Privacy Policy

Privacy Policy

Effective date: 23 Nov 2026
Policy was last reviewed or updated: 18 Nov 2026

This Privacy Policy explains how Alpaca collects, uses, discloses, and protects personal data, and the choices and rights you have. Personal data means information that identifies, relates to, or can reasonably be linked to you. It applies when you:

- visit alpaca.markets and its subdomains, including our dashboards, our documentation, our community forum, and our status page, together the “Sites”;
- use our APIs, dashboards, SDKs, command line interface (CLI), MCP servers, and Alpaca Connect, together the “Services”;
- apply for or hold an account with us, directly or through a partner app built on Alpaca; or
- contact us, attend our events, or do business with us.

Browsing the Sites does not mean you consent to optional cookies or other tracking. Where we rely on your consent, we ask for it separately, and you can withdraw it at any time. Our Cookie Policy explains the technologies we use and your choices.

Who we are

“Alpaca,” “we,” and “us” mean AlpacaDB, Inc. and its U.S. subsidiaries listed below. Where this policy describes a specific activity, “we” means the company that carries out that activity.

- **AlpacaDB, Inc.**: the Sites, developer and paper trading accounts, our APIs and market data, MCP servers, CLI, Alpaca Connect, and Broker API partner relationships
- **Alpaca Securities LLC** (Alpaca Clearing): brokerage accounts, clearing, and custody
- **Alpaca Crypto LLC**: crypto accounts
- **Alpaca Derivatives LLC**: futures and prediction market accounts
- **Alpaca Transfer Agent LLC**: transfer agent services

Our regional companies also use this policy for their clients, and for those clients “we” means that company: Alpaca Europe, A.V., S.L.U. (EEA), WealthKernel Limited, trading as Alpaca UK (UK), and AlpacaX Securities Ltd. and AlpacaX Crypto Ltd. (Bahamas).

Other notices that may apply to you

- **Financial privacy notices.** If you are a customer of Alpaca Securities LLC, Alpaca Crypto LLC, or Alpaca Derivatives LLC, the Alpaca Clearing Privacy Notice, the Alpaca Crypto Privacy Notice, or the Alpaca Derivatives Privacy Notice explains how we share your

personal information and how you can limit that sharing. For customer information those notices cover, the notice controls if it conflicts with this policy.

- **Partner apps.** If you use an app built on our Broker API or listed on Alpaca Connect, the company that provides the app has its own privacy notice for the data it collects. If the partner holds an omnibus account with us, the partner, not Alpaca, has the relationship with you. Any information we process about you for that partner is handled on its behalf under our agreement with it, so direct questions to the partner.
- **Job applicants** should read our Recruitment Privacy Policy. Employees receive a separate employee privacy notice.

Personal data we collect

What we collect depends on how you interact with us. If you only browse the Sites, we collect device and usage data, and contact details only if you give them to us.

Category	Examples	Where it comes from
Identifiers and contact details	Name, postal address, email address, phone number, account number, username	You; partners who introduce your account
Government identifiers	Social Security or tax identification number; passport, driver's license, or national ID number; images of those documents	You; partners; identity verification providers
Identity verification data	Results of identity, address, and document checks	You; identity verification providers
Account profile and suitability data	Date of birth, citizenship and tax residence, employment, income, net worth, investment experience and objectives, risk tolerance, trusted contact, industry affiliations, control person and politically exposed person status	You; partners; screening providers
Financial and transaction data	Linked bank account details; deposits and withdrawals; orders, positions, balances,	You; your bank, through bank linking providers such as

	statements, confirmations, and tax forms; futures and event contract positions; crypto wallet addresses and blockchain transaction data	Plaid; payment and blockchain analytics providers; exchanges, clearing agencies, and other market infrastructure
Credentials and security data	Login credentials, multi-factor authentication data, API key and OAuth token records, IP address, device identifiers, login history, fraud and risk signals	You; your device; security and fraud prevention providers
Connected app and AI assistant activity	The apps, AI assistants, and MCP connections you authorize, the permissions you grant, and the requests they send to our APIs and MCP servers	You; the apps and AI assistants you connect
Communications	Support requests, chat transcripts, emails, call recordings where we record calls, feedback, and survey answers	You; our support, messaging, and archiving providers
Online activity	Browser and device type; IP address and the approximate location it indicates; pages viewed and links clicked; referring site and campaign; session replays with typed text masked; product experiment assignments	Your device, through the technologies in our Cookie Policy
Privacy choices	Your cookie and opt-out choices and the record of each choice	You; your browser
Marketing and event data	Newsletter and alert preferences, event and webinar registrations, and whether you open or click our emails	You; your device; our marketing providers

