

BlackCloud Privacy Policy

1. Who We Are

BlackCloud Ltd (“**BlackCloud**”) is a company registered in England and Wales (company number: [XX]). For the purposes of UK GDPR and the Data Protection Act 2018, BlackCloud is the data controller in respect of personal data collected through the BlackCloud Platform and Website, and described in this Privacy Policy.

This Policy applies to visitors to our Website and to prospective and current Members. We take appropriate measures to secure and maintain the confidentiality and privacy of personal data in compliance with the UK GDPR and the Data Protection Act 2018. Where we are subject to EU data protection law in relation to individuals in the EEA, we also comply with the EU GDPR to the extent applicable.

You are under no obligation to provide us with your personal information; however, we may not be able to provide you with certain products and/or services if you refuse to provide it.

The Website and Platform are not intended for children, and we do not knowingly collect personal data relating to children.

2. Definitions

Controller: the entity that determines the purposes and means of the processing of Personal Data.

ICO: the Information Commissioner's Office, the UK's independent supervisory authority for data protection.

Introduction: BlackCloud's disclosure to one Member of another Member's identity in connection with an asset or opportunity listed on the Platform.

Member: any individual or entity admitted to the Platform, including Asset Owners, Members and Referral Partners, as those terms are defined in the applicable agreement entered into with BlackCloud.

Personal Data: any information relating to an identified or identifiable living individual.

Platform: the online platform operated by BlackCloud at www.blackcloud.space, together with the services provided by BlackCloud through it.

Processor: an entity that processes Personal Data on behalf of the Controller.

Special Category Data: personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic or biometric data, health data, or data concerning a person's sex life or sexual orientation.

UK GDPR: the UK General Data Protection Regulation as it forms part of UK domestic law, as amended from time to time (including by the Data (Use and Access) Act 2025).

Website: our website at www.blackcloud.space.

3. Data We Collect

We collect personal data in the following categories, depending on your relationship with the Platform:

- (a) Membership and identity data: name, surname, email address, telephone number, billing address, proof of identity, source of funds information and account login details.
- (b) Financial and transaction data: billing information and payment status. Card payments are processed by our payment service providers; we do not normally store full card details.
- (c) Investment profile data: asset class preferences, target geographies, investor classification and self-certification confirmations.
- (d) Technical and usage data: IP address, browser type, device identifiers, operating system, logs, cookies, and information about your use of our Website and Platform.

- (e) Marketing and communications data: your preferences in receiving marketing from us and our third parties and your communication preferences.
- (f) Verification data (only where necessary): where strictly required for compliance, fraud prevention or security, we may request additional verification information (for example, a copy of an identity document). We will only request such data where necessary for the relevant purpose and will limit it to what is required.
- (g) Data from third parties: we may receive personal data about you from third parties, including Referral Partners who refer you to the Platform (your identity and contact details), KYC/AML verification and screening providers (identity verification, sanctions and politically exposed person screening results), and publicly available and online sources, including Companies House and other company or regulatory registries, government databases, sanctions lists, company websites, professional and social networking platforms, search engines, news and media publications, and other publicly accessible sources.

4. How We Use Your Data and Our Lawful Basis

We process personal data for the purposes and on the legal bases set out below (as applicable):

- (a) Creating and managing your member account, and conducting KYC/AML identity verification.
Legal basis: performance of a contract with you and/or compliance with a legal obligation (where applicable) and/or our legitimate interests in verifying Members and protecting the integrity of the Platform.
- (b) Processing payments, maintaining records, and complying with tax and accounting obligations.
Legal basis: performance of a contract with you and/or compliance with a legal obligation.
- (c) To operate, maintain, secure and improve our Website and Platform (including troubleshooting, security monitoring, fraud prevention and service analytics).
Legal basis: our legitimate interests (for example, to keep our services secure and improve them), and/or compliance with a legal obligation where applicable.
- (d) To facilitate introductions between members and communicate with you about service-related matters (including changes to our terms/policies, security notices, and important administrative messages).
Legal basis: performance of a contract and/or our legitimate interests.
- (e) To comply with legal and regulatory obligations.
Legal basis: compliance with a legal obligation.
- (f) Marketing communications (where permitted)
Where required by law, we will send you marketing communications only with your consent, or where otherwise permitted (for example, “soft opt-in” for existing customers). You can opt out at any time by using the unsubscribe link in our emails or contacting us.
Legal basis: consent and/or legitimate interests (as applicable).

