CLEARHOLD

Registration Number: 2026/035423/07
Strategic Capital, Infrastructure & Diversified Group Enterprises
Contact: info@CLEARHOLD.CO.ZA | +27 (0)68 337 6816

VYLER PRIVACY POLICY

Effective date: 10/30/2026
Last updated: 10/30/2026
Platform: Vyler
Website: https://vyler.co.za
Operating company: CLEARHOLD (Pty) Ltd
Company registration number: 2026/035423/07
Privacy enquiries: support@vyler.co.za

1. INTRODUCTION

CLEARHOLD (Pty) Ltd ("CLEARHOLD", "we", "us" or "our") operates Vyler ("Vyler", "the Platform"), a transaction-protection platform designed to facilitate safer transactions between buyers and sellers through structured transaction agreements, protected payments, fulfilment requirements, inspection procedures and dispute-resolution mechanisms.

We recognise that the information entrusted to us is important and must be handled responsibly. This Privacy Policy explains how Vyler collects, uses, stores, processes, protects and shares personal information and relevant business information when individuals access or use the Platform.

Our approach is based on collecting information for legitimate purposes, limiting access to authorised circumstances, protecting stored information, and maintaining appropriate records to support secure transactions and the prevention of fraudulent or unlawful activity.

This Privacy Policy applies to Vyler's ordinary commercial transaction platform, including its website, user accounts, identity-verification processes, transaction workflows, customer-support services and associated features.

It does not govern the separate Sovereign Procurement platform.

2. APPLICABLE PRIVACY LEGISLATION

Vyler processes personal information in accordance with applicable South African law, including the Protection of Personal Information Act 4 of 2013 ("POPIA"), together with other applicable legal and regulatory requirements.

Where applicable, our processing activities may also be informed by obligations concerning customer identification, financial crime prevention, anti-money laundering controls, fraud prevention, recordkeeping and the Financial Intelligence Centre Act 38 of 2001 ("FICA").

The precise legal obligations applicable to a particular processing activity depend on the nature of the activity, the parties involved and the requirements of the relevant law.

Nothing in this Privacy Policy is intended to exclude or diminish a right afforded to an individual under applicable law.

3. OUR APPROACH TO PERSONAL INFORMATION

Vyler follows a purpose-driven approach to information collection and processing.

We seek to collect and retain information that is reasonably necessary to operate user accounts, facilitate transactions, support identity and business verification, administer payments, prevent misuse, resolve disputes and meet applicable legal obligations.

We do not sell users' personal information.

We do not publish users' private identity documents, identity-verification records, personal contact details or other confidential account information as public profile information.

Access to personal information is restricted to authorised circumstances and legitimate purposes, subject to applicable law and our operational arrangements with relevant service providers.

The fact that information is collected does not mean that every employee, service provider or other party has unrestricted access to it.

4. INFORMATION WE COLLECT

The information collected depends on whether a user registers as an individual, represents a business, initiates a transaction, receives a payment or uses another feature of the Platform.

4.1 Individual account information

Vyler may collect and retain information necessary to establish and administer an individual account, including:

- **First name and surname.**
- **Account email address.**
- **Contact information provided by the user.**
- **Account identifiers and account status.**
- **Identity-verification status and relevant verification results.**
- **Transaction participation and associated records.**
- **Information necessary to communicate with the user and provide customer support.**

Additional information may be processed where necessary for a legitimate and disclosed purpose, subject to applicable law.

4.2 Identity-verification information

Vyler uses Didit as an identity-verification service provider for relevant verification processes.

Depending on the verification process, Didit may collect and process identity documents, identity-document images, facial images, liveness-verification information and other information required to perform identity checks.

Verification may include checks involving identity information, document authenticity, facial liveness and comparison against an identity photograph associated with the relevant identity record, where the service and lawful access arrangements support that check.

Vyler does not retain the underlying identity-document images and physical identity-document copies on Vyler's own servers as part of the verification arrangement described in this policy.

Instead, Vyler retains specified information returned through or obtained from the verification process that is necessary to administer the account and its verification status. This may include the individual's name, surname and relevant verification results or status.

The underlying identity documents are processed through Didit's verification infrastructure. Their collection, storage, retention, deletion and any further processing by Didit are also subject to the applicable arrangements and privacy terms governing that service.

The fact that identity documents are not stored on Vyler's servers does not mean that the documents are not processed electronically or retained by Didit or other authorised parties involved in the verification process.

