PRIVACY POLICY

FermTrading, Inc.

Effective Date: October 19, 2026

PLEASE READ THIS PRIVACY POLICY ("POLICY") CAREFULLY. IT DESCRIBES HOW FERMTRADING, INC. COLLECTS, USES, DISCLOSES, AND PROTECTS PERSONAL DATA IN CONNECTION WITH YOUR USE OF THE SERVICE.

THIS NOTICE EXPLAINS OUR PROCESSING. IT IS NOT BLANKET CONSENT OR A WAIVER OF PRIVACY RIGHTS. WHERE CONSENT IS REQUIRED, WE REQUEST IT SEPARATELY FOR THE RELEVANT PURPOSE.

RECITALS

WHEREAS, FermTrading, Inc. ("Company") operates a simulated trading evaluation platform under the brand name "Ferm" accessible at https://tryferm.com and through associated mobile applications (iOS and Android); and

WHEREAS, the Company collects and processes certain Personal Data from Users in connection with the provision of the Service; and

WHEREAS, the Company is committed to protecting the privacy and security of such Personal Data in accordance with applicable federal, state, and international privacy laws;

NOW, THEREFORE, the Company sets forth the following Privacy Policy governing the collection, use, disclosure, retention, and protection of Personal Data:

ARTICLE I - DEFINITIONS

1.1 "Biometric Data" means data relating to the physical characteristics of an individual that can be used to identify that person, including facial geometry extracted from photographs or live selfie captures.

1.2 "Company," "Ferm," "we," "us," or "our" means FermTrading, Inc., a Delaware C Corporation, EIN 42-3681083, Delaware File Number 10684811, with its principal place of business at 4335 Cadieux Road, Detroit, MI 48224, United States.

1.3 "Personal Data" means any information that is linked or reasonably linkable to an identified or identifiable natural person. Personal Data does not include aggregated, de-identified, or anonymized information from which individual identities have been removed.

1.4 "Platform" means the Ferm web terminal (https://tryferm.com) and the Ferm mobile applications (iOS and Android).

1.5 "Processing" means any operation performed on Personal Data, whether automated or manual, including

collection, recording, organization, structuring, storage, adaptation, alteration, retrieval, consultation, use, disclosure, dissemination, alignment, combination, restriction, erasure, or destruction.

1.6 "Service" means the Ferm platform, website, mobile applications, evaluation programs, funded simulation accounts, and all related services provided by the Company.

1.7 "User," "you," or "your" means any individual who accesses, registers for, or uses the Service.

ARTICLE II - CORPORATE INFORMATION

2.1 Data Controller. The entity responsible for the Processing of your Personal Data is:

FermTrading, Inc., 4335 Cadieux Road, Detroit, MI 48224, United States

2.2 Contact Information.

Purpose	Contact
Privacy and Data Rights Requests	privacy@ferm.trade
Legal Notices	legal@ferm.trade
General Support	hello@ferm.trade
Telephone	(313) 330-7308

ARTICLE III - PERSONAL DATA WE COLLECT

3.1 Information You Provide Directly

3.1.1 Account Creation. Ferm does not use a traditional registration form. Accounts are created implicitly upon your first successful login. The following data is collected at account creation:

Data Element	Collection Method	Storage
Email address	Email OTP, Google Sign-In, or Apple Sign-In	AES-256-GCM encrypted at rest; salted SHA-256 hash for lookup
Username	Auto-generated on first login; user may update	Plaintext
First name / Last name	Optional; from Google/Apple OAuth or profile update	AES-256-GCM encrypted at rest
Google or Apple subject ID	OAuth authentication flow	Yes
Authentication provider metadata	OAuth flows	Yes
Email verification timestamp	OAuth / email verification flow	Yes
Last login timestamp	Every successful login	Yes

Data Element	Collection Method	Storage
Referral attribution	ferm_ref cookie (30-day first-touch)	Yes (referrer user UUID)

3.1.2 Checkout and Purchases. When you purchase an evaluation, we collect: the challenge tier selected, optional promo code, the optional profit-split upgrade selection, the payment processor and (for crypto) pay currency selected, purchase amount, and your country code (2-character ISO). Payment is accepted through cryptocurrency rails (BTCPay Server and NOWPayments) and through card checkout processed by TailoredPay (NMI), including Apple Pay and Google Pay via Collect.js. Card numbers and CVV codes are entered only in TailoredPay hosted fields. We do not collect card numbers, CVV codes, wallet cryptograms, or cryptocurrency private keys on our servers.

3.1.3 Payout Information. To process performance-based payouts, we collect the payout destination details you provide on the Platform (such as a USD bank account for ACH/wire, or a USDC wallet address on a supported network), which are encrypted at rest. When a payout provider requires a current residential address and Persona has not already provided a complete address, Ferm may collect that address on the payout form and forward it to the payout provider for onboarding and compliance; Ferm does not store the street address in its database.

