1 Introduction

Cygnum Capital Group Limited and its subsidiaries (together, "Cygnum Capital", "the Group", "we", "us" or "our") are committed to protecting the privacy of the individuals whose personal data we handle. This Privacy Notice explains what personal data we collect, why we collect it, the legal basis on which we use it, who we share it with, how long we keep it, and the rights you have in relation to it.

This notice applies to personal data we process about clients and prospective clients, investors and prospective investors in the funds we manage or advise, investee companies, borrowers and counterparties, and the directors, officers, shareholders, beneficial owners, employees and representatives of any of them. It also applies to service providers and business contacts, visitors to our websites, attendees at our events, and job applicants. It does not apply to our own employees, workers and contractors, whose personal data is covered by a separate Staff Privacy Notice.

The Group operates in several jurisdictions. Our principal operations are in the United Kingdom, and this notice is written primarily by reference to the UK General Data Protection Regulation ("UK GDPR"), the Data Protection Act 2018 and the Privacy and Electronic Communications Regulations 2003, each as amended by the Data (Use and Access) Act 2025. Where your personal data is processed by a Group entity in another jurisdiction, the local data protection law described in the section headed "Who we are" applies in addition, and the rights described in this notice are subject to that law.

This notice does not form part of any contract with you. It does not apply to third-party websites, applications or services, including those linked from our website, which are governed by their own privacy terms.

2 Who we are

Cygnum Capital is a specialist investment bank and alternative investment fund manager focused on Africa and emerging markets, with offices in London, Amsterdam, Dubai and Africa. Each Group entity listed below is a separate data controller for the personal data it collects and uses in the course of its own business. Where two or more Group entities jointly determine the purposes and essential means of processing, they may act as joint controllers. Where applicable, we will make available the essence of the joint-controller arrangement, including the allocation of responsibilities for responding to data subject requests. If you would like to know which entity holds your personal data, please contact us using the details in the section headed "How to contact us".

Entity	Regulatory status	Data protection law and registration
Cygnum Capital Group Limited	Group holding company, registered in England and Wales, company number 11312267	UK GDPR
Cygnum Capital Asset Management Limited ("CygCap AM")	Registered in England and Wales, company number 11543285. Authorised and regulated by the FCA, FRN 830100	UK GDPR; ICO registration ZB089181
Cygnum Capital Advisory Limited ("CygCap Adv")	Registered in England and Wales, company number 11543029. Authorised and regulated by the FCA, FRN 829523	UK GDPR; ICO registration ZB089168

Entity	Regulatory status	Data protection law and registration
Cygnum Capital B.V. ("CygCap NL")	Licensed AIFM, supervised by the Dutch Authority for the Financial Markets ("AFM") and De Nederlandsche Bank ("DNB"). Registered in the Netherlands, KvK number 82981590.	EU General Data Protection Regulation ("EU GDPR") and the Dutch GDPR Implementation Act (UAVG); supervisory authority: Autoriteit Persoonsgegevens
Cygnum Capital Middle East Limited ("CygCap ME")	Authorised and regulated by the Dubai Financial Services Authority ("DFSA"), DFSA reference F006396. Registered in the DIFC, number CL4344.	DIFC Data Protection Law No. 5 of 2020; registered with the DIFC Commissioner of Data Protection
Cygnum Capital Africa Limited (Kenya) and Cygnum Capital Nigeria Limited (Nigeria)	Not regulated by a financial services authority	Applicable local data protection law

Funds managed or advised by the Group. Many of the funds for which CygCap NL acts as alternative investment fund manager, and to which CygCap AM provides portfolio management services, are established in Luxembourg and supervised by the Commission de Surveillance du Secteur Financier ("CSSF"); others are established in other jurisdictions. The controller or controllers responsible for investor data will depend on the relevant fund structure and the purposes and means of processing. The applicable fund privacy notice, provided with its offering documents or separately, identifies the relevant controller arrangements. Where both notices apply, they should be read together; the fund-specific notice provides further information about processing undertaken for that fund. Where Group entities process investor data on behalf of a fund, for example in carrying out investor due diligence, they do so as that fund's processor or as a separate controller for their own regulatory obligations, as the case may be. The general partners of certain Group-managed funds are also Group affiliates. Where they act as controller of fund-related personal data, the relevant fund privacy notice applies.

3 The personal data we collect

The personal data we process depends on our relationship with you. It will typically include your name, job title, employer and contact details. For clients, investors, investees and counterparties, it will also include the identification and verification information we are required to obtain under anti-money laundering law. This includes copies of passports or national identity documents, proof of address, date and place of birth, nationality, tax residence and tax identification numbers, information about beneficial ownership and control, and information about the source of funds and source of wealth. We also collect information about whether you are, or are connected to, a politically exposed person, and the results of sanctions, adverse media and other screening.