4.3 Business and company information

Where a user registers or transacts on behalf of a company or other legal entity, Vyler may collect and retain relevant business information, including:

- **Registered company or entity name.**
- **Trading name, where applicable.**
- **Entity type.**
- **Registered or physical business address, as applicable.**
- **Company registration information and verification status.**
- **Business account identifiers.**
- **Relevant beneficial-ownership information and verification results, where collected or returned through the applicable verification process.**
- **Information necessary to establish whether the person acting for the entity is authorised to do so.**

Company verification may include checks against company-registration information and available records concerning directors, ownership and beneficial ownership.

The underlying company-registration documents and other supporting documents submitted through Didit are processed through the relevant verification service. Vyler does not retain those underlying document images on its own servers as part of the arrangement described in this policy.

Vyler may retain the specified business information returned through or obtained from the verification process, including the registered entity name, trading name, entity type, physical address and relevant verification information.

The extent of beneficial-ownership information retained by Vyler depends on the fields returned, the verification process and the information necessary for the relevant lawful purpose.

4.4 Transaction information

When a buyer and seller use Vyler, we may collect and retain information necessary to create, administer and document their transaction.

This may include:

- **Transaction identifiers.**
- **Buyer and seller account identifiers.**
- **Descriptions of goods or services.**
- **Transaction values and applicable fees.**
- **Delivery addresses and fulfilment arrangements.**
- **Agreed milestones and deadlines.**
- **Inspection periods and acceptance requirements.**
- **Transaction status and relevant timestamps.**
- **Delivery and fulfilment records.**
- **Supporting evidence submitted in connection with a transaction.**
- **Relevant communications and dispute records.**
- **Payment status and information received from applicable payment or transaction-protection providers.**

Transaction records enable Vyler to administer the agreed workflow, provide customer support, maintain an auditable transaction history and assist with disputes or suspected misuse.

4.5 Payment-related information

Vyler uses third-party payment and transaction-protection infrastructure, including TradeSafe, for relevant protected-funds arrangements.

Depending on the transaction and the services involved, payment-related information processed by Vyler may include transaction amounts, payment status, payment references, applicable fees, release status, refund status and information necessary to reconcile a transaction.

Payment instruments, banking information and protected funds may be handled by the relevant payment or transaction-protection provider in accordance with its role and applicable arrangements.

Vyler does not represent that it independently holds or safeguards funds that are held by a third-party provider. The handling of protected funds is subject to the relevant provider's contractual arrangements and applicable requirements.

Where banking or payment information is supplied to Vyler directly, its collection and handling must be limited to the applicable legitimate purpose and protected appropriately.

4.6 Communications and support information

If a user contacts Vyler, submits a complaint, requests assistance or participates in a dispute, we may process the information supplied in that communication.

This may include correspondence, supporting documents, transaction references, explanations of events and other information reasonably necessary to respond to the matter.

We may retain relevant communications where necessary to maintain service records, investigate complaints, resolve disputes, protect the Platform or comply with applicable legal obligations.

4.7 Technical and security information

When users access the Platform, certain technical information may be collected or generated, depending on the features and technologies in use.

This may include device and browser information, IP addresses, access timestamps, diagnostic information, security logs, authentication events and information about attempted unauthorised access.

Such information may be used to maintain system security, diagnose technical problems, prevent abuse and protect user accounts.

The precise information collected depends on the Platform's actual technical configuration.

5. HOW WE USE PERSONAL INFORMATION

Vyler processes personal information only for legitimate purposes connected with operating and protecting the Platform, providing the requested services or meeting applicable legal requirements.

These purposes may include:

5.1 Account creation and administration

We use relevant information to create user accounts, administer access, maintain account records and communicate with users about their accounts.

5.2 Identity verification

We use verification information and relevant results to establish whether an individual has completed the required identity-verification process.

This helps us reduce impersonation, fraudulent registrations and other forms of account misuse.

5.3 Company and business verification

We process relevant business information to verify the identity and registration status of legal entities and, where applicable, examine ownership and beneficial-ownership information.

These checks help establish whether a business account is associated with an identifiable entity and support the prevention of fraudulent or misleading business registrations.

5.4 Know Your Customer and Know Your Business checks

Where applicable to the transaction, service or legal obligations involved, Vyler may use verification information to support Know Your Customer ("KYC") and Know Your Business ("KYB") processes.

These processes may include identity verification, business-registration checks, ownership checks and relevant screening.

5.5 Financial crime and anti-money-laundering screening

Where applicable, Vyler may process relevant information to support sanctions screening, anti-money-laundering checks, fraud prevention, suspicious-activity assessment and other financial-crime controls.