3.1.4 Funded Account Onboarding. Upon qualification for a funded account, we collect your typed legal name (electronic signature), raw IP address, User-Agent string, and store the signed agreement PDF in encrypted cloud storage.

3.1.5 Communications. When you contact us via email or support channels, we collect the content of your messages and your contact information. We also retain copies of the transactional and marketing emails we send you, together with delivery and open/engagement events reported by our email provider. If you use Arlo, our AI support assistant, on the website, in the mobile app or in Discord, we collect your messages, the account details you choose to share in the conversation, and the conversation history. A member of our support team may read and reply to the conversation.

3.1.6 Optional Content and Features. If you use the applicable features, we collect and store: trade journal notes you write on your trades; price alerts you configure (symbol, target price, optional note); your linked social profile details from X (Twitter), Discord, TikTok, and Instagram professional (Business or Creator) accounts (provider user ID, handle, display name, avatar URL), captured once at connection time; your notification preferences; and passkey (WebAuthn) credentials you register (credential ID, public key, and device name - never your biometric data, which stays on your device).

3.1.7 Loyalty and Family Program Data (referral / affiliate). We maintain your loyalty points balance and tier, Family (referral) attribution records, commission/XP award history, Family milestone tick grants, and milestone claim records in connection with the loyalty and Family programs. The Family program is Ferm's referral and affiliate program.

3.2 Information Collected Automatically

3.2.1 When you access or use the Platform, we automatically collect the following data:

Data	Method	Storage	Purpose
IP address	HTTP headers	Hashed for correlation; raw in necessary agreement and biometric-release evidence	Fraud detection, multi-account correlation, legal audit
IP-derived location (country/region)	Server-side lookup via ipinfo.io (fallback: ipwho.is)	Country code on user profile	Restricted-jurisdiction screening, compliance
Device ID	Client-generated UUID (X-Device-Id header)	Yes	Fraud detection, referral abuse detection
User-Agent	HTTP header	Yes (up to 500 characters)	Fraud correlation
Push notification tokens	Mobile app registration (APNs on iOS, FCM on Android)	Yes, per registered device	Delivery of account, trading, and payout notifications
Device integrity signals (mobile)	Jailbreak/root and emulator detection at payout request	Stored with the payout request	Payout fraud prevention
Login timestamps	Authentication events	Yes	Security, account management
Session cookie (ferm_session)	HttpOnly JWT	Browser cookie (not in database)	Authentication
Referral cookies (ferm_ref / ferm_web_ref)	Browser cookies after advertising permission	30-day expiry	Affiliate attribution
Pageviews, clicks, errors	PostHog analytics	PostHog US cloud	Product analytics, debugging
Session replay	PostHog (all text and inputs masked)	PostHog US cloud	UX debugging
Server/API logs	Console output	AWS CloudWatch (30-day retention)	Operations, security

3.2.2 Privacy Controls for Automated Collection. PostHog is configured with the following privacy safeguards: all form inputs are masked (maskAllInputs: true), password fields are masked, all rendered text is masked in session replay (maskTextSelector applied to every element) so values such as balances, PnL, and payout amounts are never captured, and sensitive URL query parameters (including code, token, email, otp, password, session, key, signature) are redacted prior to transmission.

3.3 Trading Activity Data

3.3.1 As a simulated trading platform, we extensively track and store your trading activity. Orders are not routed to live exchanges at any account stage; evaluation and funded accounts are fully simulated, and live accounts carry a capital commitment from us as described in Section 3.1.1 of the Terms and Conditions. The data we collect is the same at every stage:

Category	Data Stored
Account state	Balance, high-water mark, status, stage, phase, scaling level, profit share percentage, breach reason, payout holds

Category	Data Stored
Loyalty and Family (referral / affiliate)	Loyalty points and tier, Family (referral) attribution, commission and XP award records, Family milestone tick grants, and milestone claim records
Orders	Symbol, side, quantity, limit price, TP/SL prices, order status, timestamps
Trades	Symbol, side, lot size, open/close price, open/close time, commission, swap, realized P&L, news-exclusion flags
Risk metrics	Per-trade risk score, fraud flags, win rate, profit factor, average hold time, short-hold trade percentage
Equity snapshots	Time-series equity, balance, unrealized P&L, high-water mark, open position count
Daily snapshots	Per-day start/end balance and equity
Fraud detection	Latency-arbitrage signals, fraud event records with severity, admin review status

3.4 Information from Third Parties

3.4.1 Identity Verification (KYC). We utilize Persona (https://withpersona.com) to conduct KYC verification. Persona directly collects your government-issued photo ID, live selfie with liveness detection, and may collect or extract identity attributes (e.g., name, date of birth, current residential address, document numbers). Ferm stores KYC status metadata: verification status, provider name, Persona inquiry ID, review reason, and approval/rejection timestamps. Ferm does not store raw ID images, selfie images, or biometric templates on Ferm systems. Authorized Ferm staff may view those images in Persona's dashboard when reviewing a verification.

