AI Fabrik

Privacy Policy

Effective date: June 16, 2026 Last updated: June 16, 2026

AI Fabrik, Inc. ("AI Fabrik," "we," "us," or "our") provides AI cloud and GPU-as-a-Service (“GPUaaS”) infrastructure and AI inference services to enterprise customers through our platform, APIs, and related infrastructure (collectively, the “Services”). This Privacy Policy explains how we collect, use, disclose, retain, and protect personal data in connection with our websites, sales activities, customer onboarding, and provision of the Services.

This Policy applies to personal data we process as a controller, for example, when you visit aifabrik.com, inquire about our Services, complete our Customer Information Authorization Form, register an account, attend our events, or otherwise interact with us. When we process personal data on behalf of a Customer as part of delivering our Services (“Customer Data”), we act as a processor or service provider under our Customer Agreement. In that role, the Customer’s privacy policy governs the personal data they upload, generate, or process using the Services.

Capitalized terms not defined here have the meanings given in our Customer Agreement or Acceptable Use Policy. Where applicable law affords greater rights or imposes stricter obligations, that law controls.

Quick reference	Where to go
Privacy questions, data subject requests	privacy@aifabrik.com
Compliance and KYC questions	compliance@aifabrik.com
Security, abuse, or incident reports	security@aifabrik.com / abuse@aifabrik.com
Data deletion / removal requests	trust@aifabrik.com
Data Protection Officer (DPO)	dpo@aifabrik.com

1. Scope and our roles under data-protection law

This Policy describes how AI Fabrik processes personal data in three distinct capacities:

- **As a controller —** for account, billing, and operational data, including data we collect from website visitors, prospective customers, authorized signers, beneficial owners, account administrators, billing contacts, technical owners, event attendees, and personnel of our

Customers during sales, onboarding, KYC, sanctions screening, billing, security operations, and support.

- **As a processor for GPUaaS workloads —** for Customer Data that a Customer (or its end users) submits to or generates through our GPU, storage, networking, and managed-service offerings. We process this Customer Data only on documented instructions from the Customer and pursuant to the Customer Agreement. The Customer is the controller for that data and is responsible for the lawful basis, notices, and consents covering it.
- **As a service provider for AI inference —** for inference requests (prompts, inputs, outputs, and model responses) submitted through our inference APIs. We process inference content solely on Customer instructions, under our Zero Data Retention model described in Section 4. AI Fabrik does not sell personal data, does not operate an advertising business, and does not use Customer Data or inference content to train our own models.

If you are an end user, employee, contractor, or beneficial owner of one of our Customers and have questions about how that Customer uses the Services or your data, please contact the Customer directly.

2. Personal data we collect

The personal data we collect depends on how you interact with us. We collect personal data directly from you, automatically through your use of our websites and Services, and from third-party sources used for identity verification, sanctions screening, and fraud prevention.

2.1 Information you provide directly

- **Identity data:** legal name, business email, business phone, job title, employer, and country of residence or work.
- **Account credentials and authentication data:** usernames, passwords (hashed and salted), SSO identifiers, multi-factor authentication (MFA) tokens, SSH key fingerprints, API keys, and recovery information.
- **Business and account data:** the information requested in our Customer Information Authorization Form, including entity legal name, jurisdiction, tax/VAT/GST identifiers, principal business address, operating countries, website and domains, business description and industry, parent and affiliate relationships, and account roles (admin, user, API/service).
- **Ownership and control data:** names, roles, ownership percentages, nationality, and country of residence for individuals who own or control 25% or more of a Customer entity, plus any individual with substantial control over a Customer or its account.
- **Know Your Customer (KYC) verification data:** government-issued ID documents (or partially obscured copies), entity formation evidence (certificates of incorporation or equivalent registry extracts), ownership and cap-table evidence, board or signer authorizations, beneficial-ownership declarations, and identity-verification tokens or results provided by approved KYC vendors.

