

Privacy Policy

Kitearn Inc. | Effective and last updated: August 1, 2026

Plain-language summary

Kitearn uses information to provide its website and app, personalize financial-product matches and tools, prevent fraud, communicate with you, and—when you ask us to—send information to financial-product providers. Those providers make their own eligibility or credit decisions and use information under their own privacy notices. This summary is for convenience; the full Policy below controls.

1. Scope and who we are

This Privacy Policy explains how Kitearn Inc. ("Kitearn," "we," "us," or "our") collects, uses, discloses, and retains personal information when you visit kitearn.com, use a Kitearn mobile application, create an account, communicate with us, or use any product or service that links to this Policy (collectively, the "Services").

Kitearn provides digital financial tools and may help consumers identify, compare, request, or access financial products or services offered by third parties. Depending on availability, the Services may include a loan marketplace and lender referrals, earned wage access or cash advances, bank accounts or payment cards, payments or money transfers, rewards, and credit-building products. Unless product-specific terms expressly state otherwise, Kitearn is a financial technology company and is not a bank or lender. A bank, lender, employer, program partner, or other financial provider may make eligibility, underwriting, account-opening, or servicing decisions.

This Policy applies to information controlled by Kitearn. A third-party provider's privacy notice governs information that the provider collects directly or receives and processes for its own purposes. Product-specific disclosures, a U.S. Consumer Privacy Notice, or an additional consent may also apply. If a product-specific notice conflicts with this Policy, the product-specific notice controls for that product and information.

You may use certain marketplace features without registering, while an account may be required for other features or products. This Policy applies to both guest and registered use of the Services.

The Services are intended for individuals in the United States. They are not directed to business or commercial applicants unless we expressly say otherwise.

2. Personal information we collect

The information we collect depends on the Services you use, the information you choose to provide, applicable law, and the providers involved. We may collect the following categories:

- **Account and contact information.** Name, email address, mobile number, mailing address, username, password or authentication data, communication preferences, and account settings.
- **Identity and eligibility information.** Date of birth, age, Social Security number or taxpayer identification number, government-issued identification information, citizenship or residency information, and identity-verification results. If a feature requires a photograph, selfie, or liveness check, we will provide any additional notice or consent required by law.

- **Financial and transaction information.** Bank or payment-account information, balances, transaction history, direct deposits, payroll deposits, recurring obligations, card or payment transactions, repayment history, account status, and information needed to initiate or service a requested transaction. When an account-connectivity provider is used, Kitearn generally receives account data or a connectivity token rather than your bank login credentials.
- **Employment, income, and payroll information.** Employer, occupation, employment status and tenure, income, pay schedule, hours worked, earned wages, payroll deposits, benefits, and other information supplied by you, an employer, payroll system, or authorized data provider.
- **Application and financial-profile information.** Requested amount, product preferences, loan or advance purpose, housing information, recurring expenses, and answers to questionnaires used to identify potentially relevant products.
- **Referral, product-status, and risk information.** The products or links shown or selected; referral and affiliate identifiers; whether a referred application, account, or transaction was submitted, approved, opened, or funded; fraud indicators; identity-risk signals; and prior Kitearn account, transaction, or repayment history. Kitearn does not currently obtain your consumer report or credit score; a lender or other financial provider may do so under its own notice and authorization.
- **Device, internet, and app activity.** IP address, cookie or mobile advertising identifiers, device ID, device and browser type, operating system, app version, language, referring URLs, screens or pages viewed, buttons clicked, session dates and duration, crash logs, diagnostics, and similar usage events.
- **Location information.** Approximate location derived from an IP address or device settings. We collect precise geolocation only when a feature requires it, you permit it through your device, and any required notice or consent has been provided.
- **Communications and support information.** Emails, chat messages, survey responses, complaints, call or support records, and—if notice is provided—recordings or transcripts of telephone or video interactions.
- **Marketing and referral information.** How you learned about Kitearn, campaign or affiliate identifiers, interactions with advertisements and messages, referral activity, and preferences.
- **Derived information and inferences.** Information we derive from the categories above, such as likely product fit, eligibility indicators, fraud or security risk, user preferences, and engagement segments.

We may create aggregated, deidentified, or anonymized information that cannot reasonably be linked to you. We may use and disclose that information for lawful purposes and will not attempt to reidentify data that applicable law requires us to maintain in deidentified form.