3.4.2 Payment Processors. We receive transaction metadata (amount, currency, status, provider transaction ID) from BTCPay Server, NOWPayments, and TailoredPay (NMI). Sensitive payment instrument data is entered and processed entirely on processor-hosted flows. Card numbers, CVV codes, and Apple Pay or Google Pay wallet data are entered only in TailoredPay Collect.js and are never stored by Ferm.

3.4.3 Authentication Providers. Google and Apple may provide your email address and name during OAuth sign-in, subject to your consent settings with those providers.

3.4.4 Payout Providers. To disburse payouts, our payout providers Bridge (bridge.xyz) and Rise Works (riseworks.io) collect and verify recipient information directly, which may include your name, address, bank account details, and cryptocurrency wallet addresses, and return to Ferm the onboarding status, verification status, and transfer status of your payout. Use of a payout rail requires acceptance of the applicable provider's own terms of service.

3.4.5 Linked Social Accounts. If you choose to link an X (Twitter) account to your profile, X provides your X user ID, handle, display name, and avatar URL. We do not store X access tokens after linking completes.

ARTICLE IV - USE OF PERSONAL DATA

4.1 We Process your Personal Data for the following purposes:

Purpose	Description
Provide the Service	Create and manage accounts; deliver simulated trading evaluations, funded accounts, and the trading terminal
Authenticate Users	Email OTP, Google Sign-In, Apple Sign-In, session management
Process Payments	Evaluation purchases via cryptocurrency checkout (BTCPay Server and NOWPayments) and card checkout including Apple Pay and Google Pay (TailoredPay)
Verify Identity (KYC)	Persona identity verification required before receiving a funded or live account and before any payout
Process Payouts	Disburse payouts to user-designated bank accounts or USDC wallets on supported networks through our payout providers (Bridge and Rise Works)
Send Push Notifications	Deliver account, trading, and payout notifications to registered mobile devices via Apple APNs and Firebase Cloud Messaging, subject to your notification preferences
Customer Support	Respond to inquiries, account issues, and disputes
Family Program (referral / affiliate)	Track Family (referral) attributions, calculate commissions, award Family milestone ticks, credit prize evaluations, process affiliate payouts
Legal Agreements	Generate, deliver, and record electronic funding agreement signatures
Enforce Platform Rules	Detect breaches, manage account status, apply payout holds
Security and Fraud Prevention	Detect multi-account abuse, referral fraud, manipulative trading patterns, and enforce Terms
Analytics and Improvement	Analyze usage patterns, troubleshoot errors, and improve Platform functionality
Compliance	Satisfy AML/CFT, sanctions screening, and other legal obligations

4.2 Marketing Communications. Optional Ferm promotional offers and product news by email require an affirmative choice in notification settings. We retain the scope, source, version and time of that choice. You may withdraw through settings or the unsubscribe link in each marketing email. Existing account creation, a purchase, acceptance of Terms or an administrator preference does not by itself supply marketing consent. Necessary service emails such as login codes, invoices and agreement delivery remain separate.

ARTICLE V - DISCLOSURE OF PERSONAL DATA

5.1 Sale and Sharing. We do not sell Personal Data for money or build remarketing audiences. Advertising measurement disclosures may fall within broader statutory definitions of sale or sharing, depending on the applicable law and provider use. We therefore provide an advertising opt-out through Privacy settings and honor Global Privacy Control for advertising measurement without requiring you to resolve that classification.

5.2 Service Providers. We disclose Personal Data to the following categories of third-party service providers who Process data on our behalf:

Provider	Role	Data Shared
BTCPay Server (pay.ferm.trade)	Cryptocurrency invoice checkout	Order ID, amount, item description, buyer email
NOWPayments (nowpayments.io)	Cryptocurrency checkout (USDC, USDT, and other enabled coins/chains)	Order ID, amount, pay currency, payment status callbacks
TailoredPay (NMI)	Card checkout via Collect.js hosted fields, Apple Pay, and Google Pay	Order ID, amount, billing name, payment token, and payment status callbacks. Card number, CVV, and wallet payment data never stored by Ferm
Bridge (bridge.xyz)	Payout disbursement: USD ACH/wire and USDC on supported networks	Identity and onboarding data collected directly by Bridge; bank account or wallet destination; transfer amounts and status
Rise Works (riseworks.io)	Alternative payout disbursement rail	Recipient enrollment data collected directly by Rise; payment amounts and status
Persona (withpersona.com)	KYC / identity verification	Ferm user UUID; Persona directly collects government ID, selfie, and biometric data
PandaDoc	Historical funding agreement document delivery and e-signature	Trader name, email, and agreement document content for agreements processed via PandaDoc
Resend	Transactional and marketing email delivery	Recipient email address, email content, delivery and engagement metadata
Intercom	Customer support messenger	User identifier (signed JWT), profile attributes needed for support, message content you submit
OpenAI	AI processing for Arlo, our support assistant	Messages you send to Arlo and the account details you choose to share in the conversation
Discord	Arlo support threads in the Ferm Discord server	Messages you send in a support thread and your Discord user ID
PostHog (US cloud)	Product analytics, session replay	User UUID, email, username, behavioral events (with masking)