- **Workload and use-case data:** the information provided in the Intended Workload and Capacity Request and AI Model Training / Inference Addendum sections of our Customer Information Authorization Form, including primary workload type, business purpose, requested GPU type and quantity, estimated compute, model parameters and license, base model identifiers, technical architecture diagrams, and end-use statements.
- **Billing and payment data:** legal billing entity, billing address, tax ID, purchase orders, budget owners, payment method (invoice/PO, ACH/wire, credit card, marketplace), bank or wire references, source of funds, expected monthly spend, and transaction records. Credit-card payments are processed by Stripe; we do not store full card numbers. We may receive limited billing metadata such as last-four digits, card brand, payment status, and transaction confirmations.
- **Contact, support, and communications:** information you provide when you contact us by email, sales chat, support tickets, phone, or web form, including the content of those communications and any attachments.
- **Event and marketing data:** registration information for webinars, workshops, conferences, demos, and other events; survey responses; and marketing preferences.
- **Sanctions, export, and end-use declarations:** the certifications you make in Section 8 of the Customer Information Authorization Form and any supporting evidence you provide.

2.2 Information we collect automatically

When you visit our websites or use the Services, we and our service providers automatically collect:

- **Device and technical data:** IP address, browser type and version, operating system, device identifiers, language settings, time zone, and referring or exit URLs.
- **Usage and telemetry data:** pages visited, features and APIs called, sessions and clickstreams, login and authentication events, account identifiers, model identifiers, token usage counts, timestamps of requests, error codes, GPU and storage utilization, network egress patterns, error and crash reports, performance metrics (latency, throughput, uptime), and other operational signals required to deliver, secure, and improve the Services. *This telemetry does not include the content of prompts, inputs, outputs, or model responses for inference workloads operating under our Zero Data Retention model (see Section 4).*
- **Security and abuse signals:** authentication anomalies, impossible-travel and VPN/anonymizer indicators, account-takeover indicators, scanning or denial-of-service patterns, malware signatures observed in egress, and other signals used to detect, investigate, and prevent abuse and security incidents.
- **Cookies and similar technologies:** we use first-party and selected third-party cookies, pixels, SDKs, and local storage for authentication, security, analytics, and (with your consent where required) marketing. See Section 9 for details.

2.3 Information from third parties

To verify identity, screen for sanctions and fraud risk, and protect our Services, we receive personal data from:

- **Identity-verification and KYC providers** that we engage to confirm the identity of authorized signers, beneficial owners, and account administrators.
- **Restricted-party screening and sanctions-list providers** (including data sourced from OFAC SDN, BIS Entity List, Denied Persons List, and UN, EU, UK, and other applicable lists).
- **Payment processors, banks, and credit-reference providers** for payment validation, fraud prevention, and credit assessment.
- **Public and commercial registries** (corporate registries, company-information services, regulatory filings, court records) for entity verification and ownership analysis.
- **Threat-intelligence and security providers** for IP reputation, malware detection, and abuse indicators.
- **Marketing, analytics, and event partners,** where you have engaged with us through their platforms.
- **Referrers and resellers** who introduce you to AI Fabrik, subject to their own privacy notices.

2.4 Submissions on behalf of others

If you submit personal data about another person — for example, a beneficial owner, account administrator, billing contact, or technical owner — you confirm that you are authorized to share that information with us and that the individual has been given notice of, and where required has consented to, the processing described in this Policy.

2.5 Sensitive data

We do not seek to collect sensitive personal data (such as racial or ethnic origin, religious beliefs, health data, biometric data, precise geolocation, or government-issued identifiers beyond what is required for KYC). Please do not submit sensitive personal data to us unless we expressly request it for a specific compliance purpose. Where we must process sensitive data (for example, partially obscured government ID images for KYC), we apply enhanced safeguards, including encryption at rest and access restricted to our compliance team. We delete the government-ID image shortly after identity verification is complete, and retain only the verification and screening record (such as the result, date, and lists checked) for the period required by applicable export-control, sanctions, and other legal obligations (see Section 7).

3. Why we process personal data and our legal bases

We process personal data for the purposes set out below. Where the EU/UK GDPR or similar laws apply, we identify our legal basis. We do not rely on legitimate interests where those interests are overridden by your rights and freedoms.