3. How we collect information

- **Directly from you.** For example, when you create an account, complete a questionnaire or application, connect an account, request a product, contact support, participate in a survey, or communicate with us.
- **Automatically from the Services.** Through cookies, software development kits (SDKs), pixels, local storage, logs, mobile identifiers, analytics tools, and similar technologies.
- **From financial, employment, and product providers.** Such as banks, lenders, card issuers, program managers, payment processors, account-connectivity services, payroll or employment-data providers, employers, and providers whose products you ask us to help you access.
- **From identity and fraud sources.** Such as identity-verification services, fraud-prevention providers, public records, sanctions and watchlists, and specialty identity or device-data providers, when permitted by law.

- **From marketing and business partners.** Such as affiliates, referral partners, publishers, advertising networks, app stores, social platforms, analytics providers, and co-marketing partners.
- **From public and other lawful sources.** Including publicly available records and information that third parties lawfully make available to us.

4. How we use personal information

We may use personal information to:

- Provide, operate, maintain, and improve the Services; create and secure your account; authenticate you; and remember your settings.
- Understand your needs and personalize product comparisons, recommendations, educational content, and financial tools.
- At your request, identify potential financial providers, prefill or route information, connect you with a provider, facilitate an application or transaction, and support product delivery and servicing.
- Verify identity, satisfy know-your-customer or other compliance requirements, match users with potentially relevant products, and support a financial provider's eligibility process without making that provider's credit decision.
- Process payments, transfers, subscriptions, advances, repayments, rewards, or other transactions available through the Services.
- Detect, investigate, and prevent fraud, identity theft, abuse, security incidents, prohibited conduct, and violations of our agreements.
- Communicate with you about your account, applications, transactions, security, support requests, product updates, and legal notices.
- Send marketing or promotional communications, subject to your choices and applicable law, and measure the effectiveness of campaigns and referrals.
- Analyze usage, troubleshoot errors, conduct research, develop new features, test models, and improve accessibility, performance, and user experience.
- Comply with law, regulatory requirements, court orders, audits, examinations, recordkeeping obligations, and lawful requests; establish, exercise, or defend legal claims.
- Protect the rights, property, safety, and integrity of Kitearn, our users, partners, and the public; and carry out a corporate transaction.
- Fulfill another purpose disclosed to you at collection or with your consent.

5. Product matching, referrals, and automated tools

Kitearn may use information you provide and information from authorized sources to rank, filter, or recommend financial products. Depending on the product or partner, Kitearn may either direct you to a third-party site where you provide information directly, or—after your request or authorization—transmit selected contact, application, identity, employment, income, or financial information to one or more financial-product partners. We will identify or describe the applicable recipient or category of recipients in the relevant flow.

A match or recommendation is not an approval, commitment, or guarantee of terms. Kitearn does not currently obtain consumer reports or credit scores. Unless expressly stated in product-specific terms, the relevant financial provider—not Kitearn—obtains any consumer report, determines final eligibility, underwriting, pricing, account opening, or credit, and provides any legally required decision or adverse-action notice.

Some states provide a right to opt out of certain profiling used to make decisions that produce legal or similarly significant effects. Where applicable, you may exercise that right as described in Section 12. We may deny a request where an exception applies, including when processing is necessary to provide a product you requested, prevent fraud, or comply with law.

6. How we disclose personal information

We may disclose personal information to the following recipients for the purposes described in this Policy:

- **Financial-product and referral partners.** When you ask to see, apply for, open, or use a product, we may disclose information to banks, lenders, earned-wage-access providers, card issuers, program managers, payment providers, employers, or other financial partners. These parties may use the information as independent businesses under their own privacy notices and, where you separately consent, may contact you by email or text about completing an application, servicing a requested product, or their own offers.
- **Service providers and contractors.** Companies that provide cloud hosting, account connectivity, payroll connectivity, identity verification, fraud prevention, credit data, payments, customer support, communications, analytics, security, document management, professional advice, and other services on our behalf.
- **Advertising, analytics, and marketing partners.** Partners that help us understand use of the Services, measure campaigns, attribute referrals, prevent advertising fraud, or show or evaluate advertising, subject to your privacy choices.
- **Affiliates and business partners.** Current or future corporate affiliates and partners with whom we offer a co-branded or integrated service, as permitted by law and disclosed to you.
- **Legal and safety recipients.** Courts, regulators, law enforcement, government agencies, auditors, attorneys, insurers, and other parties when we believe disclosure is required or appropriate to comply with law, protect rights or safety, investigate wrongdoing, or enforce agreements.
- **Corporate transaction recipients.** Actual or prospective buyers, investors, lenders, advisers, or other participants in a merger, financing, reorganization, sale of assets, acquisition, bankruptcy, or similar transaction, subject to appropriate confidentiality protections.
- **Recipients you direct or authorize.** Other parties when you direct us to disclose information, intentionally interact with them through the Services, or provide consent.