Provider	Role	Data Shared
Sentry	Error and crash monitoring (web + mobile)	Error reports and stack traces; personally identifying fields are not intentionally sent and URLs are redacted
Apple	Sign in with Apple (web + iOS); Apple Push Notification service (iOS push delivery)	OAuth tokens; email and name per user consent; device push tokens for notification delivery
Google	Google Sign-In (web + mobile); Firebase Cloud Messaging (Android push delivery)	OAuth tokens; email, given name, family name; device push tokens for notification delivery
X (Twitter)	Optional profile linking	OAuth flow on X domains; X user ID, handle, display name, avatar URL
ipinfo.io / ipwho.is	IP geolocation for restricted-jurisdiction screening	Your IP address, resolved to country/region; results are used for geo-compliance and the IP is stored only in hashed form (except the funding agreement audit record)
Amazon Web Services (AWS) - US-East-1	Application hosting, primary application database (RDS PostgreSQL), S3 storage, CloudWatch logging, Secrets Manager	All platform data, including user, account, trading, transaction, and payout records, processed in US infrastructure
Cloudflare	DNS, SSL, PostHog reverse proxy	Request routing metadata; proxy strips cookies before forwarding
Google Sheets	Internal, access-controlled export of Family program (referral / affiliate) analytics for staff reporting	Pseudonymized Family (referral) and commission aggregates

5.3 Market Data and Charting Providers. The following providers supply market data to the Platform and do not receive any User Personal Data: Bybit, Hyperliquid, Jump (crypto price feeds); Hydromancer (Hyperliquid market data for cryptocurrency, 24/7, and stock instruments); ForexFactory (economic calendar). Charts are rendered using TradingView and TitanCharts charting libraries, which display market data only and do not receive User Personal Data from Ferm.

5.4 Legal and Regulatory Disclosure. We may disclose your Personal Data without notice if required or permitted to:

(a) Comply with applicable law, regulation, legal process, court order, subpoena, or governmental request;

(b) Respond to law enforcement or regulatory authorities;

(c) Meet AML/CFT and sanctions compliance obligations;

(d) Enforce our Terms and Conditions and investigate suspected fraud, abuse, or prohibited conduct;

(e) Protect the rights, property, safety, and security of Ferm, its Users, and the public;

(f) Cooperate with payment dispute or payment fraud investigations through our payment and payout

providers.

5.5 Business Transfers. In the event of a merger, acquisition, reorganization, bankruptcy, or sale of all or a portion of the Company's assets, User Personal Data may be among the assets transferred to the successor entity. Users will be notified as required by applicable law.

ARTICLE VI - BIOMETRIC DATA AND IDENTITY VERIFICATION

6.1 Collection. Biometric Data (facial geometry) is collected exclusively by Persona - not by Ferm - for the sole purpose of identity verification. The KYC process includes:

(a) A valid government-issued photo identification document (scanned or photographed);

(b) A live selfie with liveness detection for biometric face matching against the ID photo;

(c) Current residential address collection when required for identity verification or payout-provider onboarding; and

(d) Screening against global sanctions lists and Politically Exposed Persons (PEP) databases.

6.2 Timing. KYC is not required to register, or to start, purchase, pass, or breach an evaluation. KYC is required before signing a funded trader agreement or live account agreement - and therefore before receiving a funded or live account - and before any payout, including Family commission (affiliate) payouts.

6.3 What Ferm Stores. Ferm stores KYC status metadata: verification status, provider name, Persona inquiry ID, review reason, and approval/rejection timestamps. Ferm does not store raw ID images, selfie images, or biometric templates on Ferm systems. Authorized Ferm staff may view those images in Persona's dashboard when reviewing a verification.

6.4 Provider Storage and Retention. Persona processes verification images, facial-geometry information and identity attributes. Illinois capture stays disabled until Ferm verifies the applicable provider retention/destruction controls and configures the specific period shown in the separate pre-capture notice. Before a new or resumed inquiry, Ferm saves the exact notice and release, their versions and hashes, the affirmative action, timestamp and residence/location evidence, and associates the inquiry with that record. For provider notices see https://withpersona.com/legal/privacy-notices.

6.5 Separate Permission and Verification Availability. EU, EEA, UK, Texas and Washington residence does not by itself prevent you from starting Persona identity verification. Eligibility remains subject to identity checks, supported documents, sanctions screening and other applicable requirements. Illinois residents must execute the separate electronic written release before capture; unknown or conflicting residence must be resolved first. Any legally required biometric notice and separate permission must be completed before biometric collection. Starting KYC or accepting this Privacy Policy is not a substitute for that permission. Contact hello@ferm.trade about available verification methods and applicable refund rights, or privacy@ferm.trade about consent and withdrawal. Declining or withdrawing optional consent does not waive mandatory rights.