Purpose	Legal basis (EEA/UK)	Examples
Provide the Services: create and administer accounts, provision GPU and storage capacity, enable authentication and access control, process payments, send service notifications, and provide support.	Performance of a contract; legitimate interests in operating the Services.	Onboarding a new Customer, issuing API keys, provisioning a B300 cluster, billing for usage, responding to support tickets.
Verify identity and screen for risk: perform KYC, beneficial-ownership verification, sanctions and restricted-party screening, fraud detection, and export-control review.	Legal obligation; legitimate interests in preventing fraud, abuse, and unlawful use of GPU compute.	Running OFAC, BIS Entity List, EU and UK consolidated-list checks against signers and beneficial owners; checking ECCN/ITAR classification for model weights.
Comply with law: meet export-control, sanctions, anti-money-laundering, tax, accounting, and other legal and regulatory obligations applicable to AI cloud and GPU-as-a-Service providers.	Legal obligation.	Responding to BIS, OFAC, or other regulator inquiries; retaining records to evidence export-compliance decisions; lawful disclosure to authorities.
Protect security and prevent abuse: detect, investigate, and respond to unauthorized access, malware, denial-of-service activity, scanning, account takeover, crypto-mining, and other Acceptable Use Policy violations.	Legal obligation; legitimate interests in securing the Services and protecting Customers and third parties.	Reviewing flow logs for egress anomalies, suspending compromised accounts, investigating suspected exploit-generation workloads.
Operate and improve the Services: monitor capacity, reliability, and performance; capacity-plan and forecast; conduct internal analytics; develop new features.	Legitimate interests in operating and improving the Services. We use aggregated or de-identified data wherever possible.	Aggregating GPU utilization across the fleet, modeling PUE, analyzing inference-endpoint latency.
Marketing and events: send updates about products, features, events, and offerings; measure marketing	Consent (where required); legitimate interests in marketing to existing	Sending a newsletter, inviting you to an industry event, retargeting on advertising platforms with consent.

effectiveness; personalize content where permitted.	business contacts, subject to opt-out.	
Establish, exercise, or defend legal claims; manage corporate transactions; protect rights, property, and safety.	Legitimate interests; legal obligation as applicable.	Responding to subpoenas, defending litigation, due diligence in financing or M&A.

Automated decision-making. We use automated processing for identity verification, sanctions and restricted-party screening, and fraud detection. These checks support human review; we do not make decisions producing legal or similarly significant effects based solely on automated processing without human involvement. Where the EU/UK GDPR applies, you have the rights described in Article 22.

4. Zero Data Retention and AI-specific data practices

Because AI Fabrik provides infrastructure for AI training, fine-tuning, and inference, we apply additional safeguards specific to AI workloads. The most important of these is our Zero Data Retention commitment for inference content.

4.1 Zero Data Retention for inference content

Our inference Services are designed as stateless compute services. By default:

- Prompts, inputs, outputs, and model responses are processed in memory.
- AI Fabrik does not store inference content.
- AI Fabrik does not log prompts or responses.
- AI Fabrik does not use inference content for model training or to improve our own models.

This Zero Data Retention model applies to prompts, inputs, outputs, and model responses. It does not apply to the limited operational metadata described in Section 2.2 (such as account identifier, model identifier, token usage counts, request timestamps, error codes, and IP address), which we collect to operate, secure, and bill the Services.

4.2 GPUaaS Customer Data

- **Customer Data and model artifacts are Customer-controlled.** Datasets, model weights, prompts, fine-tuning data, outputs, and checkpoints that a Customer uploads or generates on the GPUaaS Services are Customer Data. We do not use Customer Data to train or improve our own models, and we do not access Customer Data except as necessary to provide, secure, and support the Services or as required by law.
- **Tenant and workload isolation.** We operate with logical and, where contractually committed, physical isolation between Customer workloads. Provider personnel access to Customer compute environments is least-privilege, logged, and subject to internal review.

- **Operational telemetry, not Customer content.** We collect operational and performance telemetry (GPU utilization, interconnect health, system events, scheduler decisions) needed to operate clusters at scale. This telemetry is not the substantive content of training data, prompts, or model outputs.

4.3 Compliance review for high-risk AI workloads

- **Enhanced due diligence.** For large training runs, frontier-model access, or workloads flagged by the AI Model Training / Inference Addendum (including those touching D:5 countries, cyber-offensive use cases, dual-use research, or restricted end users), we conduct enhanced due diligence and may decline, condition, or escalate the engagement to legal and export-compliance review.
- **No bypass of safety, telemetry, or abuse monitoring.** Consistent with our Acceptable Use Policy, we do not approve workloads designed to bypass model safety controls, content filtering, telemetry, logging, or abuse monitoring.