Business contact data	Name, job title, company, work email, and phone number of partner, prospect, and vendor contacts	You; your employer; business contact data providers; public professional profiles
Community content	Posts, replies, and profile details on our forum and community channels	You
Referral and rewards data	Referral codes, whether you were referred or referred someone, and rewards you earn	You; our referral program provider
Inferences	Whether you are a business or individual visitor; product interests; fraud and risk scores; eligibility for products such as options, margin, or futures	Created by us from the data above

Identity verification. Federal law requires us to verify the identity of each person who opens a brokerage, crypto, or futures account. We use identity verification providers to check your details and ID document.

Sensitive personal data. Government identifiers, citizenship and immigration status, financial account information, and account login credentials are sensitive personal data under some laws. We use them only to provide the Services, verify identity, secure accounts, prevent fraud, and meet legal and regulatory obligations. We do not use them to infer characteristics about you or for advertising.

How we use personal data

Purpose	Examples
Provide the Services	Create and run your account; execute, clear, and settle trades; hold assets in custody; process deposits and withdrawals; provide our APIs, dashboards, MCP servers, CLI, Alpaca Connect, and market data
Open accounts and meet know your customer duties	Verify identity, screen against sanctions and watch lists, assess eligibility and suitability, and monitor for money laundering and fraud

Comply with law and regulation	Keep the books and records that securities and commodities laws require; report to the Consolidated Audit Trail, regulators, and tax authorities; respond to legal process
Communicate with you	Send service and account notices, provide support, and send newsletters and alerts you ask for
Keep the Sites and Services secure	Authenticate users; detect and prevent fraud, abuse, and security incidents; monitor errors and performance
Improve the Sites and Services	Measure usage, fix problems, and run product experiments
Marketing and advertising	Tell you about our products, measure campaigns, run referral and rewards programs, and, subject to your choices, show our ads on other sites
Protect rights and run the business	Enforce our terms; handle claims and disputes; manage audits; complete mergers, financings, or other corporate transactions

We do not use personal data for a new purpose that is incompatible with these without telling you and, where the law requires, asking for your consent.

Cookies, analytics, and advertising

We and our providers use cookies, pixels, browser storage, and similar technologies on the Sites. Our Cookie Policy lists each one, what it does, and how long it lasts, and explains your choices, including which Sites do not show our consent controls.

In the EEA, the UK, and Québec, optional technologies stay off until you allow them. Elsewhere they are on until you opt out using “Cookie settings” in the footer or, in the United States, the “Do Not Sell or Share My Personal Information” link. We treat a Global Privacy Control (GPC) signal as an opt-out from your first visit, and we keep a record of each choice, including your IP address.

Some analytics tools record session replays of your clicks, scrolling, and page changes, with what you type masked. Our emails contain web beacons that show whether you opened them and which links you clicked. Your browser’s “Do Not Track” setting has no agreed meaning, so we do not respond to it.

How we disclose personal data

We disclose personal data only as described here.

- **Service providers.** Companies that work for us under contracts that limit how they can use the data, such as cloud hosting, identity verification, payments, customer support, communications archiving, security, analytics, and AI providers.
- **Partners who introduced your account.** If you opened your account through a partner app, we exchange account, transaction, and verification information with that partner so it can provide its service and meet its obligations.
- **Our affiliates.** Companies in the Alpaca group, for the purposes in this policy and as our financial privacy notices describe.
- **Market and financial infrastructure.** Exchanges, clearing and settlement agencies, custodians, cash sweep banks, other brokers when you transfer an account, and market data providers that require subscriber details.
- **Regulators, law enforcement, and legal process.** Including the SEC, FINRA, the CFTC, the NFA, FinCEN, and tax authorities, when the law requires it or to protect rights, safety, and property, including lawful requests by public authorities to meet national security or law enforcement requirements.
- **Advertising and analytics partners.** Subject to your choices in Cookies, analytics, and advertising, companies such as Google, Reddit, and HubSpot receive device identifiers and browsing activity through cookies and pixels.
- **Apps, AI assistants, and people you direct us to share with**, such as a connected app, a trusted contact, or an authorized agent.
- **Corporate transactions and advisers.** A buyer, investor, or successor in a merger, acquisition, financing, or sale of assets, and our professional advisers and auditors, all under confidentiality obligations.

We do not sell personal data for money. Under California and some other state laws, letting advertising partners collect browsing data through our Sites can count as a “sale” or “sharing.” Additional information for US residents explains how to opt out.