6.6 No Sale or Trade. Ferm does not sell, lease, trade or otherwise profit from Biometric Data. Permitted

processing and disclosures are limited to the purposes, recipients and authority stated in the applicable pre-capture notice and law.

6.7 Retention and Destruction Policy. For Illinois biometric identifiers and biometric information within the applicable requirements, the retention deadline is the earlier of satisfaction of the initial purpose for collection or three years after the last interaction, with any earlier legally required deadline preserved. A shorter verified provider period stated in the pre-capture notice controls. Ferm must verify provider destruction controls before enabling Illinois capture and retain records of destruction requests and outcomes. Consent/audit records that do not contain biometric templates may be retained separately for legal claims and compliance. Contact privacy@ferm.trade to request review or withdrawal; withdrawal does not affect processing lawfully completed before it.

6.8 Device Biometrics. The Ferm mobile application optionally uses Face ID or Touch ID to protect the locally stored session token. This is device-local only, is not transmitted to Ferm servers, and is entirely distinct from Persona KYC biometrics.

ARTICLE VII - COOKIES AND TRACKING TECHNOLOGIES

7.1 Cookies Used. The following cookies and local storage mechanisms are employed by the Platform:

Cookie / Storage	Classification	Purpose	Duration
ferm_session	Strictly Necessary	HttpOnly JWT authentication session	~6 hours / session
ferm-session-hint	Strictly Necessary	Signed HttpOnly session hint for web middleware routing	30 days
ferm_ref / ferm_web_ref	Advertising / Referral attribution	Family program first-touch attribution after advertising permission	30 days
ferm_optional_consent / ferm.cookieConsent.v1	Necessary preference record	Versioned analytics and advertising choices	Cookie: 180 days; local choice until changed or version expires
PostHog cookies/local storage	Performance / Analytics	Product analytics and session replay (when enabled)	Per PostHog defaults
Google Ads conversion cookies	Advertising / Conversion measurement	Measure completed paid evaluation purchases for Google Ads. Not used for remarketing or ad personalization.	Per Google defaults
ferm-auth (local storage)	Functional	Cached user profile for UX (not the session token)	Until cleared
ferm.deviceId (local storage)	Functional / Security	Device fingerprint for fraud detection	Persistent

7.2 Optional Measurement. PostHog analytics and Google Ads advertising measurement have separate choices

in Privacy settings and stay disabled until the relevant choice is made, regardless of inferred location. Advertising measurement records the purchase amount, currency and a pseudonymous transaction key after a confirmed paid evaluation. Network requests also disclose connection information such as IP address and browser metadata to the provider. Ferm does not deliberately include email addresses, payment credentials or trading records in this event. Google Analytics, Meta Pixel, remarketing audiences and ad personalization are not enabled by this implementation. Native optional PostHog analytics is disabled until a native consent control is available.

7.3 Third-Party Cookies. The following third parties may set cookies on their own domains during interactions initiated through the Platform:

Third Party	Context
PostHog	When analytics is enabled (proxied via e.ferm.trade; proxy strips inbound cookies)
Google Ads	When conversion measurement is enabled, to record a completed paid evaluation purchase
BTCPay Server	On pay.ferm.trade during crypto invoice checkout
NOWPayments	On NOWPayments domains during crypto checkout
TailoredPay	On tailoredpay.transactiongateway.com during card and wallet checkout
Persona	On Persona domains during KYC verification
Bridge / Rise Works	On their domains during payout onboarding and terms acceptance
Intercom	When the support messenger is loaded
Google / Apple / X (Twitter)	On their domains during OAuth sign-in or account-linking redirects

7.4 Managing Cookies. Privacy settings provides separate optional analytics and advertising/referral choices worldwide, including withdrawal. Necessary authentication storage supports core access. Withdrawal stops subsequent optional SDK processing and clears accessible optional storage; browser controls can also manage stored data. Server-side referral cookies are cleared through the withdrawal endpoint.

7.5 Browser Signals. Global Privacy Control disables advertising/referral measurement. The older Do Not Track signal is not used as a consent mechanism.