If we rely on your consent for any processing, you can withdraw your consent at any time. Withdrawal of consent does not affect the lawfulness of processing carried out before withdrawal.

Direct marketing

During the registration process on our website, when your personal data is collected, you will be asked to indicate your preferences for receiving direct marketing communications from BlackCloud via Email.

You can ask to stop sending you marketing communications at any time by following the opt-out links within any marketing communication sent to you or by contacting us at [EMAIL].

If you opt out of receiving marketing communications, you will still receive service-related communications that are essential for administrative or customer service purposes.

Special category and criminal offence data

We do not seek to collect Special Category Data and ask that you do not provide it to us unless we specifically request it. Where our KYC/AML, sanctions and PEP screening processes involve information that touches on criminal offences or alleged unlawful conduct (for example, a sanctions designation), we process that information in reliance on the condition in Schedule 1 to the Data Protection Act 2018 relating to the prevention or detection of unlawful acts, and/or another applicable substantial public interest condition.

Automated Decision-Making

We do not currently make decisions based solely on automated processing (including profiling) that produce legal effects concerning you or similarly significantly affect you. Where we use automated tools to support sanctions or PEP screening or KYC verification, any adverse match is reviewed by a member of our team before any decision is made to decline, suspend or terminate your Membership. If this changes, we will update this Policy and, where required by law, provide you with information about the logic involved and your right to request human intervention.

5. Who We Share Your Data With

We do not sell your personal data. We may share it in the following circumstances:

- **With other Members (limited)**

When a formal Introduction is made, your name, professional contact details and the relevant listing details are disclosed to the counterparty Member. This disclosure is made under the non-disclosure and non-circumvention obligations in the applicable agreement entered into with BlackCloud.

- **With service providers**

We use carefully selected third-party service providers to help us operate the Platform, including:

- KYC/AML verification and identity screening providers;
- Secure document storage and data hosting providers;
- Email and communication platform providers; and
- Payment service providers
- IT security and fraud prevention services

All service providers are required to process your data only on our documented instructions and are bound by appropriate data processing agreements.

- **With other recipients**

We may also share personal data, where necessary: (a) with our group companies, including Kofman + Partners Ltd, for the purposes of operating and administering the Platform, providing shared administrative, IT and back-office support, internal reporting and governance, and, where you request or engage advisory services from Kofman + Partners Ltd in connection with a Transaction, for the purpose of providing those services, in each case on the basis of our legitimate interests in the efficient administration of our group's business or the performance of a contract with you; (b) with the Referral Partner who referred you, limited to confirming your status as a referred party and the fees relevant to calculating that Referral Partner's commission; and (c) with our professional advisers, auditors, insurers and bankers, for the purposes of obtaining advice, managing risk and complying with our legal and other obligations.

- **With regulators and law enforcement**

We may disclose personal data to the Financial Conduct Authority, HMRC, law enforcement authorities or other competent regulators where we are required to do so by law, court order or regulatory direction.

6. In the event of a business transfer

If BlackCloud is acquired, merged or its assets transferred to a third party, personal data held about Members may be transferred as part of that transaction. We will notify affected Members in advance where legally permissible.

7. International Transfers

Where we transfer personal information outside the UK or the EEA, we will ensure appropriate safeguards are in place (for example, adequacy regulations/decisions or standard contractual clauses), as required by applicable law.

