Vector Capital Privacy Policy

Effective date 25 September 2026

1 About this policy

This Privacy Policy explains how Vector Capital (Pty) Ltd (Vector Capital, we, us or our) collects, uses, shares, stores and protects personal information. It also explains the choices and rights available to the people and organisations whose information we process.

The policy applies to our clients, prospective clients, website visitors, representatives of companies and other organisations, beneficial owners, directors, authorised persons, suppliers and other people who interact with us. We process personal information in accordance with the Protection of Personal Information Act 4 of 2013 (POPIA) and other laws that apply to our activities.

2 Responsible party and scope

Vector Capital (Pty) Ltd is the responsible party for the personal information described in this policy when we determine why and how that information is processed. We are a South African financial services provider authorised under FSP number 55141.

This policy covers personal information processed through our website, correspondence, consultations, client onboarding, investment advice, market execution, discretionary portfolio management, treasury and fixed-income services, digital-asset services where available, and our relationships with service providers and business partners.

3 Personal information we collect

The personal information we collect depends on the relationship and service involved. It may include:

- identity information, including names, identity or passport numbers, nationality, date of birth, photographs, signatures and specimen signatures;
- contact and relationship information, including residential, postal and email addresses, telephone numbers, family or professional relationships and communication preferences;
- client due-diligence information, including tax residence and identification numbers, source of funds and wealth, beneficial ownership, politically exposed person status, sanctions-screening results and information needed for anti-money-laundering checks;
- financial and investment information, including bank and custody details, assets, liabilities, income, investment holdings, transactions, liquidity needs, objectives, time horizon, risk tolerance and investment experience;
- professional and organisational information, including occupation, employer, directorships, company registration details, mandates, authorities and ownership or control structures;
- service and communication records, including applications, agreements, instructions, advice records, suitability assessments, complaints, correspondence and recordings where notice has been given;
- website and technical information, including IP address, device and browser information, cookie identifiers, pages viewed and interaction data; and
- other information that a person provides to us or that we must collect to provide a service or comply with law.

4 Special personal information

Some compliance checks or client circumstances may involve special personal information or information about alleged or actual criminal behaviour. We process this information only where POPIA or another law permits it and only to the extent reasonably necessary for the relevant purpose. We apply additional access and security controls where appropriate.

5 How we obtain personal information

We usually obtain personal information directly from the person or organisation concerned. We may also obtain it from:

- an authorised representative, adviser, family member, employer, trustee or other person acting on the person's behalf;
- public records and public sources, including company, court, insolvency, professional and sanctions records;
- identity-verification, screening, credit-reference, fraud-prevention and market-data providers;
- banks, custodians, brokers, fund administrators, trading venues and other financial institutions involved in providing a requested service;
- our affiliates and business partners, where sharing is lawful and relevant to the relationship; and
- website, email and information-security systems that record technical and communication data.

If a person supplies information about another individual, the person should have authority to do so and should make this policy available to that individual where reasonably practicable.

6 Why we process personal information

We process personal information for purposes that include:

- responding to enquiries and considering whether we can establish a client or business relationship;
- verifying identity, authority, beneficial ownership, source of funds and other information required for client due diligence;
- assessing a client's circumstances, objectives, risk profile and the suitability or appropriateness of products and services;
- providing investment advice, executing transactions, managing portfolios, administering mandates and communicating about accounts and services;
- coordinating with banks, brokers, custodians, administrators, issuers and other providers needed to implement instructions or an agreed mandate;
- meeting legal, regulatory, tax, reporting, record-keeping, audit and supervisory requirements;
- preventing and investigating fraud, money laundering, terrorist financing, market abuse, security incidents and other unlawful conduct;
- managing risk, complaints, disputes, legal claims, conflicts of interest, internal governance and business continuity;
- operating, securing, measuring and improving our website, systems, communications and services; and
- sending service communications and, where permitted, information about relevant services or events.

7 Grounds for lawful processing

Depending on the circumstances, we process personal information with consent; to take steps requested before entering into a contract; to conclude or perform a contract; to comply with a legal obligation; to protect a legitimate interest of the person concerned; or to pursue our legitimate interests or those of a third party where the processing is reasonable and does not unjustifiably infringe privacy.

Where processing depends on consent, consent may be withdrawn by contacting us. Withdrawal does not affect processing that occurred lawfully before withdrawal, and it does not prevent processing based on another lawful ground.

8 Regulatory checks and required information

Financial-services and anti-money-laundering laws may require us to identify and verify clients, representatives and beneficial owners, understand the nature and purpose of a relationship, establish source of funds or wealth, monitor transactions and report specified matters to authorities. We may be unable to establish or continue a relationship, process an instruction or provide a service if required information is not supplied or cannot be verified.

We may screen relevant people and organisations against sanctions, politically exposed person, adverse-media, fraud and other compliance databases. A potential match is reviewed before we take action where the circumstances require human assessment.