7. Sale, sharing, and targeted advertising

Kitearn does not sell personal information to data brokers for cash. However, some U.S. state privacy laws define "sale," "sharing," or "targeted advertising" broadly. Depending on how our Services and partner relationships operate, the following may be considered a sale or sharing under those laws:

- disclosing identifiers, contact information, application or financial-profile information, referral events, and related inferences to a financial-product partner in connection with compensation based on a click, lead, submitted or approved application, opened or funded account, revenue share, placement, advertising fee, or another conversion event; and
- allowing advertising, analytics, or attribution partners to receive identifiers and internet or app activity for cross-context behavioral advertising, targeted advertising, or campaign measurement.

We do not knowingly sell or share personal information of anyone under 18. We do not sell or share Social Security numbers, government identification numbers, bank-account credentials, precise geolocation, consumer reports, or biometric information for cross-context behavioral advertising. You may opt out of activities treated as sale, sharing, or targeted advertising under applicable law as described in Section 12. An opt-out does not prevent disclosures you direct in order to receive a requested product or service, or disclosures otherwise permitted by law.

8. Cookies, SDKs, analytics, and privacy signals

We and our partners may use cookies, SDKs, pixels, tags, local storage, mobile identifiers, and similar technologies to keep the Services working, remember preferences, secure accounts, understand performance, attribute referrals, and support marketing. These technologies may collect device, internet, and app activity described in Section 2.

These tools may include Google Analytics, Google Ads, Meta Pixel or Meta SDK, affiliate or conversion tracking, and other advertising or attribution technologies used on our website or mobile applications. We do not use these tools to send Social Security numbers, government-ID data, bank-account credentials, precise geolocation, consumer reports, or biometric information for advertising.

You can control cookies through browser settings and certain mobile permissions through device settings. You may also be able to reset or limit use of a mobile advertising identifier. Disabling a technology may affect functionality. Where required by law, we treat a legally recognized opt-out preference signal, such as Global Privacy Control (GPC), as a request to opt out of sale or sharing for the browser or device that sends the signal. Because there is no uniform industry standard for other "Do Not Track" signals, we do not respond to them unless legally required.

Our Services may link to third-party sites, apps, or services. Their privacy practices are governed by their own notices, and we encourage you to review them before providing information.

9. Communications and marketing choices

You may unsubscribe from promotional email by using the link in the message. You may opt out of promotional text messages by replying STOP or following the instructions provided. We may still send non-promotional communications, including security alerts, account notices, transaction messages, responses to requests, and legally required notices.

When a referral flow contains a separate, clear consent for one or more identified financial-product partners or described categories of partners, those partners may contact you by email or text for the purposes stated in that consent, including completing an application, servicing a requested product, or marketing their products. Each partner is responsible for honoring the consent and its own opt-out obligations. Kitearn does not authorize partner telephone calls unless you separately consent to them in the applicable flow.

Kitearn's own text-message opt-in data and consent are not transferred to third parties or affiliates as blanket consent for their own marketing or promotional purposes. We may disclose that information to vendors that help us deliver Kitearn messages and to other parties when required by law. A partner may send marketing texts only when you provide separate, legally compliant consent for that partner or category of partners.

10. Data retention

We retain personal information for no longer than reasonably necessary for the purposes described in this Policy, unless a longer period is required or permitted by law. Retention depends on the nature and sensitivity of the information, the product or account involved, the duration of our relationship, operational needs, fraud and security risk, contractual commitments, applicable statutes of limitation, and legal, regulatory, audit, dispute, and recordkeeping requirements.

For example, we may retain account, application, transaction, consent, identity-verification, and compliance records after account closure when required for financial-services recordkeeping, fraud prevention, dispute handling, or legal claims. Cookie and analytics retention varies by technology and configuration. When information is no longer required, we take reasonable steps to delete, destroy, or deidentify it.