Apps and AI assistants you connect

You can connect apps and AI assistants to your Alpaca account. What they can do depends on how you connect.

How you connect	What the app or assistant can do
An AI assistant connected to our hosted MCP server	With a live account, read account details, balances, positions, orders, and market data. It cannot move money or place trades. With a paper trading account, it can also place simulated trades.

Our MCP Server or CLI that you run yourself with your API keys	Anything your API keys allow, including placing live orders if you use live keys
An app on Alpaca Connect, using OAuth	What you grant when you authorize it: read-only access, trading access, or both
Our Broker MCP Server, for Broker API partners	Partner staff approved by the partner can look up the accounts, profiles, positions, activities, and transfers of the partner's customers. Production access is read-only. Sandbox access uses test data.

- **What we share and keep.** We send a connected app or assistant only the data it requests within the permissions you granted. We log the requests it sends us, such as the tool it called and its inputs, for security, fraud prevention, and securities record-keeping. We do not receive your conversation with an AI assistant unless the assistant includes it in a request.
- **The other company's terms apply.** The company behind the app or assistant is not part of Alpaca and does not act for us. Its own terms govern how it uses your data, including for training its models.
- **If you are a partner app's customer.** Your partner may look up your account through our Broker MCP Server with an AI assistant it chooses, under its own privacy notice.
- **You can disconnect at any time.** Revoke the app's access or delete the API key in your dashboard, and remove the connector from your assistant. This stops future sharing but does not delete data the app already has.

How we use AI and automated tools

We use AI tools, including large language models, to help our staff answer support requests, review documents, write and test code, and carry out compliance work. When these tools process personal data, the provider acts as our service provider under a written contract that does not allow it to use that data to train its models, and we give the tools only the personal data a task needs.

AI-assisted support. When you contact support, an AI assistant may answer first. We tell you when you are talking to an AI assistant, and you can ask for a person.

Automated decisions. We use automated tools to help screen for fraud, sanctions, and risk, and to help assess applications. Decisions that have a legal or similarly significant effect on you, such as declining or restricting an account, involve human review.

International transfers

We are based in the United States and process personal data there and in other countries where we or our service providers operate. When we transfer personal data from the EEA or the UK to a country without an adequacy decision, we use an approved safeguard:

- **From the European Union:** our certification under the EU-U.S. Data Privacy Framework, or the European Commission's Standard Contractual Clauses.
- **From the United Kingdom:** our certification under the UK Extension to the EU-U.S. Data Privacy Framework, or the UK International Data Transfer Addendum to those clauses.

We add technical and organizational measures such as encryption and access controls. You can ask us for a copy of the safeguard we use.

How long we keep personal data

We keep personal data for as long as we need it for the purposes in this policy, and then delete or anonymize it. To set retention periods we consider how long we have a relationship with you, legal and regulatory requirements, possible disputes or claims, and our legitimate business needs. For example:

Data	How long we keep it
Brokerage account records, orders, and statements	At least six years after the account closes, as SEC Rule 17a-4 requires
Business communications we must archive	As SEC, FINRA, CFTC, and NFA rules require, generally three to six years
Cookies and similar technologies	As listed in our Cookie Policy

If you ask us to delete personal data, we will do so, except where we must keep it to meet a legal obligation such as securities record-keeping rules.

How we protect personal data

We protect personal data with administrative, technical, and physical safeguards designed for a regulated financial services company, including encryption, access controls, monitoring, and staff training. Only authorized staff and service providers who need personal data for their work can access it, and they must keep it confidential. No system is perfectly secure, so we cannot guarantee that unauthorized access will never happen.

If a security incident affects your personal data, we will notify you and the relevant authorities as the law requires. For brokerage customers, that includes notice within 30 days after we become aware that sensitive customer information was, or is reasonably likely to have been, accessed or used without authorization, as SEC Regulation S-P requires.

To report a security vulnerability, email bugreport@alpaca.markets. Our Security page describes our vulnerability disclosure and bug bounty program.

Your choices and rights

Your choices. You can unsubscribe from marketing email at any time (we will still send account and service messages), change your cookie and advertising choices in the footer of the Sites or with GPC, revoke connected apps and AI assistants in your dashboard, and limit certain sharing as our financial privacy notices describe.

Your rights. Depending on where you live, you may have the right to:

- know what personal data we hold about you and get a copy, including in a portable format;
- correct inaccurate personal data;
- delete personal data;
- opt out of the sale or sharing of personal data, targeted advertising, and certain profiling;
- in some states, get a list of the specific third parties to which we disclosed your personal data;
- object to or restrict certain processing, and withdraw consent where we rely on it; and
- not be discriminated against for using these rights.