9 When we share personal information

We may share personal information where lawful and reasonably necessary with:

- our affiliates, including Berkeley Financial group entities, when they support a service, relationship, compliance function or legitimate business purpose;
- banks, custodians, brokers, exchanges, trading venues, fund managers, product providers, administrators and payment or settlement providers;
- identity-verification, screening, information-technology, cloud, communications, cybersecurity, analytics, document-management and other operational service providers;
- auditors, lawyers, tax advisers, insurers, consultants and other professional advisers who are subject to confidentiality duties;
- the Financial Sector Conduct Authority, Financial Intelligence Centre, South African Revenue Service, Information Regulator, law-enforcement agencies, courts and other competent authorities;
- a prospective buyer, investor, funder or successor in connection with a proposed or completed corporate transaction, subject to appropriate confidentiality and legal safeguards; and
- another person when the data subject instructs or authorises us to disclose the information or when disclosure is otherwise permitted or required by law.

Service providers may process personal information only for the agreed services and must protect it as required by contract and applicable law. Recipients that act as independent responsible parties process information under their own legal duties and privacy notices.

10 International processing

Our international services and technology arrangements may require personal information to be processed outside South Africa. When section 72 of POPIA applies, we take reasonable steps to ensure that the transfer relies on a permitted basis. This may include an adequate foreign law, binding corporate rules, a binding agreement that provides an appropriate level of protection, consent where appropriate, contractual necessity, or another condition allowed by POPIA.

11 Direct marketing

We may send information about our services when the recipient has consented or when another lawful basis permits it. Electronic marketing messages will identify the sender and provide a way to opt out. A person may object to direct marketing or withdraw marketing consent at any time by using the unsubscribe method in the message or contacting us. We may still send communications needed to administer an existing relationship or meet legal duties.

12 Website cookies and external links

Our website uses cookies and similar technologies for security, essential functions, consent management and analytics where permitted. The Vector Capital Cookie Policy explains the cookies in use and how visitors can manage their choices.

The website may link to websites or services operated by other organisations. Their privacy practices are governed by their own notices, and Vector Capital is not responsible for how they process personal information.

13 Retention and deletion

We keep personal information only for as long as reasonably necessary for the purpose for which it was collected, to provide services, to meet legal and regulatory duties, to resolve disputes, or to establish, exercise or defend legal claims. Retention periods differ according to the record and relationship.

Where the Financial Intelligence Centre Act applies, client identification and verification records are generally retained for five years after the business relationship ends, and transaction records are generally retained for five years after the transaction. Other financial-services, tax, corporate and legal requirements may require a different period. When information is no longer required or authorised to be retained, we delete, destroy or de-identify it in a manner intended to prevent reconstruction.

14 Information security and incidents

We use reasonable technical and organisational measures designed to protect personal information against loss, damage, unauthorised destruction, unlawful access and unlawful processing. Measures may include access controls, authentication, encryption where appropriate, secure service-provider arrangements, monitoring, backups, staff confidentiality duties and incident-response procedures.

No system can be guaranteed to be completely secure. If there are reasonable grounds to believe that an unauthorised person has accessed or acquired personal information, we will investigate and notify the Information Regulator and affected data subjects where POPIA requires notification, subject to any lawful delay or restriction.

15 Rights of data subjects

Subject to POPIA, PAIA and other applicable law, a data subject may:

- ask whether we hold personal information about them and request access to it;
- request correction or deletion of information that is inaccurate, irrelevant, excessive, outdated, incomplete, misleading or unlawfully obtained;
- object on reasonable grounds to processing based on a legitimate interest, unless legislation permits or requires the processing;
- object to direct marketing and withdraw consent where processing depends on consent;
- ask for information about the identity of third parties that have had access to their personal information where the law provides that right;
- challenge a decision based solely on automated processing where it produces legal consequences or substantially affects them and POPIA restricts that processing; and
- lodge a complaint with the Information Regulator South Africa.

Requests may be sent to the Information Officer using the contact details below. We may need to verify the requester's identity and authority before acting. A request may be refused or limited where the law permits or requires this, and an access request may be subject to the procedures and fees allowed under PAIA.

16 Children

Our services are not directed to children. We do not knowingly process a child's personal information without the consent of a competent person or another authorisation permitted by law. A parent, guardian or other competent person who believes that a child has provided personal information to us should contact the Information Officer.

17 Changes to this policy

We may update this policy when our services, processing activities, service providers or legal obligations change. The current version will be published with its effective date. Where appropriate, we may also communicate a material change directly to affected people.

18 Contact details

Questions, objections and requests relating to personal information may be directed to:

Vector Capital (Pty) Ltd
Company registration number 2024/672135/07
Authorised Financial Services Provider FSP 55141
Information Officer
Email info@vectorcapital.co.za
Physical address: Unit 108, Bakers Square, Paardevlei, 8 De Beers Avenue, Somerset West, Western Cape, 7130, South Africa

A person who believes that Vector Capital has interfered with the protection of their personal information may lodge a complaint with the Information Regulator South Africa:

Information Regulator South Africa
Woodmead North Office Park, 54 Maxwell Drive, Woodmead, Johannesburg, 2191

Telephone 010 023 5200 or toll-free 0800 017 160
Email POPIAComplaints@inforegulator.org.za
Website inforegulator.org.za