5. How and with whom we share personal data

We share personal data only where necessary for the purposes in Section 3 and only with recipients bound by appropriate confidentiality and data-protection obligations. We do not sell personal data, and we do not share personal data for cross-context behavioral advertising, except as expressly described in this Policy.

5.1 Categories of recipients

- **Service providers and processors:** vendors that operate our cloud infrastructure, identity and access management, billing and payments (including Stripe for credit-card processing), support ticketing, analytics, marketing automation, communications, and security monitoring, under contracts that require them to process personal data only on our instructions and with appropriate safeguards.
- **KYC, sanctions-screening, and fraud-prevention providers:** to verify identity, screen against restricted-party lists, validate payment instruments, and assess fraud risk.
- **Data-center, network, and hardware partners:** co-location providers and operators of the facilities where our infrastructure is hosted, and connectivity and interconnect partners. These parties operate the physical and network layer and have limited access to operational metadata necessary for that role.
- **Auditors, advisors, and insurers:** accountants, legal counsel, compliance consultants, security auditors, and insurance providers, subject to professional confidentiality.
- **Public authorities and law enforcement:** where required to comply with a lawful request, court order, subpoena, or applicable export-control, sanctions, anti-money-laundering, or tax obligation, or where we have a good-faith belief that disclosure is necessary to protect rights,

safety, property, or the integrity of the Services. We assess each request for legal validity and narrow the disclosure to what the law requires.

- **In a corporate transaction:** in connection with a merger, acquisition, financing, reorganization, sale of assets, or similar transaction (including diligence). Any successor will be bound by privacy commitments at least as protective as this Policy or will provide affected individuals with notice and choice where required.
- **With your direction:** where you instruct us to share data with a third party (e.g., a reseller or systems integrator you have engaged to manage your AI Fabrik account).
- **Sub-processors:** we use third-party sub-processors to host and operate the Services, process payments, verify identity, screen for sanctions, and provide support, analytics, and security monitoring. We will provide information about our sub-processors on request.

5.2 Resellers, MSPs, and managed access

Where a Customer engages a reseller, managed service provider, or systems integrator to access AI Fabrik on its behalf, that party is required by contract to verify its sub-customers, flow down our Acceptable Use, sanctions, and export terms, and protect personal data with safeguards no less protective than ours. The reseller is the direct point of contact for its sub-customers' personal data.

6. International data transfers

AI Fabrik operates and processes data primarily in the United States. Because we serve a global Customer base and use service providers in multiple jurisdictions, your personal data may be transferred to, stored, or processed in countries other than the one in which you reside, including countries that may have data-protection rules different from your own.

Where we transfer personal data from the EEA, the UK, or Switzerland to a country not recognized as offering an adequate level of protection, we rely on appropriate safeguards, including:

- the European Commission's Standard Contractual Clauses (SCCs) and their UK and Swiss equivalents (e.g., UK International Data Transfer Agreement or Addendum);
- supplementary technical, contractual, and organizational measures, including encryption in transit and at rest and access controls;
- vendor due diligence and transfer-impact assessments where required by law.

Customers may, depending on the Services purchased, select a region in which their workloads run. Region selection controls the primary location of Customer Data processing; certain operational data and metadata necessary to deliver the Services may be processed in other regions for resilience, support, and security purposes, as described in our customer agreement.

Where we transfer personal information of individuals in China to the United States, we do so subject to the separate consent and safeguards described in Section 11.4 (China — PIPL).

7. Data retention

We retain personal data only for as long as necessary to fulfill the purposes for which it was collected, including to satisfy legal, accounting, tax, export-control, or reporting requirements, to enforce our agreements, and to defend against legal claims. Specific retention periods reflect:

- the nature, sensitivity, and volume of the data;
- the purposes for which we process it and whether those purposes can be achieved by other means;
- applicable legal, regulatory, and contractual retention requirements (for example, export-control and AML records);
- the risk of harm from unauthorized use or disclosure.

