with applicable data protection legislation not specifically addressed above (including but not limited to Canada, Brazil, Australia, or other jurisdictions with comprehensive privacy laws), we will comply with the applicable requirements of such laws. To exercise your rights, please contact us at info@i4ml.com.

9. Data Breach Notification

In the event that we become aware of a security breach that results in the unauthorized access to, disclosure of, or loss of your personal information, we will take the following steps:

Investigation and Containment. We will promptly investigate the incident to determine its scope and impact, and take immediate steps to contain the breach and prevent further unauthorized access.

Notification to Affected Users. We will notify affected users without unreasonable delay and in compliance with applicable law. The notification will include: (a) a description of the nature of the breach; (b) the categories of personal information affected; (c) a description of the measures we have taken or propose to take to address the breach; (d) recommendations for steps you can take to protect yourself; and (e) contact information for further inquiries.

Notification to Regulatory Authorities. Where required by applicable law, we will notify the relevant regulatory authorities within the time periods prescribed by those laws. For users subject to the GDPR, we will notify the relevant supervisory authority within 72 hours of becoming aware of a breach that is likely to result in a risk to individuals' rights and freedoms, except where the breach is unlikely to result in such a risk.

Record-Keeping. We will maintain records of all data breaches, including those that do not trigger notification obligations, as part of our incident response documentation.

The specific notification timelines and procedures may vary depending on the nature of the breach and the applicable legal requirements. Nothing in this section limits our obligations under applicable data breach notification statutes, which shall control to the extent they impose more specific requirements. Nothing in this section creates an independent basis for liability beyond the limitations set forth in the Terms and Conditions. i4ml's liability for any data breach, including any failure to comply with the notification obligations described in this section, is subject to the limitation of liability provisions in Section 14 of the Terms and Conditions.

10. Third-Party AI Provider Data Practices

Because the i4ml platforms rely on third-party AI providers for core functionality, we want to be transparent about how your data flows to these providers.

What is transmitted. When you execute a prompt, run a workflow, query a RAG pipeline, or deploy an agentic workflow, the inputs you provide (including prompts, context documents, and retrieved knowledge base excerpts) are transmitted to the relevant AI provider's API for processing.

What is not transmitted. Your account information (name, email, password) is not transmitted to AI providers. Your credit balance and payment information are not transmitted to AI providers. Only the specific inputs required for the AI operation are transmitted.

Provider data practices. Each AI provider has its own policies regarding data retention, data use for model training, and data security. As of the effective date of this Privacy Policy, the providers we integrate with include OpenAI and Anthropic. We encourage you to review their respective privacy policies and terms of service. As of the effective date of this Privacy Policy, the API terms of our current providers state that customer API inputs are not used for model training. We review provider terms periodically; if a provider materially changes its data practices, we will update this Privacy Policy accordingly.

Fine-tuning data. Training datasets submitted for fine-tuning are uploaded to the external fine-tuning provider via its API. The provider's data handling policy governs how that data is stored, processed, and retained. We provide metadata about your fine-tuning jobs but do not independently store copies of your training datasets beyond what is necessary for transmission.

11. Cookies and Similar Technologies

Session Cookies. We use a single session cookie to maintain your authenticated session. This cookie is strictly necessary for the operation of the Services. It is configured as secure, httpOnly, and sameSite=lax, and it does not contain personal information beyond a session identifier. The cookie expires at the end of your session or after 24 hours of inactivity.

We do not use third-party tracking cookies, advertising cookies, or cross-site tracking technologies on the i4ml platforms. We do not serve targeted advertisements and do not participate in advertising networks.

Analytics. We do not use third-party analytics services that place cookies on your device. Our analytics are based on server-side log data as described in Section 3.2.

12. Do Not Track Signals

Some web browsers transmit "Do Not Track" (DNT) signals. Because there is no uniform standard for interpreting DNT signals, we do not currently respond to DNT signals. However, as stated in Section 11, we do not use third-party tracking cookies or cross-site tracking technologies.

13. Children's Privacy

The Services are not directed to individuals under the age of eighteen (18). We do not knowingly collect personal information from children under 18. If we become aware that we have collected personal information from a child under 18, we will take steps to delete that information promptly. If you believe that we have inadvertently collected information from a child under 18, please contact us at info@i4ml.com.

14. Changes to This Privacy Policy

We may update this Privacy Policy from time to time. For material changes, we will provide you with notice at least thirty (30) days before the changes take effect, via email to the address associated with your account or through a prominent notification within the Services. For non-material changes, we will revise the "Last Updated" date at the top of this page. Your continued use of the Services after the effective date of the revised Privacy Policy constitutes your acceptance of the changes.

We encourage you to review this Privacy Policy periodically. Previous versions of this Privacy Policy are available upon request.

15. Contact Information

If you have questions about this Privacy Policy, wish to exercise your data protection rights, or have a complaint about our data practices, please contact us at:

Data Privacy Inquiries The Institute of Machine Learning 113 Mill Plain Rd, #1102, Danbury, CT 06811 Email: info@i4ml.com Website: www.i4ml.com

For users in the EEA or UK, if you are not satisfied with our response to your inquiry, you have the right to lodge a complaint with your local supervisory authority.