Where we provide services, enter into transactions or receive payments, we process financial information such as bank account details and payment records, together with the records of our communications and dealings with you. As explained below, these records include recordings of certain telephone calls and electronic communications. When you visit our website, we collect technical information such as your IP address, browser type and pages visited, including through cookies. When you attend our events, we collect registration details and any access or dietary requirements you choose to give us. When you apply to work with us, we collect your CV, employment and education history, professional qualifications, references and the results of pre-employment checks.

Special category and criminal offence data. We do not seek to collect special category personal data, such as information about health, religion or political opinions, except where it is necessary for a specific and limited purpose. Examples include health information contained in an access or dietary requirement you have told us about. Politically exposed person screening may incidentally reveal special category data, but PEP status is not, by itself, special category data. Where permitted or required by law, we process information about criminal convictions, offences and alleged offences. We do so to meet our obligations relating to money laundering, terrorist financing, fraud, bribery and corruption, and international sanctions. For job applicants to regulated roles, we also do so to assess fitness and propriety. Where special category data is processed, we identify an applicable Article 9 condition in addition to an Article 6 lawful basis. Criminal offence data is processed only where authorised under Article 10 and applicable domestic law. Where required under UK law, we satisfy the relevant Schedule 1 condition of the Data Protection Act 2018 and maintain an Appropriate Policy Document. Equivalent requirements under EU GDPR, Dutch law and DIFC law are applied where applicable.

4 How we obtain your personal data

Most of the personal data we hold is provided directly by you or by the organisation you represent, whether in correspondence, in meetings, through onboarding forms or through our website. We also obtain personal data from other Group entities. Other sources include the funds we manage and their administrators, depositaries and transfer agents. We may also obtain it from co-investors, co-lenders and development finance institutions with whom we invest, and from recruitment agencies and referees.

In addition, we obtain personal data from third-party screening and due diligence providers, credit reference and fraud prevention agencies, public registers such as Companies House and other company and beneficial ownership registers, regulators' public registers, court and insolvency records, sanctions lists, the press and media, and professional networking sites.

Where you provide us with personal data about other individuals, such as the directors, shareholders, beneficial owners, guarantors, signatories or employees of an organisation, you should make sure they are aware that you are doing so. Please also draw this notice to their attention.

5 How we use your personal data and our legal basis

We may only use your personal data where the law allows us to. The table below sets out the main purposes for which we use personal data and the legal basis on which we rely for each.

Purpose	Legal basis
Carrying out client, investor, investee and counterparty due diligence, including identity verification, beneficial ownership, source of funds and source of wealth, politically exposed person, sanctions and adverse media screening, both at onboarding and on an ongoing basis	Legal obligation (anti-money laundering, counter-terrorist financing and sanctions laws in the UK, the Netherlands, Luxembourg and the DIFC); legitimate interests in managing financial crime and reputational risk; an applicable Article 9 condition for special category data and Article 10 authorisation for criminal offence data, supported by the relevant domestic-law conditions where required
Providing our investment banking, advisory and asset management services, managing and administering funds and investments, and performing our contracts	Performance of a contract with you; legitimate interests where the contract is with the organisation you represent

Purpose	Legal basis
Meeting our regulatory obligations, including record keeping, recording of telephone calls and electronic communications, regulatory and transaction reporting, market abuse surveillance, managing conflicts of interest and responding to regulators	Legal obligation; legitimate interests in operating a compliant business
Tax reporting under FATCA and the Common Reporting Standard	Legal obligation
Preventing and detecting fraud and other crime, and reporting suspicions to the authorities	Legal obligation; legitimate interests, including recognised legitimate interests in detecting and preventing crime
Managing our relationship with you, sending you information about our services, insights and events, and developing our business	Legitimate interests; consent where required for electronic marketing
Operating our website and understanding how it is used	Legitimate interests; consent for non-essential cookies
Recruitment, including assessing applications, obtaining regulatory references and carrying out fitness and propriety and background checks for regulated roles	Steps prior to entering a contract; legal obligation (including the FCA's Senior Managers and Certification Regime and the DFSA's approved individual regime); legitimate interests
Establishing, exercising or defending legal claims, and recovering amounts due to us	Legitimate interests; legal claims for special category data
Business reorganisations, such as a sale, merger or restructuring of any part of the Group	Legitimate interests

Where we rely on legitimate interests, we have considered whether our interests are outweighed by your rights and freedoms and concluded that they are not. You can ask us for more information about this assessment. Where we rely on consent, you may withdraw it at any time without affecting the lawfulness of processing carried out before withdrawal.