Indicative retention windows:

- **Account and billing records:** retained for operational and legal purposes, typically up to seven (7) years in accordance with applicable legal and regulatory requirements, including tax, accounting, AML, and export-control recordkeeping.
- **KYC and beneficial-ownership documentation:** retained for the term of the Customer relationship and for the period required by export-control, sanctions, and AML rules thereafter. Government-ID images are deleted shortly after identity verification; the verification and screening record is retained for that required period.
- **Usage and operational metadata:** retained for a limited period necessary for billing, fraud prevention, security, and capacity planning.
- **Security logs and abuse-investigation records:** retained for the period necessary to detect and investigate incidents and as required by law.
- **Inference content (prompts, inputs, outputs, model responses):** not retained. See Section 4.1 (Zero Data Retention).
- **Marketing data:** retained until you unsubscribe or opt out, and for a short additional period to honor your preferences.

When personal data is no longer needed, we delete, anonymize, or aggregate it. Customers may request deletion of their account data through the channels in Section 14, subject to our legal-retention obligations. Customer Data is handled under the deletion and return terms of the Customer Agreement.

8. Security

We maintain administrative, technical, and physical safeguards designed to protect personal data from unauthorized access, disclosure, alteration, loss, and destruction. Our security program is aligned with industry-recognized frameworks and includes:

- encryption of data in transit (TLS) and at rest, with key management using provider-managed and (where supported) customer-managed keys;

- identity and access management with multi-factor authentication for administrators, least-privilege access, role-based permissions, and named accounts;
- network segmentation, tenant isolation, and operational monitoring of GPU compute and storage environments;
- vulnerability and patch management, secure software development practices, and internal security reviews;
- audit logging for administrative activity, with logs retained and reviewed in line with our security policies;
- physical security at the data centers where our infrastructure is hosted, including access controls, monitoring, and environmental safeguards;
- an incident-response program to investigate, contain, and remediate security incidents, and to notify affected parties as required by law and contract.

No method of transmission or storage is completely secure. While we work to protect personal data, we cannot guarantee its absolute security. Customers are responsible for safeguarding credentials, managing user access, and meeting their portion of the shared-responsibility model described in our Customer Agreement and Acceptable Use Policy.

8.1 Data breach notification

In the event of a confirmed data breach affecting personal data, AI Fabrik will notify affected Customers and, where required, regulators and individuals, in accordance with applicable law and our Customer Agreement.

9. Cookies and similar technologies

We use first-party cookies and selected third-party cookies, pixels, SDKs, and local storage on our websites for purposes including authentication and session management, security and abuse prevention, preferences, analytics, and (where you consent) marketing.

Where required by law (including in the EEA and UK), we obtain consent for non-essential cookies and allow you to manage your preferences. For more information about the specific cookies we use and how to manage them, contact us at privacy@aifabrik.com.

We do not currently respond to “Do Not Track” browser signals. Where required by U.S. state law, we honor recognized opt-out signals (such as Global Privacy Control).

10. Your rights and choices

Depending on where you live and the law that applies, you may have the following rights regarding personal data we hold about you:

- **Right to access** the personal data we process about you and to receive information about how we process it.
- **Right to rectification** of inaccurate or incomplete personal data.
- **Right to erasure ("right to be forgotten"),** subject to legal-retention and other exceptions.
- **Right to restrict or object to processing,** including objecting to direct marketing at any time.
- **Right to data portability,** to receive your personal data in a commonly used, machine-readable format.
- **Right to withdraw consent** where processing is based on consent (without affecting the lawfulness of processing before withdrawal).
- **Right to lodge a complaint** with a supervisory authority or other regulator with jurisdiction over your data.
- **Right to opt out** of "sales" or "sharing" of personal data and of targeted advertising and certain profiling, as defined under U.S. state laws. We do not sell personal data and do not engage in cross-context behavioral advertising as defined under those laws.

To exercise your rights, contact us at privacy@aifabrik.com. We may need to verify your identity before responding, and may decline requests where an exception applies (for example, where retention is required by law). We will respond within the time frame required by applicable law (typically within 30 to 45 days).

If you are an end user, employee, or contractor of a Customer and your request concerns Customer Data, please direct your request to the relevant Customer; we will support the Customer's response as required by the applicable Customer Agreement.

