COCOA
INVEST

PRIVACY POLICY

How we collect, use and protect personal data

Version: 1.2
Effective date: 13 September 2026

This policy explains how COCOA Invest Ltd ("COCOA", "we", "us" or "our") collects and uses personal data when you visit our website, use our app, apply for or hold an account, invest through us or contact us.

It applies wherever you access or use our services and should be read with our Cookie Policy, customer terms and the information for the product you choose. Service availability is governed by those terms and applicable law; this policy does not itself make any service available in a country or jurisdiction.

1. Who we are and how to contact us

COCOA Invest Ltd is the controller of the personal data covered by this policy. We are registered in England and Wales under company number 14765783 at 71–75 Shelton Street, Covent Garden, London WC2H 9JQ. We are authorised and regulated by the Financial Conduct Authority (FCA), firm reference number 1017814.

This policy covers applicants, customers, prospective customers, website and app users and people who communicate with us, wherever they are located. Our services are for adults and we do not knowingly open accounts for children.

Contact our Data Protection Lead at support@cocoainvest.com. Please do not attach identity documents or other sensitive documents to your initial email. If we need them, we will explain how to provide them securely.

2. What we collect, why and on what basis

Personal data	How we use it and our main lawful basis
Identity and contact	Name, date of birth, nationality, address, email, telephone and account identifiers: to assess and administer your application and account (contract) and meet regulatory duties (legal obligation).
KYC and financial crime	Identity documents, proof of address, selfie/video, liveness and face-match results, device/fraud signals, sanctions, PEP and adverse-media results: to verify identity and prevent financial crime (legal obligation and substantial public interest).

Personal data	How we use it and our main lawful basis
Financial and payment	Bank-account details, payment status, account-ownership checks and information you authorise through open banking: to process and reconcile payments, prevent fraud and deliver the service (contract, legal obligation and legitimate interests).
Account and investment	Applications, acceptances, products, portfolios, orders, holdings, cash, fees, FX, distributions, withdrawals and confirmations: to perform our contract, keep regulatory records and protect legal rights.
Communications	Emails, secure messages, calls, chats, complaints, feedback and notices: to support you, evidence instructions and meet legal and regulatory duties.
Device data and essential diagnostics	IP address, device and app identifiers, browser, operating system, login/audit records, network-derived location, security alerts and technical error details: to operate and secure the service, detect faults and investigate failures (legitimate interests and legal obligation). Optional behaviour tracking is described in section 8 and is treated separately.
Preferences and marketing	Channel preferences, consent and campaign engagement: to respect your choices and send permitted marketing (consent or legitimate interests where electronic-marketing law allows).

You must provide information marked as required during onboarding or an order. Without it, we may be unable to verify you, open or maintain an account, execute an instruction or comply with law.

We collect special-category personal data only where it is necessary and permitted by law, principally biometric data used to verify identity and information you choose to provide so that we can meet an accessibility need.

3. Identity checks, biometric data and automated decisions

Didit is our identity-verification and fraud-prevention technology provider. We use Didit for identity-document verification, proof-of-address checks, facial matching, liveness testing and financial-crime screening. Depending on the check, it may process identity-document and contact details, document images, proof of address, selfie/video and liveness media, facial measurements, IP address, device fingerprint, network-derived location and sanctions, PEP, adverse-media or fraud indicators.

Facial information used to identify you is special-category biometric data. We process it to prevent fraud and unlawful acts and to meet financial-crime controls, relying on the substantial-public-interest conditions available under UK law. COCOA is controller for the checks we instruct; Didit generally acts as processor, although its own notice explains limited processing it undertakes as an independent controller for security and fraud prevention.

Automated checks may approve an application, request more information, refer it for review, restrict an account or cause us to refuse a service. If an automated outcome has a legal or similarly significant effect, email support@cocoainvest.com to ask for human review and provide additional evidence. We may be legally restricted from explaining every financial-crime indicator.

4. Where data comes from and who receives it

We obtain data directly from you; from your device and use of our services; and, where relevant, from Didit, GoCardless, your bank, product and custody providers, fraud-prevention and screening sources, public registers, regulators and professional advisers.

We do not sell personal data. We disclose only what is reasonably necessary to:

- Didit and other identity, fraud, sanctions and screening providers;
- GoCardless, your bank and other payment or open-banking providers;
- the bank, issuer, custodian, depositary, nominee, broker or FX provider involved in your product or order, as identified where relevant in the product documents;
- PostHog for the optional analytics and recordings described in section 8; Sentry for technical error reporting; and hosting, cybersecurity, communications, document-delivery, support and professional-service providers acting under appropriate controls;
- Apple and Google for app distribution and device-platform services; and
- the FCA, ICO, HM Revenue & Customs, law-enforcement bodies, courts, ombudsmen or another authority where requested or required.

Where aggregate or non-identifying information is sufficient, we do not provide customer-level data. A provider or regulator may nevertheless require an individual record or sample for an audit, legal obligation or regulatory responsibility. Some regulated providers act as independent controllers and their own privacy notices also apply.

5. Payments and open banking

GoCardless Ltd ("GoCardless") provides payment and open-banking technology. It is authorised by the Financial Conduct Authority under the Payment Services Regulations 2017, registration number 597190, for the provision of payment services. An open-banking connection is made only after you authorise it through the relevant bank or provider screen. Depending on the permission shown, information may include account-holder name, account number and sort code, address, balance and transaction information. We use it only for the stated purpose, such as verifying account ownership, arranging or reconciling a payment and preventing fraud.

You can withdraw an open-banking permission through the relevant bank or provider. This will not reverse an authorised payment or remove records we must retain. GoCardless and your bank may act as independent controllers for their regulated services.