ARTICLE VIII - DATA SECURITY

8.1 We implement industry-standard technical and organizational measures to protect your Personal Data against unauthorized access, destruction, loss, alteration, disclosure, or misuse:

Measure	Implementation
Encryption in transit	HTTPS/TLS (SSL) for all web, API, and mobile traffic

Measure	Implementation
Encryption at rest	AES-256-GCM for email addresses, legal names, and payout wallet addresses
Hashed identifiers	Salted SHA-256 for email lookup and IP address correlation
Session security	HttpOnly, Secure, SameSite=Strict cookies; JWT with ~6-hour expiry
HTTP security headers	Helmet middleware
CORS restrictions	Allowlisted origins with trusted-origin middleware
Access controls	Role-based admin access; production secrets in AWS Secrets Manager
Webhook verification	Signature verification for Persona, BTCPay, NOWPayments, TailoredPay, Resend, and payout-provider webhooks
Rate limiting	Applied to auth, checkout, payout, and agreement endpoints
No stored card data	Card numbers, CVV codes, and Apple Pay or Google Pay wallet data are entered only in TailoredPay Collect.js and are never collected or stored by Ferm
Agreement storage	Signed PDFs in AWS S3 with AES-256 server-side encryption
Log redaction	API logs redact emails, JWTs, wallet addresses, and secret-shaped keys
Session replay privacy	PostHog masks all form inputs and all rendered text in session replay

8.2 While we strive to protect your Personal Data, no method of transmission over the Internet or method of electronic storage is 100% secure. We cannot guarantee absolute security. You are responsible for maintaining the confidentiality of your login credentials.

ARTICLE IX - DATA RETENTION

9.1 We retain Personal Data only for as long as necessary to fulfill the purposes described in this Policy, unless a longer retention period is required or permitted by law.

Data Category	Retention Period
Active account data	Duration of account activity and as needed to provide the Service
Trading and account history	Duration of account relationship plus reasonable post-closure period for disputes, fraud investigation, and legal compliance
Payment and transaction records	Minimum seven (7) years (accounting, tax, and reconciliation)
KYC status metadata	Duration of account relationship plus period required by AML/legal obligations
Biometric and ID data	The applicable pre-capture retention schedule and earlier mandatory deadlines in Article VI; ID records and biometric identifiers may have different retention periods
Email login codes	10-minute expiry; database records cleaned after approximately 24 hours

Data Category	Retention Period
Server logs (CloudWatch)	30 days
Support conversations with Arlo	One (1) year after your last message, and longer only when the law or an open dispute requires it
PostHog analytics data	Per PostHog project retention settings
Funding agreement audit records	Minimum seven (7) years or duration of applicable legal claims
Closed, breached, or terminated accounts	Retained as needed for fraud prevention, dispute resolution, chargeback defense, and legal compliance

9.2 General Principle. Personal Data is retained only as long as necessary for the purposes described in this Policy, unless a longer retention period is required or permitted by applicable law, regulation, or legal process.

ARTICLE X - INTERNATIONAL DATA TRANSFERS

10.1 FermTrading, Inc. is headquartered in the United States. Our primary infrastructure is hosted in the United States (AWS US-East-1, N. Virginia; PostHog US cloud).

10.2 If you are accessing the Service from outside the United States - including from the European Economic Area (EEA), the United Kingdom, Canada, Australia, or other jurisdictions - your Personal Data will be transferred to, stored, and processed in the United States, where data protection laws may differ from those of your jurisdiction.

10.3 Transfer Safeguards. Use of the Service is not consent to an otherwise unlawful international transfer. Transfers subject to EEA or UK restrictions require an applicable legal mechanism, such as a relevant adequacy decision or executed contractual safeguards with the required assessments and supplementary measures. Contact privacy@ferm.trade for recipient locations, the applicable mechanism and information about or a copy of relevant safeguards, subject to lawful redactions.

10.4 Availability. Service availability is subject to applicable law and the contractual jurisdiction restrictions in the Terms. A restricted jurisdiction is not necessarily subject to comprehensive sanctions.

ARTICLE XI - YOUR PRIVACY RIGHTS

11.1 Rights Available to All Users

Regardless of your jurisdiction, you may contact us at privacy@ferm.trade to:

(a) Request information about the Personal Data we hold about you;

(b) Request correction of inaccurate Personal Data;

(c) Request deletion of your Personal Data, subject to legal retention requirements;

(d) Withdraw consent for Processing where consent is the legal basis.

11.2 California Residents - CCPA/CPRA

If you are a California resident, you have the following rights under the California Consumer Privacy Act (CCPA) as amended by the California Privacy Rights Act (CPRA):

(a) Right to Know. You have the right to request disclosure of the categories and specific pieces of Personal Data we have collected, the sources of collection, the business purposes for collection, and the categories of third parties with whom we share it.

(b) Right to Delete. You have the right to request deletion of your Personal Data, subject to certain legal exceptions (e.g., fraud prevention, legal compliance, transaction completion).

(c) Right to Correct. You have the right to request correction of inaccurate Personal Data.

(d) Right to Opt-Out of Sale/Sharing. You can disable advertising measurement through Privacy settings at any time. Global Privacy Control also disables it. These choices apply without a sign-in requirement. Contact privacy@ferm.trade for other applicable sale/sharing opt-out requests, requests to limit sensitive-information processing, or authorized-agent requests. Verification requirements depend on the request and applicable law.