The scope of screening depends on the services used, available verification information, the nature of the transaction and applicable legal requirements.

Information may be reviewed or escalated where there are reasonable grounds to suspect fraud, impersonation, unlawful activity or misuse of the Platform.

5.6 Transaction administration

We process information to create and administer transactions, record agreed requirements, track milestones, communicate transaction status and support the completion of agreed fulfilment and inspection procedures.

5.7 Payment administration

We process relevant transaction and payment-status information to support payment reconciliation, protected-funds workflows, applicable fee calculations, refunds and communication with payment or transaction-protection providers.

5.8 Dispute resolution

Where a transaction is disputed, relevant information may be used to establish the agreed terms, assess the information submitted by the parties, document the dispute and communicate with the parties and relevant service providers.

5.9 Fraud prevention and security

We may process account, transaction, verification and technical information to identify suspicious activity, detect misuse, investigate suspected fraud, protect the integrity of the Platform and take appropriate protective measures.

5.10 Audits and compliance reviews

User and transaction information may be reviewed as part of authorised audits, internal controls, security reviews, compliance assessments and investigations into suspected irregularities.

Access must be limited to information relevant to the review and to persons or service providers authorised to conduct it.

5.11 Customer support and service improvement

We may use relevant information to respond to enquiries, resolve technical issues, improve reliability, investigate service failures and maintain the quality and security of the Platform.

5.12 Legal obligations and protection of rights

We may process, retain or disclose information where reasonably necessary to comply with applicable law, respond to lawful requests, establish or defend legal claims, enforce contractual terms or protect the rights and security of users and other parties.

6. DIDIT AND THE HANDLING OF VERIFICATION DOCUMENTS

Didit performs the identity-verification and related document-processing functions assigned to it under our service arrangements.

For the verification processes described in this policy, Didit may process identity documents, facial images, liveness information, company-registration documents and other supporting materials necessary to conduct the relevant checks.

Vyler's own systems retain the specified account and business information required for the Platform, rather than the underlying identity-document and company-document images processed through Didit.

The information retained by Vyler may include:

- **An individual's first name and surname.**
- **Relevant identity-verification status or results.**
- **A company's registered name.**
- **Its trading name, where applicable.**
- **Its entity type.**
- **Its physical or relevant registered address.**
- **Relevant company-verification and beneficial-ownership information, where available and necessary.**

Didit may process additional information to perform verification services. The fact that Vyler does not store the underlying documents on its servers does not eliminate Didit's responsibilities or the need for users to review the applicable Didit privacy information.

The parties' precise responsibilities, retention periods, security obligations and permitted uses of information must be determined by the applicable service and data-processing agreements.

Vyler does not promise that Didit deletes all verification information immediately after a check. Any such claim would depend on Didit's actual retention arrangements and applicable legal obligations.

7. BENEFICIAL OWNERSHIP AND BUSINESS SCREENING

Where business verification requires it, Vyler may process information concerning the persons who ultimately own or control a company or other legal entity.

Beneficial-ownership checks may help establish the identity of relevant owners or controllers, verify business information and identify potential inconsistencies or risks.

Such information may also be used, where appropriate and lawful, in connection with sanctions screening, financial-crime prevention, account-risk assessment, audits and investigations into suspected fraudulent activity.

Beneficial-ownership information is treated as confidential account or compliance information. It is not automatically published or made available to other users merely because it has been collected or verified.

Any disclosure must have an appropriate lawful basis and be limited to the relevant purpose.

A match, discrepancy, ownership connection or screening alert does not, by itself, establish that a person has committed wrongdoing. Any necessary review should take account of the relevant facts and the reliability of the information available.

8. HOW WE SHARE INFORMATION

Vyler does not sell personal information.

We may share relevant information with third parties only where there is an appropriate operational, contractual or lawful reason to do so, subject to applicable law and appropriate safeguards.

8.1 Didit

We use Didit for identity verification and related document-processing services.

Information is supplied to or processed by Didit as necessary to perform the relevant verification checks. Didit may process identity and company documents that Vyler does not retain on its own servers.

8.2 TradeSafe

We use TradeSafe for relevant transaction-protection and protected-funds services.

We may exchange transaction references, relevant user or business identifiers, transaction amounts, payment status, fulfilment information and other information necessary to administer the transaction and the applicable protected-funds process.

The information exchanged depends on the specific services and integration in use.

8.3 Payment and financial service providers

Where required to facilitate a payment, refund, reconciliation or other payment-related process, relevant information may be shared with the payment provider involved.

Each provider's role and handling of information are subject to the applicable contractual arrangements and legal requirements.