11. Security

We use administrative, technical, and physical safeguards designed to protect personal information, taking into account the nature of the information and the risks involved. These measures may include access controls, encryption in transit and at rest where appropriate, monitoring, vendor oversight, secure development practices, and incident-response procedures. No transmission, storage system, or security measure can be guaranteed to be completely secure. You are responsible for maintaining the confidentiality of your credentials and for promptly notifying us of suspected unauthorized access.

Kitearn's Services are offered to U.S. users, and Kitearn does not currently authorize its employees, founders, contractors, developers, support teams, or vendors outside the United States to access personal information for the Services. If this practice changes, we will update this Policy and use safeguards required by applicable law.

12. Your privacy rights and choices

Depending on where you live and subject to legal exceptions, you may have the right to:

- confirm whether we process your personal information and access or obtain a portable copy of it;
- correct inaccurate personal information;
- delete personal information;
- opt out of sale, sharing, targeted advertising, or certain profiling;
- limit certain uses or disclosures of sensitive personal information;
- withdraw consent where processing is based on consent;
- appeal our denial of a privacy request; and
- receive equal service and not be discriminated against for exercising a privacy right.

To submit a request, email privacy@kitearn.com with the subject "Privacy Request" and describe the right you wish to exercise. You may also use any privacy-request or privacy-choices control made available in the Services. To opt out of marketing, use the methods in Section 9. Where required, we will honor a recognized browser-based opt-out preference signal as described in Section 8.

To opt out of activities treated as a sale, sharing, or targeted advertising, email privacy@kitearn.com with the subject "Do Not Sell or Share" or use a privacy-choices control made available in the Services. Where required, a recognized Global Privacy Control signal provides an additional opt-out method for the browser or device that sends it.

We will verify requests by matching information you provide with information we maintain and may request additional information where reasonably necessary. We will use verification information only for verification, fraud prevention, and compliance. If we cannot verify your identity or authority, or if an exception applies, we may deny the request and explain the basis as required by law.

An authorized agent may submit a request on your behalf where permitted by law. We may require proof of the agent's authority and may ask you to verify your identity or confirm that you authorized the request. Parents or legal guardians may submit appropriate requests regarding a child where applicable.

If we deny a request and your state provides an appeal right, you may appeal by emailing privacy@kitearn.com with the subject "Privacy Appeal". We will respond within the period required by applicable law and provide information about any further complaint process available to you.

13. Additional disclosures for California residents

This section supplements the rest of the Policy for California residents. The terms used here have the meanings given in the California Consumer Privacy Act, as amended (CCPA). Legal exemptions may apply, including for certain information governed by the Gramm-Leach-Bliley Act, the California Financial Information Privacy Act, or the Fair Credit Reporting Act.

13.1 Notice at collection and 12-month disclosure

The table below describes categories of personal information Kitearn may have collected during the preceding 12 months, or expects to collect when the corresponding feature is used. Our actual collection depends on the Services available to and used by you. Section 3 describes source categories, Sections 4–7 describe purposes and recipients, and Section 10 describes retention criteria.

CCPA category	Examples	Source categories	Recipients and sale / sharing status
Identifiers	Name, contact details, online identifiers, IP address, account credentials, SSN, taxpayer or government ID information.	You; devices; identity, financial, employment, product, marketing, and fraud providers.	Service providers, financial-product partners, affiliates, legal/corporate recipients, and advertising/analytics partners for limited online identifiers. May be sold/shared to financial-product partners in compensated referrals; online identifiers may be shared for targeted advertising.
Customer-record information	Address, phone, employment, income, bank/payment information, and other information described by California Civil Code § 1798.80(e).	You; financial, employment, identity, and product providers.	Service providers, financial-product partners, affiliates, and legal/corporate recipients. May be sold to a financial-product partner in a compensated referral; sensitive information is not shared for cross-context advertising.
Protected characteristics	Age and, where legally required for eligibility or compliance, citizenship, residency, marital, military, or similar status.	You; identity and compliance providers.	Service providers, financial-product partners when necessary, and legal recipients. Not sold or shared for targeted advertising.