How to make a request. Email privacy@alpaca.markets. We will verify your identity before acting, usually by matching information we already hold or by asking you to sign in. You can use an authorized agent, who must show us your signed permission. We will respond within the time the law requires. If we decline your request, we will tell you why, and you may appeal by replying to our decision. If you are not satisfied with the outcome of an appeal, you can contact your state attorney general or your data protection authority.

Some rights do not apply to information we must keep under securities, commodities, tax, or anti-money laundering laws, or to information that our financial privacy notices cover.

Additional information for US residents

This section applies to residents of California and other states with consumer privacy laws. It does not apply to personal information covered by the Gramm-Leach-Bliley Act and the rules that implement it, such as information we collect to provide brokerage, crypto, or futures accounts to you, which our financial privacy notices address. It mostly concerns website visitors, developer and paper trading account holders, people who connect apps and AI assistants, business contacts, event attendees, and market data customers.

Personal information we collected in the last 12 months

Category (California law)	Sources	Purposes	Disclosed for a business purpose to	Sold or shared

Identifiers	You, your device, partners, providers	All purposes in How we use personal data	Service providers, affiliates, partners, authorities	No
Personal records (Cal. Civ. Code § 1798.80(e))	You, partners, verification providers	Accounts, verification, compliance, support	Service providers, affiliates, partners, authorities	No
Protected classification characteristics (age, citizenship)	You, partners	Verification, eligibility, compliance	Service providers, affiliates, authorities	No
Commercial information (products and services you use, transactions)	You, partners, market infrastructure	Services, compliance, improvement	Service providers, affiliates, partners, authorities	No
Internet and network activity, including requests from apps you connect	Your device, apps you connect	Security, improvement, marketing	Service providers, analytics providers	No
Approximate geolocation (from IP address)	Your device	Security, geographic restrictions, analytics	Service providers	No
Audio, electronic, and visual information (ID images,	You	Verification, support, recordkeeping	Service providers, authorities	No

call recordings, chat transcripts)				
Professional or employment information	You, your employer, business contact providers	Eligibility, business relationships	Service providers, affiliates	No
Inferences	Created by us	Fraud prevention, eligibility, marketing	Service providers	No
Sensitive personal information (government IDs, account credentials, financial account information, citizenship)	You, partners, providers	Only the permitted purposes in Personal data we collect	Service providers, authorities	No

We keep each category for the periods in How long we keep personal data. We do not have actual knowledge that we sell or share the personal information of consumers under 16. We use sensitive personal information only for purposes that the law allows without offering a right to limit, so we do not provide a “Limit the Use of My Sensitive Personal Information” link.

Right to know. You can ask about personal information we collected about you, including information older than 12 months, unless providing it would be impossible or involve disproportionate effort.

Opting out of sale, sharing, and targeted advertising. Use the “Do Not Sell or Share My Personal Information” link in the footer of our Sites, or turn on Global Privacy Control in your browser.

California “Shine the Light.” We do not share personal information with third parties for their own direct marketing.

Additional information for the EEA and the UK

Controllers. If you are a client of Alpaca Europe, your controller is Alpaca Europe, A.V., S.L.U. in the EEA or WealthKernel Limited (trading as Alpaca UK) in the UK. For visits to our Sites, business contacts, and services our U.S. companies provide directly, your controller is the company in Who we are. We need the information we ask for to open and run your account and to meet our legal obligations, and without it we may not be able to provide our services.

Data protection officer. You can reach the data protection officer for Alpaca Europe, and the privacy team for our U.S. companies, at privacy@alpaca.markets.

Legal bases.

Purpose	Legal basis
Provide the Services and manage your account	Performance of a contract
Identity verification, AML, sanctions, recordkeeping, regulatory reporting	Legal obligation
Security, fraud prevention, error monitoring, service improvement, business relationship management	Legitimate interests in running a secure and effective business
Optional cookies, analytics, and advertising on our Sites	Consent
Marketing emails	Consent, or legitimate interests for existing customers and business contacts where the law allows, with an opt-out in every message

Your rights. If you are in the EEA or the UK, you have the rights in Your choices and rights, including the right to object at any time to processing based on legitimate interests and to direct marketing, and to withdraw consent without affecting earlier processing. EU and UK individuals also have the rights described in EU-U.S. Data Privacy Framework and UK Extension. You can complain to your local data protection authority.