8. Retention

We retain personal data only for as long as necessary for the purposes for which it was collected, taking into account our legal and regulatory obligations. Where retention is required for legal compliance, we will retain the minimum data necessary and will apply appropriate access restrictions during the retention period. We periodically review the data we hold and delete or anonymise it once it is no longer needed.

Data Type	Retention Period
Member account and profile data	Duration of membership plus 6 years after termination
KYC/AML verification records	5 years from the end of the business relationship (as required by the Money Laundering Regulations 2017)
Introduction records	6 years from the end of the relevant contractual relationship or the completion or termination of any transaction arising from the Introduction, whichever is later.
Communications and transaction records	6 years from the end of the relevant relationship or transaction
Technical and usage data (logs, cookies)	Up to 12 months
Prospective member enquiry data (unsuccessful applicants)	Up to 12 months
Financial and transaction data (payment and billing records)	6 years from the end of the relevant accounting period, for tax and accounting purposes
Marketing preference data	Until you withdraw consent or opt out, plus a short period afterwards to record your preference

9. Your Rights

Under UK GDPR, you have the following rights in relation to your personal data. You can request a copy of the personal data we hold about you (a Subject Access Request), and ask us to correct any inaccurate or incomplete data. You can request that we delete your personal data where there is no overriding lawful basis for us to retain it, or ask us to restrict our processing of it in certain circumstances, such as while a dispute is resolved. You can also ask to receive your data in a structured, machine-readable format so that it can be transferred to another controller.

Where we process your data based on legitimate interests, you can object to that processing; we will stop unless we can demonstrate compelling legitimate grounds to continue. Where we rely on your consent, you can withdraw it at any time, without affecting the lawfulness of anything we did with your data before you withdrew it. If we ever make a decision about you based solely on automated processing that has a legal or similarly significant effect on you, you have the right to request human intervention, express your point of view, and contest that decision.

To exercise any of these rights, please contact us at [\[EMAIL\]](#). We will respond to your request within one calendar month of receipt. Where a request is complex, or we have received a number of requests from you, we may extend this

period by a further two months; if so, we will let you know within one month of your request and explain why the extension is necessary. You will not normally have to pay a fee to exercise your rights, but we may charge a reasonable administrative fee, or decline to act on a request, if it is clearly unfounded, repetitive, or excessive.

10. How to Complain

If you are unhappy with how we have handled your personal data, you may complain to us directly in the first instance by contacting [EMAIL]. We will acknowledge your complaint within 30 days of receipt and aim to resolve it without undue delay.

This does not affect your right to complain to the Information Commissioner's Office (ICO) at any time, whether or not you have raised the matter with us first. You can contact the ICO at ico.org.uk or by calling 0303 123 1113.

11. Security

We implement appropriate technical and organisational security measures to protect your personal data against unauthorised access, loss, destruction or alteration. These measures include encrypted storage, access controls, role-based permissions and regular security reviews. However, no method of transmission over the internet or electronic storage is completely secure, and we cannot guarantee absolute security.

We have procedures in place to deal with any suspected personal data breach and will notify you and the ICO of a breach without undue delay where we are legally required to do so. If you become aware of any security incident affecting your Platform account, please notify us immediately at [EMAIL].

12. Cookies

We use cookies and similar tracking technologies on www.blackcloud.space. Full details of the cookies we use, their purpose and how to manage your preferences are set out in our Cookie Policy, available at www.blackcloud.space/cookies.

13. Changes to This Policy

We may update this Privacy Policy from time to time to reflect changes in applicable law, regulatory requirements, technology, or our practices. We encourage you to review this Privacy Policy periodically to ensure that you remain informed about how we process your personal data. Where appropriate, we may also notify you of material changes. If you do not agree with any changes to this Privacy Policy, you should immediately cease using our Website and Platform and notify us promptly. Any changes will take effect on the date stated in that notice.

14. Contact Us

If you have any questions about this Privacy Policy, want to exercise your rights, or have a privacy-related complaint, please contact us:

BlackCloud (**Data Controller**)

Email: [EMAIL]

Address: [ADDRESS]