Data Privacy Notice

This Privacy Notice ("**Notice**"), together with our website terms of use and any documents referred to in it, explains the types of personal data Citrus Capital LTD collects, how we collect and process it, who we may share it with in connection with our services, and the rights and choices you have.

This Notice is addressed to individuals outside our organisation, including visitors to our website, clients and potential clients (and their representatives), contacts at counterparties and advisers, suppliers and service providers, and visitors to our offices. It applies to personal data provided directly to us or obtained from third parties. (Personal data processed for internal employment purposes is covered by our internal policies.)
We are committed to fair and transparent processing in accordance with applicable UK data protection law, including the **UK GDPR** and the **Data Protection Act 2018** (as amended from time to time). If you have questions about this Notice, contact dataprotection@citruscf.com

Who is responsible for your personal data?
Citrus Capital LTD ("**Citrus Capital**", "**we**", "**our**", "**us**") is incorporated in England and Wales (No. 16295942), authorised and regulated in the UK by the Financial Conduct Authority (FRN 1034933), and has its registered office at City Reach, 5 Greenwich View Place, London, E14 9NN, United Kingdom.
Citrus Capital is the **data controller** of personal data described in this Notice.
We are also registered with the Information Commissioner's Office (ICO) under registration number ZB902149.

Personal data we collect about you
"Personal data" is information that identifies you or can be linked to you. The categories we may collect and process (non-exhaustive) include:

- Identity & Contact Data – name, title, role, employer, business contact details; for compliance purposes, date of birth, nationality, and government ID details.
- Business Information – information provided during pitches/engagements/transactions; board and authorisation details; correspondence and instructions.

- KYC/AML & Due Diligence Data – beneficial ownership, sanctions/PEP screening results, adverse media results, directorships, criminal record information where permitted by law.
- Financial & Billing Data – bank and invoicing details, payment records.
- Services & Communications Data – emails and letters; recorded lines/meeting recordings where legally required or disclosed; meeting notes.
- Website/Technical Data – IP address, device/browser type, log files, analytics and cookies (see our Cookies Policy).
- Physical Access & Security – visitor logs and CCTV where in operation.
- Recruitment Data – CVs, qualifications, references, interview notes, right-to-work checks.
- Special Categories/Criminal Data – processed only where necessary and lawful (e.g., for anti-financial-crime checks or regulatory obligations).

How we use your personal data

We may use personal data to:

- Provide and administer services – corporate finance activities, mandates and transactions.
- Onboard and verify – identity verification, KYC/AML, sanctions screening and ongoing monitoring.
- Meet legal and regulatory obligations – FCA rules, tax reporting, anti-financial-crime, and responding to regulators or authorities.
- Manage relationships and contracts – engagement letters, billing and payment processing.
- Communicate – routine correspondence and updates relating to services and transactions.
- Operate our website and IT – security, support, maintenance, analytics.
- Recruit – assess and progress applications and keep appropriate records.
- Protect legal rights – risk management, fraud prevention, establishing or defending legal claims.
- Professional updates/marketing – sector or firm updates where permitted (with opt-out).

Lawful grounds for using your data

We rely on one or more of the following lawful bases:

- Contract – to take steps at your request or perform a contract with you/your organisation.
- Legal obligation – to comply with UK law and regulatory requirements (e.g., AML/CTF).
- Legitimate interests – to operate and improve our business, ensure IT and site security, manage engagements, and send professional updates to business contacts (balanced against your rights).
- Consent – where required (e.g., certain marketing or where special category data is involved). You may withdraw consent at any time.

Automated processing

We do not carry out automated decision-making or profiling that produces legal or similarly significant effects.
However, we may use automated tools for purposes such as sanctions screening, anti-money laundering checks, or adverse media searches. These tools are always subject to human review and oversight before any decision is made.

Information about other people
If you provide information about someone else (e.g., a colleague, director or beneficial owner), you should ensure they are aware of this Notice and that you are authorised to share their data with us.

Children's data
Our services are directed at business professionals and corporate clients. We do not knowingly collect or process personal data relating to children under the age of 18. If you believe that we have inadvertently collected such data, please contact us and we will delete it.

Disclosure of your personal data
We may share personal data, where appropriate and lawful, with:

- Service providers – IT hosting/support, communications platforms, screening/verification, and other outsourced functions under contract.
- Professional advisers – auditors, insurers, lawyers and accountants.
- Transaction participants – counterparties and their advisers where necessary for a deal.
- Regulators and authorities – FCA, HMRC, law enforcement or courts, where required.
- Group/Corporate – in the context of a restructure, merger or sale, subject to confidentiality.

We require recipients to protect personal data and use it only for lawful purposes. We do **not** sell personal data.

International transfers
Some of our IT and communications providers (for example, Microsoft and Google) may store or access data outside the UK. In such cases, we ensure that international transfer safeguards are in place, including the UK International Data Transfer Agreement (IDTA) or Standard Contractual Clauses (SCCs), and conduct Transfer Risk Assessments where required.

Security of your personal data
We implement technical and organisational measures designed to protect personal data against unauthorised access, alteration, disclosure and loss, including access controls, encryption in transit and at rest where appropriate, network security, staff training and governance policies. We test and review these measures regularly.

How long we keep your personal data

We retain personal data only as long as necessary for the purposes for which it was collected and to meet legal, regulatory and business requirements. Typical periods include (subject to applicable rules):

- Client/matter files – generally at least 6 years after matter/relationship ends.
- KYC/AML records – generally at least 5 years after relationship ends.
- Recruitment data – usually up to 6 months if unsuccessful (longer if you consent or if necessary to defend legal claims); retained within HR files if hired.
- Website logs/analytics – short operational/security periods.

We may retain data longer where required for investigations, regulatory requests or legal claims.

Failure to provide personal data

If you do not provide information we need to comply with law or to perform a contract, we may be unable to proceed with onboarding, deliver services or complete a transaction.

Your rights

Subject to legal limitations, you have rights to:

- Be informed about our processing (this Notice).
- Access your personal data.
- Rectify inaccurate or incomplete data.
- Erase data in certain circumstances.
- Restrict processing in certain circumstances.
- Object to processing based on legitimate interests and to direct marketing.
- Data portability where applicable.
- Withdraw consent where processing relies on consent.

When you exercise these rights, we may need to verify your identity before acting on your request. We aim to respond within one month, although this may be extended by a further two months for complex requests. If an extension is required, we will inform you within the first month.

To exercise your rights, contact dataprotection@citruscf.com.

You also have the right to complain to the ICO at www.ico.org.uk

You can also contact the ICO at: Information Commissioner’s Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF. Tel: 0303 123 1113.

Marketing

We may send professional updates relevant to our services. For business contacts, we may rely on our legitimate interests or the “soft opt-in” provisions under the Privacy and Electronic Communications Regulations (PECR). In other cases, we will obtain your consent before sending marketing communications. You can opt out at any time using the unsubscribe link or by emailing unsubscribe@citruscf.com.

Contact us

Questions, requests and complaints regarding this Notice or our handling of personal data should be sent to dataprotection@citruscf.com.

You can also reach us at:

Address: City Reach
5 Greenwich View Place
London E14 9NN
United Kingdom

Telephone: +44 (0) 800 208 4784

Changes to this Notice

We may update this Notice from time to time to reflect changes in law or in our processing activities. Any changes will be posted on this page with an updated “Last updated” date. Please review it periodically.

Last updated: August 2025