Where personal data is needed to meet a legal obligation or to enter into a contract, and you do not provide it, we may be unable to onboard you, provide our services or proceed with a transaction.

Recording of communications. In line with FCA requirements, telephone conversations and electronic communications relating to certain activities are recorded and retained. These include activities relating to transactions in financial instruments and client orders. Recordings may be used for regulatory compliance, monitoring, training, and the investigation of complaints or disputes. Comparable record-keeping or communications-recording requirements may apply to our regulated entities in the Netherlands and the DIFC, depending on the activity and applicable regulatory rules.

Direct marketing. We will only send you electronic marketing where the law permits us to. For individuals, this generally means with your consent or, where the statutory conditions are met, under the soft opt-in for existing customers. Different rules apply to communications sent to corporate email addresses. Every marketing message will tell you how to unsubscribe. You can object to direct marketing at any time, and we will stop.

6 Automated tools and artificial intelligence

We use automated screening systems and artificial intelligence tools to help us carry out due diligence, sanctions, politically exposed person and adverse media screening, and regulatory reporting. These tools help our staff identify and prioritise information. They do not make decisions about you. Decisions with legal or similarly significant effects, such as whether to onboard a client, are subject to meaningful review and determination by appropriately qualified staff; automated outputs are not treated as determinative. If this changes, we will update this notice and tell you about the safeguards that apply, including your right to make representations, to obtain human intervention and to contest the decision.

The AI tools we use are provided under enterprise terms that prohibit the provider from using our data to train its models. They are subject to our data protection due diligence and, where appropriate, a data protection impact assessment before deployment.

7 Who we share your personal data with

We share personal data within the Group where this is necessary for the purposes described above. Intra-group sharing is governed by our Intra-Group Data Transfer Agreement, which sets out each entity's role as controller or processor and the international transfer safeguards that apply.

We also share personal data with third parties where necessary. These are:

- the funds we manage or advise, and their boards, administrators, depositaries, custodians, transfer agents and auditors;
- co-investors, co-lenders, development finance institutions, banks, brokers and other counterparties to transactions in which we are involved;
- our professional advisers, auditors and insurers;
- service providers who support our business, including providers of IT, cloud hosting, communications, client onboarding and screening, outsourced operational and administrative support, payroll and recruitment services.

Service providers acting as our processors may only use your personal data on our instructions and under contracts that require them to keep it secure.

We disclose personal data to regulators, tax authorities, law enforcement agencies, financial intelligence units, courts and other public bodies where we are required or permitted to do so. In the UK, these include the FCA, HM Revenue & Customs, the National Crime Agency and the Information Commissioner. In the Netherlands, they include the AFM, DNB and FIU-Nederland. In Luxembourg, they include the CSSF and the Cellule de Renseignement Financier. In the DIFC and UAE, they include the DFSA and the UAE Financial Intelligence Unit. Where the law allows, we will tell you about a request for your personal data before we respond. We will not do so where this would prejudice the prevention or detection of crime, or where we are prohibited by law from doing so, for example under the anti-money laundering "tipping off" provisions.

We may also share personal data with a prospective buyer, investor or successor, and their advisers, in connection with a sale, merger or reorganisation of any part of the Group, subject to appropriate confidentiality protections.

We do not sell personal data.

8 International transfers

Because we operate internationally, personal data may be transferred between the UK, the European Economic Area, the DIFC and other countries in which the Group, the funds we manage or our service providers operate.

Where personal data is transferred from the UK, the EEA or the DIFC to a country that has not been recognised as providing an adequate level of protection, we put appropriate safeguards in place. Depending on the transfer and applicable law, safeguards may include the UK International Data Transfer Agreement or UK Addendum to the EU Standard Contractual Clauses, the EU Standard Contractual Clauses, and approved DIFC transfer mechanisms. We assess transfer risks and implement supplementary measures where required; the relevant mechanism depends on the exporter, importer and destination. In limited cases we rely on a derogation, such as where the transfer is necessary for the performance of a contract with you or for the establishment, exercise or defence of legal claims. You can request a copy of the relevant safeguards by contacting us.

9 How long we keep your personal data

We keep personal data for as long as necessary for the purpose for which it was collected, and for any longer period required by law or regulation, or needed to deal with potential legal claims. Our retention periods are set out in our Records Retention Schedule. The main periods are summarised below.