11. Region-specific disclosures

11.1 European Economic Area, United Kingdom, and Switzerland

Where the EU GDPR, UK GDPR, or Swiss FADP applies, AI Fabrik, Inc. is the controller for the processing described in this Policy. AI Fabrik does not maintain an establishment in the EEA, the UK, or Switzerland, and relies on Standard Contractual Clauses (and their UK and Swiss equivalents) for outbound transfers from those regions, as described in Section 6. We rely on the legal bases identified in Section 3. You may contact our Data Protection Officer at dpo@aifabrik.com or lodge a complaint with your local supervisory authority. Cross-border transfers from the EEA/UK/Switzerland are protected as described in Section 6.

11.2 United States — California and other state-privacy laws

If you are a California resident, the California Consumer Privacy Act, as amended by the CPRA ("CCPA"), gives you the rights described in Section 10. We have collected the categories of personal information described in Section 2 over the past 12 months from the sources described in Section 2.3 and for the

business purposes described in Section 3. We have disclosed those categories to the categories of recipients listed in Section 5. We do not sell personal information or share it for cross-context behavioral advertising, as those terms are defined under the CCPA.

Residents of Colorado, Connecticut, Delaware, Indiana, Iowa, Kentucky, Maryland, Minnesota, Montana, Nebraska, New Hampshire, New Jersey, Oregon, Tennessee, Texas, Utah, and Virginia have similar rights under their respective state privacy laws. To exercise these rights, including any right to appeal a denied request, contact us at privacy@aifabrik.com.

11.3 Other jurisdictions

We respect privacy rights provided under other applicable laws in jurisdictions in which we operate or have Customers.

11.4 China (PIPL)

Where we collect personal information from individuals located in the People's Republic of China — such as the authorized signers, beneficial owners, account administrators, and contacts of a prospective or current Customer — and transfer it to the United States, we do so in accordance with the Personal Information Protection Law (PIPL).

Cross-border transfer and separate consent. Onboarding requires transferring your personal information from China to AI Fabrik, Inc. in the United States, where it is hosted and processed. Before collection, we obtain your separate, specific consent to this transfer — distinct from your acceptance of this Policy — and inform you of the overseas recipient (AI Fabrik, Inc., United States), the purposes, the categories of personal information transferred, and how to exercise your rights with the recipient.

Sensitive personal information. Certain items collected for identity verification and compliance — such as government-issued ID documents — are sensitive personal information under PIPL. We collect them only where necessary for KYC, sanctions, and export-control compliance, obtain your separate consent for processing sensitive personal information, and apply enhanced safeguards.

Your rights. Subject to PIPL, you may access, correct, or delete your personal information, withdraw consent, and request an explanation of our processing rules. Contact privacy@aifabrik.com.

Transfer safeguards. We assess the volume and sensitivity of the personal information we transfer and apply the transfer conditions required under PIPL and the measures issued by the Cyberspace Administration of China. We maintain a personal-information protection impact assessment for these transfers and apply the encryption and access controls described in Section 8.

11.5 Governing law

Except where superseded by applicable data-protection law in the jurisdiction where you reside, this Privacy Policy is governed by the laws of the State of California, without regard to its conflict-of-laws principles.

12. Children

Our Services are intended for businesses and are not directed to children. We do not knowingly collect personal data from individuals under 18. If you believe a child has provided us with personal data, contact privacy@aifabrik.com and we will take appropriate steps to delete it.

13. Changes to this Policy

We may update this Policy from time to time. When we do, we will revise the “Last updated” date at the top, and where the changes are material, we will provide additional notice (such as email to account contacts or in-product notification) before the changes take effect. We encourage you to review this Policy periodically.

14. How to contact us

If you have questions about this Policy, our privacy practices, or your rights, contact us at:

AI Fabrik, Inc.

Attn: Privacy Office / Data Protection Officer

399 Bradford Street, Suite 105, Redwood City, CA 94063, USA

Email: privacy@aifabrik.com

Data Protection Officer: dpo@aifabrik.com

Compliance (KYC, export, sanctions): compliance@aifabrik.com

Security and abuse: security@aifabrik.com / abuse@aifabrik.com

Data deletion requests: trust@aifabrik.com