(e) Right to Non-Discrimination. We will not discriminate against you for exercising any of these rights.

(f) Categories of Personal Data Collected. In the preceding twelve (12) months, we have collected the following categories of Personal Data as defined by the CCPA: Identifiers (name, email, IP address, device ID); Commercial Information (purchase history, transaction records); Internet or Electronic Network Activity (browsing history, interactions with the Platform); Geolocation Data (country code); and Biometric Information (collected by Persona for KYC, not by Ferm directly).

(g) Authorized Agents. You may designate an authorized agent to submit requests on your behalf by providing written authorization.

11.3 European Economic Area and United Kingdom - GDPR / UK GDPR

If you are located in the EEA or the United Kingdom, the following provisions apply:

(a) Lawful Bases for Processing. We Process your Personal Data under the following lawful bases:

Lawful Basis	**Applicable Processing**
Performance of a contract	Providing the Service, processing transactions, managing your account and necessary non-biometric eligibility verification
Compliance with legal obligations	Specific applicable sanctions, tax-record and other legal duties; we do not treat every contractual identity check as a statutory AML obligation
Legitimate interests	Necessary and proportionate fraud prevention, platform security and enforcing Terms, subject to applicable balancing and objection rights

Lawful Basis	Applicable Processing
Consent	Optional analytics, advertising/referral measurement and marketing email; biometric processing only when the applicable ordinary and special-category conditions and required separate permission have been established

(b) Your Rights. You have the right to:

(i) Access - request confirmation of whether we Process your Personal Data and obtain a copy thereof;

(ii) Rectification - request correction of inaccurate or incomplete Personal Data;

(iii) Erasure - request deletion of your Personal Data where there is no compelling reason for continued Processing;

(iv) Restriction - request restriction of Processing in certain circumstances;

(v) Data Portability - receive your Personal Data in a structured, commonly used, machine-readable format;

(vi) Object - object to Processing based on legitimate interests or for direct marketing purposes;

(vii) Withdraw Consent - withdraw consent at any time where Processing is based on consent, without affecting the lawfulness of Processing prior to withdrawal.

(c) Supervisory Authority. You have the right to lodge a complaint with your local data protection supervisory authority. A list of EU supervisory authorities is available at https://edpb.europa.eu/about-edpb/board/members_en. The relevant UK authority is the Information Commissioner's Office (ICO) at https://ico.org.uk/.

(d) International Transfers. Article X describes international transfers and how to request details of applicable safeguards. This notice does not replace the required transfer mechanism.

11.4 Canadian Residents - PIPEDA

If you are a Canadian resident, the following rights apply under the Personal Information Protection and Electronic Documents Act (PIPEDA) and applicable provincial privacy laws:

(a) Right to Access. You have the right to request confirmation of whether we Process Personal Data relating to you and to obtain a copy thereof.

(b) Right to Correct. You have the right to request correction of inaccurate, outdated, or incomplete Personal Data.

(c) Right to Withdraw Consent. You may withdraw consent for the collection, use, or disclosure of your Personal Data at any time, subject to legal or contractual restrictions and reasonable notice.

(d) Contact. If you have questions or concerns about our privacy practices, please email privacy@ferm.trade. You may also contact the Office of the Privacy Commissioner of Canada at (800)

282-1376.

11.5 Australian Residents - Privacy Act 1988

If you are an Australian resident, the following rights apply under the Australian Privacy Act 1988 and the Australian Privacy Principles (APPs):

(a) Right to Access. You have the right to request access to the Personal Data we hold about you.

(b) Right to Correct. You have the right to request correction of inaccurate, out-of-date, incomplete, irrelevant, or misleading Personal Data.

(c) Complaints. If you believe we have breached the APPs, you may lodge a complaint with us at privacy@ferm.trade. If you are not satisfied with our response, you may contact the Office of the Australian Information Commissioner (OAIC) at https://www.oaic.gov.au/.

11.6 U.S. State Biometric Privacy Laws

(a) Illinois Biometric Information Privacy Act (BIPA). Where applicable, you receive written notice of biometric collection, purpose, disclosures and retention before providing the separate written release. Article VI states the retention/destruction policy and circumstances in which capture is unavailable. You may contact privacy@ferm.trade about the notice, release or destruction.

(b) Texas Capture or Use of Biometric Identifier Act (CUBI). If you are a Texas resident, the same protections apply. Biometric identifiers are collected solely for identity verification, are not sold or disclosed except as permitted by law, and are destroyed within a reasonable time after the purpose is fulfilled.

(c) Washington State Biometric Privacy Law (RCW 19.375). If you are a Washington resident, you are hereby notified that Biometric Data is collected for the commercial purpose of identity verification. You may request deletion by contacting privacy@ferm.trade.

(d) Additional U.S. State Laws (Virginia VCDPA, Colorado CPA, Connecticut CTDPA, Utah UCPA). Residents of these states may exercise rights to access, correct, delete, and opt-out of certain Processing as applicable under their respective state privacy laws by contacting privacy@ferm.trade.