6. International transfers and security

Our principal storage is in the United Kingdom or European Economic Area. If personal data is accessed or transferred elsewhere, we use a lawful mechanism where required, such as UK adequacy regulations, the UK International Data Transfer Agreement, the UK Addendum to EU Standard Contractual Clauses or binding corporate rules, together with appropriate risk assessment and safeguards. Contact us for information about the relevant protection.

We use proportionate measures designed to protect personal data, including access controls, authentication, encryption, audit logging, supplier checks, confidentiality, incident procedures and data minimisation. No digital service can guarantee absolute security, so keep your login details and devices secure and tell us promptly about suspected unauthorised access.

7. How long we keep data

In line with UK legal and regulatory requirements, including applicable FCA rules, we retain the records needed to demonstrate that we have completed customer onboarding, identity verification and anti-money laundering checks.

Verification records are securely stored on our behalf by our specialist identity-verification provider, using encryption and controlled access. We retain the necessary compliance evidence for the periods required by applicable law and regulation.

Record	Usual period
Customer, account, contract, transaction, communication and complaint records	Usually six years after the relationship ends or transaction completes, whichever is later.
KYC and anti-money-laundering evidence	Usually five years after the relationship ends, or longer where another legal, FCA, complaint or fraud requirement applies.
Raw selfie/video/liveness media and reusable biometric templates held for COCOA verification	Retained in line with the legal and regulatory requirements applying to the check. Where the material is necessary compliance evidence, the KYC period above applies. Retention of other biometric material is limited to what is necessary for its verification or fraud-prevention purpose.
Unsuccessful or abandoned applications	Usually 12 months, except where KYC, sanctions, fraud, complaint or legal requirements justify longer.
Security logs and inactive marketing prospects	Security logs normally up to 24 months; inactive prospect data normally 24 months after the last meaningful interaction. A minimal suppression record may be kept to respect an opt-out.

Optional analytics and recordings are not retained simply because financial-services records must be kept. Their retention is limited by the usability or performance question being examined, whether individual detail is still needed and whether an identified issue has been resolved. The applicable period will be stated before optional collection begins. When relying on the aggregate-statistics exception, we retain individual-level information only as long as needed to produce the aggregate results. Consent records are kept for as long as needed to honour the choice and demonstrate lawful use.

A period may be extended where necessary for an investigation, regulatory request, complaint, litigation or legal hold. Afterwards we delete or anonymise the data, or isolate it from routine use where immediate backup deletion is not possible.

8. Analytics recordings and communications

We may communicate by email, SMS, telephone, push notification, in-app or secure message, post, WhatsApp or another channel you permit and we support. Essential service, security and regulatory messages are not marketing. We send marketing only where privacy and electronic-marketing law permits and you may opt out using the unsubscribe option supplied with the message or by emailing support@cocoainvest.com.

PostHog provides usage analytics and session-recording technology for our website and apps. Where enabled with your consent, this may collect pages or screens visited, buttons or links used, event times, device and app details, and session or account identifiers linking activity to you. Session recordings reconstruct your on-screen interactions to help us identify usability problems. The consent information will explain the features offered and the data involved before collection begins.

We require a separate opt-in before optional individual behaviour tracking or recordings begin, including before login. Accepting the Customer Agreement, acknowledging this policy or confirming a product does not provide that consent. Refusing does not prevent you from using our core service. Where optional tracking is offered, a withdrawal control must also be available; withdrawal stops future optional collection, recordings and related optional event forwarding. You can also contact support@cocoainvest.com. We retain a limited record of your choice to respect it and demonstrate compliance.

Sentry supports fault detection and error reporting. Diagnostic information may include error messages, app or browser version, device information and events leading to an error. We limit collection to what is needed for the stated purpose. Essential security and fault diagnostics are separate from optional usage analytics; general session recording does not become essential merely because it helps debugging. Recordings must exclude sensitive information such as passwords, payment details and identity-verification documents.

PostHog and Sentry process the relevant information under our instructions and contractual controls; section 6 explains international-transfer safeguards. Necessary diagnostics rely on our legitimate interests in a reliable, secure service and applicable legal duties. Optional individual analytics and recordings require consent. Any lawful exception for limited aggregate statistics requires clear information and a simple, free objection route. It does not cover retained individual activity histories or general session replay.

This section covers technologies built into our mobile apps as well as our website and customer web app. Our Cookie Policy gives further information about device storage and choices. Device or browser controls are additional to the choices we must provide.

9. Your rights

Depending on the circumstances and the law that applies to you, you may ask us to access, correct, delete or restrict personal data; provide portable data; explain processing; or review a qualifying automated decision. You may withdraw consent at any time and object to processing based on legitimate interests. These rights are not absolute: financial-crime, FCA and legal-record duties may require us to keep or use information.

Email support@cocoainvest.com. We may verify your identity and normally respond within one month, subject to any lawful extension.

Your right to object: You may object at any time to direct marketing. You may also object to legitimate-interest processing because of your particular situation.

10. Questions, complaints and changes

Contact our Data Protection Lead at support@cocoainvest.com. We will acknowledge a data-protection complaint within 30 days, investigate it without undue delay and communicate the outcome. You may also complain to the UK Information Commissioner's Office at ico.org.uk/make-a-complaint or, where another data-protection law applies, to the competent supervisory authority in the country where you live or work. Contacting us first does not affect that right.

We may update this policy when our services, providers or legal obligations change. Our website shows the current version and effective date. For a material change, we will give any required notice summarising the change, its effective date and a link to the dated policy. Minor editorial corrections do not require a separate notice unless the law requires one. If a new use requires consent, we will ask separately before it begins.