CCPA category	Examples	Source categories	Recipients and sale / sharing status
Commercial information	Products considered, requested, obtained, or used; transaction and interaction history.	You; Services; financial-product and payment partners.	Service providers, financial-product partners, affiliates, and analytics partners. May be sold/shared in compensated referrals or for targeted advertising where permitted.
Internet or electronic activity	Browsing, app interactions, clicks, referral URLs, device and diagnostic events.	Automatically from devices and Services; analytics, advertising, and referral partners.	Service providers and analytics, advertising, referral, security, and corporate recipients. May be sold/shared for targeted advertising, analytics, or attribution.
Geolocation	Approximate location; precise location only when enabled and disclosed.	IP address; device with permission; fraud providers.	Service, security, fraud, and analytics providers; financial partners where necessary. Approximate location may be shared for advertising; precise location is not sold/shared for targeted advertising.
Audio, electronic, or visual data	Support calls, chat, recordings, ID images, selfies, or similar data when the feature is used and notice is provided.	You; support and identity-verification providers.	Service providers, legal recipients, and financial partners when necessary. Not sold/shared for targeted advertising.
Professional or employment information	Employer, occupation, employment status, income, pay schedule, hours, and payroll data.	You; employer, payroll, employment-data, and financial providers.	Service providers, financial-product partners, and legal recipients. May be sold to a financial-product partner in a compensated referral; not shared for targeted advertising.
Inferences	Product-fit, eligibility, preference, engagement, fraud, and risk indicators.	Derived from information described in this Policy.	Service providers, financial-product partners, analytics partners, and legal/corporate recipients. May be sold/shared in compensated referrals or for targeted advertising, except sensitive-derived inferences.
Sensitive personal information	SSN, account login or financial-account data, precise geolocation, government ID data, and other data treated as sensitive by law.	You; authorized financial, identity, employment, credit, or compliance providers.	Service providers and financial-product partners only for requested services, security, compliance, or other permitted purposes. Not sold/shared for cross-context behavioral advertising.

13.2 California rights

Subject to the CCPA's scope and exceptions, California residents may request to know or access, correct, or delete personal information; obtain information about categories, sources, purposes, recipients, sales, and sharing; opt out of sale or sharing; limit use and disclosure of sensitive personal information when used beyond permitted purposes; and receive nondiscriminatory treatment. You may exercise these rights through Section 12.

California's "Shine the Light" law may allow certain residents to request information about disclosure of personal information to third parties for their own direct-marketing purposes. You may submit such a request to privacy@kitearn.com. We do not disclose text-message opt-in consent for third parties' own marketing.

14. Nevada and other U.S. state disclosures

Nevada residents may submit a verified request to opt out of a covered sale under Nevada law by emailing privacy@kitearn.com. We will process the request as required by law.

Residents of other states with comprehensive privacy laws may have rights described in Section 12, including access, correction, deletion, portability, opt-out, appeal, and nondiscrimination rights. The exact rights, definitions, and exceptions vary by state. If a state law requires us to provide a list of specific third parties to which we disclosed personal information, you may request that list through Section 12 where the right applies.

15. Financial privacy and consumer reports

Information collected in connection with a financial product may be governed by federal or state financial privacy laws and may be exempt from some state privacy-law provisions. If Kitearn or a financial partner establishes a customer relationship covered by the Gramm-Leach-Bliley Act or Regulation P, a separate U.S. Consumer Privacy Notice will describe applicable collection, sharing, and opt-out practices. A bank, lender, card issuer, or other financial partner may provide its own notice.

Consumer reports and information derived from them are governed by the Fair Credit Reporting Act (FCRA). Kitearn does not currently obtain your consumer report or credit score. A lender or other financial provider may obtain and use a consumer report under its own privacy notice, permissible purpose, and any required authorization. The provider that makes a credit decision or takes adverse action based on a consumer report is responsible for any required adverse-action notice. Kitearn may receive limited referral-status information, such as whether an application was submitted, approved, opened, or funded, but not the consumer report itself. You retain any rights available under the FCRA.

16. Children's privacy

The Services are intended only for individuals who are at least 18 years old and are not directed to children under 13. We do not knowingly collect personal information from children under 13. If you believe a child has provided personal information to us, contact privacy@kitearn.com. We will investigate and take appropriate steps, including deletion where required. We do not knowingly sell or share personal information of consumers under 18.

17. Changes to this Policy

We may update this Policy as our Services, practices, partners, or legal obligations change. We will post the updated Policy and revise the "Last updated" date. If changes are material, we will provide additional notice or obtain consent when required by law. Your use of the Services after an update is subject to the updated Policy to the extent permitted by law.

18. Contact us

Questions, concerns, or privacy requests may be sent to:

Kitearn Inc.
Attn: Privacy
Privacy: privacy@kitearn.com
Support: support@kitearn.com
General: info@kitearn.com
Website: <https://kitearn.com>