ARTICLE XII - EXERCISING YOUR RIGHTS

12.1 How to Submit a Request. To exercise any privacy right described in this Policy, please contact us at:

Email: privacy@ferm.trade

Mail: FermTrading, Inc., Attn: Privacy, 4335 Cadieux Road, Detroit, MI 48224, United States

12.2 Identity Verification. To protect your privacy and security, we may require you to verify your identity before Processing your request. Verification may include confirming data points we maintain about you.

12.3 Response Timeframe. We will acknowledge receipt of your request and respond within thirty (30) days. If

your request is complex or we receive a high volume of requests, we may extend this period by an additional fifteen (15) days, and we will notify you of any such extension and the reason therefor.

12.4 Authorized Agents. You may designate an authorized agent to submit a request on your behalf. We may require the agent to provide proof of authorization and may still require you to verify your identity directly.

12.5 Appeals. If we deny your request, we will provide a written explanation. You may appeal by contacting privacy@ferm.trade. If your appeal is denied, you may contact the applicable supervisory authority or attorney general's office in your jurisdiction.

ARTICLE XIII - CHILDREN'S PRIVACY

13.1 The Service is not directed to individuals under the age of eighteen (18) or the age of majority in their jurisdiction, whichever is higher. We do not knowingly collect Personal Data from children.

13.2 If we become aware that we have collected Personal Data from a child without verification of parental consent, we will take steps to delete such information and terminate the associated account.

13.3 If you believe that a child has provided us with Personal Data, please contact us immediately at privacy@ferm.trade.

ARTICLE XIV - THIRD-PARTY LINKS AND SERVICES

14.1 The Service may contain links to third-party websites, applications, or services that are not owned or controlled by the Company. This Policy does not apply to third-party services.

14.2 We are not responsible for the privacy practices of third parties. We encourage you to review the privacy policies of any third-party service before providing your Personal Data.

14.3 The following third-party privacy policies are relevant to your use of the Service:

(a) Persona: https://withpersona.com/legal/privacy-notices

(b) PostHog: https://posthog.com/privacy

(c) Bridge: https://www.bridge.xyz/legal

(d) Rise Works: https://www.riseworks.io/privacy

(e) NOWPayments: https://nowpayments.io/privacy-policy

(f) Intercom: https://www.intercom.com/legal/privacy

(g) Sentry: https://sentry.io/privacy/

(h) TailoredPay (NMI): https://www.nmi.com/privacy-policy

(i) Google Ads: https://policies.google.com/privacy

ARTICLE XV - CHANGES TO THIS POLICY

15.1 We may update this Privacy Policy from time to time to reflect changes in our data practices, legal requirements, or business operations.

15.2 If a revision is material, we will endeavor to provide notice by posting the updated Policy on our website and updating the "Effective Date" at the top of this document.

15.3 Changes in Processing. Continued use does not grant consent to a new processing purpose. We request fresh consent where required and provide notice of material changes before they take effect where required by law.

15.4 We encourage you to review this Policy periodically for any changes.

ARTICLE XVI - GENERAL PROVISIONS

16.1 Mandatory Rights. Nothing in this notice or the Terms limits rights, remedies, supervisory authority powers or jurisdiction rules that cannot lawfully be excluded. Contractual governing-law provisions do not displace applicable privacy law.

16.2 Severability. If any provision of this Policy is held to be invalid, illegal, or unenforceable, such provision shall be modified to the minimum extent necessary to make it enforceable, and the remaining provisions shall continue in full force and effect.

16.3 Nature of Notice. This Policy explains processing and complements the Terms and any separate purpose-specific notice. It does not replace an applicable consent, statutory obligation or mandatory right.

16.4 No Waiver. The failure of the Company to enforce any provision of this Policy shall not constitute a waiver of such provision or the right to enforce it at a later time.

16.5 Assignment. The Company may assign this Policy in connection with a merger, acquisition, or sale of assets without your consent, provided the successor entity agrees to be bound by the terms hereof.

ARTICLE XVII - ACKNOWLEDGMENT

This notice explains the following; it does not require blanket consent:

(a) You have read and understood this Privacy Policy in its entirety;

(b) All trading on Ferm is simulated and Personal Data is collected solely for the purposes described herein;

(c) Your Personal Data will be transferred to and processed in the United States;

(d) Persona biometric verification is subject to the availability limits and separate permission described in Article VI;

(e) You may exercise your privacy rights at any time by contacting privacy@ferm.trade; and

(f) Any acknowledgment that you received this notice is distinct from optional marketing, tracking and biometric consent.

FermTrading, Inc.

4335 Cadieux Road, Detroit, MI 48224, United States

privacy@ferm.trade | legal@ferm.trade | hello@ferm.trade

© 2026 FermTrading, Inc. All rights reserved.