Type of record	Typical retention period
Customer due diligence records and supporting transaction records	At least 5 years after the end of the business relationship or the occasional transaction (Money Laundering Regulations 2017; Dutch Wwft; Luxembourg AML Law), and at least 6 years in the DIFC under DFSA rules
Records of services, transactions and regulated business	At least 5 years, and longer where required by the relevant regulator or the limitation period for claims
Recorded telephone calls and electronic communications	5 years, extendable to 7 years where requested by the FCA
Records relating to regulatory references under the Senior Managers and Certification Regime (SM&CR)	6 years
Marketing and business contact data	Until you unsubscribe or the contact is no longer relevant, reviewed every 2 years
Unsuccessful job applications	12 months after the recruitment process ends
Website and cookie data	As set out in our Cookie Policy

We may keep personal data for longer where we are required to do so by a court, regulator or law enforcement agency, or where it is relevant to an actual or potential investigation or legal claim.

10 How we protect your personal data

We use appropriate technical and organisational measures to protect personal data against unauthorised access, loss, misuse, alteration or destruction. These include access controls, encryption, multi-factor authentication, secure cloud hosting, staff training, and confidentiality obligations on our staff and service

providers. Our information security arrangements are overseen by our Data and IT Governance Committee and are regularly reviewed.

No method of transmission over the internet is entirely secure. If a personal data breach occurs, we will notify the relevant supervisory authority where required. We will also notify you without undue delay where the breach is likely to result in a high risk to your rights and freedoms.

11 Your rights

Depending on the circumstances and the law that applies, you have the following rights in relation to your personal data:

- the right to be informed about how we use your personal data, which this notice is intended to meet;
- the right to obtain a copy of the personal data we hold about you;
- the right to have inaccurate or incomplete personal data corrected;
- the right to have your personal data erased where we no longer have a lawful basis to keep it;
- the right to restrict our use of your personal data, for example while a dispute about its accuracy is resolved;
- the right to object to processing based on our legitimate interests, and an absolute right to object to direct marketing;
- the right to receive personal data you have provided to us in a portable format where we process it by automated means on the basis of consent or contract;
- the right to withdraw consent at any time where we rely on it;
- rights in relation to automated decision-making, as described above.

These rights are not absolute. They may be limited where we are required to keep or use personal data to comply with our legal and regulatory obligations, including our obligations to prevent financial crime. They may also be limited where exercising them would prejudice the prevention or detection of crime or where legal professional privilege applies.

To exercise any of these rights, please contact us using the details below. We may need to verify your identity before we respond. We will respond within the time limit required by the applicable law, generally one month under the UK and EU GDPR, subject to the statutory rules on when that period begins, identity verification, clarification and permitted extensions. Where a request is complex, or you have made several requests, we may extend this by up to two further months, and we will tell you if we do. We will make reasonable and proportionate searches for the information you request, in accordance with the requirements of the applicable data protection law.

12 How to contact us

If you have any questions about this notice or how we handle your personal data, or you wish to exercise your rights, please contact:

Data Protection Lead
Cygnum Capital Group Limited
130–132 Buckingham Palace Road, London SW1W 9SA, United Kingdom
Email: data.controller@cygnumcapital.com

13 Complaints

If you are unhappy with how we have handled your personal data, please raise a complaint with us in the first instance using the contact details above. You can do so by email or in writing. You do not need to use any

particular form or wording. For complaints governed by UK data protection law, we will acknowledge receipt within 30 days, take appropriate steps to investigate and respond without undue delay, keep you informed about progress as appropriate, and inform you of the outcome. Other applicable local complaint-handling requirements will also be observed.

You also have the right to complain to a data protection supervisory authority. For processing by our UK entities, this is the Information Commissioner's Office (www.ico.org.uk). Where another Group entity processes your personal data, or you live or work in another jurisdiction, you may also complain to the relevant authority. In the Netherlands, this is the Autoriteit Persoonsgegevens (www.autoriteitpersoonsgegevens.nl). In Luxembourg, it is the Commission Nationale pour la Protection des Données (www.cnpd.lu). In the DIFC, it is the Commissioner of Data Protection (www.difc.ae). Elsewhere, you may complain to the data protection authority in the country where you live or work, or where the relevant Group entity is established. We would, however, appreciate the opportunity to address your concerns first.

14 Cookies

Our website uses cookies and similar technologies. Strictly necessary cookies are used to make the website work. Other cookies are used only where you have consented or where the law otherwise permits, as explained in our Cookie Policy. You can manage your cookie preferences at any time through the settings on our website.

15 Children

Our services and website are not directed at individuals under the age of 18. We do not knowingly collect personal data from children, except where a minor is a beneficial owner or connected person and their information must be collected to meet our due diligence obligations.

16 Changes to this notice

We review this notice regularly and will update it when our processing or the law changes. The current version will always be available on our website, and where changes are significant, we will take reasonable steps to bring them to your attention.

This notice was last updated in November 2026.