EU-U.S. Data Privacy Framework and UK Extension

AlpacaDB, Inc. complies with the EU-U.S. Data Privacy Framework (EU-U.S. DPF) and the UK Extension to the EU-U.S. DPF as set forth by the U.S. Department of Commerce. AlpacaDB, Inc. has certified to the U.S. Department of Commerce that it adheres to the EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) with regard to the processing of

personal data received from the European Union in reliance on the EU-U.S. DPF and from the United Kingdom (and Gibraltar) in reliance on the UK Extension to the EU-U.S. DPF. If there is any conflict between the terms in this Privacy Policy and the EU-U.S. DPF Principles, the Principles shall govern. To learn more about the Data Privacy Framework (DPF) program, and to view our certification, please visit https://www.dataprivacyframework.gov/. Our entry is on the Data Privacy Framework List.

Covered U.S. subsidiaries. Alpaca Securities LLC, Alpaca Crypto LLC, Alpaca Derivatives LLC, and Alpaca Transfer Agent LLC, U.S. subsidiaries of AlpacaDB, Inc., also adhere to the EU-U.S. DPF Principles, including under the UK Extension to the EU-U.S. DPF, and are covered by our certification.

Data covered. We apply the EU-U.S. DPF Principles to all personal data we receive from the European Union and the United Kingdom in reliance on the EU-U.S. DPF and the UK Extension. That includes contact details, account and transaction data, online activity, and business contact data of customers, partners, website visitors, and business contacts, which we use for the purposes in How we use personal data, and human resources data about our employees in the EU and the UK, which we use to manage the employment relationship. We disclose this data only to the types of third parties in How we disclose personal data and for the purposes described there.

Your rights under the DPF. EU and UK individuals have the right to access the personal data we hold about them and to correct, amend, or delete it where it is inaccurate or has been processed in violation of the EU-U.S. DPF Principles. EU and UK individuals can also choose (opt out) whether their personal data is disclosed to a third party, other than a service provider acting for us, or used for a purpose materially different from the purpose for which it was originally collected or later authorized. We will ask for your express consent (opt in) before we disclose sensitive personal data to such a third party or use it for such a purpose. To exercise these rights, contact us at privacy@alpaca.markets.

Onward transfers. We remain responsible under the EU-U.S. DPF Principles if a third party that we transfer personal data to as our agent processes it in a manner inconsistent with the Principles, unless we prove that we are not responsible for the event giving rise to the damage.

Disclosure to public authorities. We may be required to disclose personal data in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.

Enforcement. The Federal Trade Commission has jurisdiction over the compliance of AlpacaDB, Inc. and its covered U.S. subsidiaries with the EU-U.S. Data Privacy Framework (EU-U.S. DPF) and the UK Extension to the EU-U.S. DPF.

Questions and complaints. In compliance with the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF, AlpacaDB, Inc. commits to resolve DPF Principles-related complaints about our collection and use of your personal information. EU and UK individuals with inquiries or complaints regarding our handling of personal data received in reliance on the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF should first contact AlpacaDB, Inc. at privacy@alpaca.markets.

Independent recourse. In compliance with the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF, AlpacaDB, Inc. commits to cooperate and comply respectively with the advice of the panel established by the EU data protection authorities (DPAs) and the UK Information Commissioner's Office (ICO) and the Gibraltar Regulatory Authority (GRA) with regard to unresolved complaints concerning our handling of personal data received in reliance on the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF, including human resources data transferred in the context of the employment relationship. This recourse is free of charge to you.

Binding arbitration. Under certain conditions, you may invoke binding arbitration for complaints regarding our compliance with the EU-U.S. DPF Principles that are not resolved by any of the other DPF mechanisms, as described in Annex I of the EU-U.S. DPF Principles.

Children and custodial accounts

Our Sites and Services are not directed to children, and we do not knowingly collect personal data directly from anyone under 18. A parent or guardian may open a custodial account for a minor, in which case we receive the minor's information from the adult who opens the account and use it only to provide and administer that account and meet our legal obligations. If you believe a child has given us personal data directly, contact privacy@alpaca.markets and we will delete it.

Changes to this policy

We will update this policy when our practices or the law change, and at least once a year. The date at the top shows the latest version, and earlier versions are available on request. If we make a material change, we will tell account holders by email or with a notice on the Sites before the change takes effect, and we will ask for consent where the law requires.

Contact us

AlpacaDB, Inc., Attn: Privacy
3 East Third Avenue, Suite 214, San Mateo, CA 94401, USA
privacy@alpaca.markets
+1 650 489 2017