8.4 Technology and infrastructure providers

We may use service providers to host, maintain, secure and operate the Platform, deliver communications, monitor technical performance or provide other necessary technical services.

Such providers should receive only the information reasonably necessary to perform their assigned functions and must be subject to appropriate confidentiality, security and data-processing requirements where applicable.

8.5 Auditors and professional advisers

Relevant information may be made available to authorised auditors, legal advisers, accountants, compliance professionals or other professional advisers where necessary for legitimate audit, legal, financial, security or compliance purposes.

8.6 Law enforcement and public authorities

We may disclose relevant information where required or authorised by applicable law, pursuant to a valid legal process, or where disclosure is otherwise lawfully necessary to investigate or report suspected unlawful activity.

We will not treat every informal request for information as sufficient authority to disclose confidential user data.

8.7 Transaction counterparties

A buyer and seller may need access to specific information about one another to complete a transaction.

For example, a seller may need the buyer's delivery details, while a buyer may need relevant seller or fulfilment information.

Any such sharing should be limited to the information reasonably required for the transaction and the applicable service.

8.8 Business transfers

If CLEARHOLD undergoes a lawful restructuring, merger, acquisition or transfer of relevant business assets, information may be transferred as part of that process where legally permissible and subject to appropriate safeguards.

The receiving party must handle transferred information in accordance with applicable law.

9. PRIVATE INFORMATION AND PUBLIC VISIBILITY

Vyler's ordinary escrow platform is intended for private commercial transactions between users.

Personal identity documents, private account information, verification records, beneficial-ownership information and confidential transaction records are not automatically displayed publicly.

Information collected for identity verification, business verification, KYC, KYB, financial-crime screening and account security remains subject to the access restrictions and purposes described in this Privacy Policy.

Where transaction information must be shared with a counterparty, service provider, auditor or public authority, the sharing must be limited to the relevant legitimate purpose and permitted by applicable law.

A user's participation in a transaction does not grant other users unrestricted access to that user's private information.

10. LEGAL BASIS FOR PROCESSING

POPIA requires personal information to be processed lawfully and for a specific, explicitly defined and lawful purpose.

Depending on the circumstances, Vyler may rely on one or more lawful grounds for processing, including:

- **The user's consent, where consent is the appropriate legal basis.**
- **Processing necessary to take steps requested by the user before entering into a contract.**
- **Processing necessary to perform a contract with the user.**
- **Processing necessary to comply with an obligation imposed by law.**
- **Processing justified by a legitimate interest recognised under applicable law, subject to the relevant requirements and safeguards.**

The applicable basis depends on the specific information and processing activity.

Consent to a particular verification process does not mean that all subsequent processing is automatically based on consent. Where another lawful basis applies, the processing must be justified on that basis.

Where consent is relied upon, users may withdraw it in circumstances permitted by law. Withdrawal does not necessarily invalidate processing lawfully performed before withdrawal or prevent processing required under another applicable lawful basis.

Where information is necessary to complete a requested transaction, satisfy a legal requirement or perform a required verification, refusing to provide that information may prevent us from providing the relevant service.

11. RETENTION OF PERSONAL INFORMATION

Vyler retains personal information only for as long as reasonably necessary for the purpose for which it was collected, subject to applicable legal, contractual and operational requirements.

Retention periods may vary according to the category of information and the reason it is held.

For example:

- **Account information may be retained while an account remains active and for an appropriate period after closure.**
- **Verification results may be retained as necessary to administer verified accounts, prevent repeated abuse, support audits and meet applicable legal obligations.**
- **Business and beneficial-ownership information may be retained where necessary for business verification, compliance checks, transaction administration and lawful recordkeeping.**
- **Transaction records may be retained for the duration necessary to administer transactions, resolve disputes, establish contractual rights and comply with applicable retention requirements.**
- **Dispute and investigation records may be retained for as long as necessary to resolve the matter, support an audit or investigation, or establish or defend legal claims.**
- **Security logs may be retained for an appropriate period to detect, investigate and prevent unauthorised activity.**

When information is no longer required, we will take appropriate steps to delete, destroy, de-identify or otherwise dispose of it securely, subject to applicable law and legitimate retention requirements.

The retention periods applied by Didit, TradeSafe and other service providers are governed by their respective arrangements and applicable requirements. They may differ from Vyler's own retention periods.

Closing a Vyler account does not necessarily result in the immediate deletion of every record associated with it, particularly where continued retention is lawful and necessary.

12. INFORMATION SECURITY

Vyler takes reasonable and appropriate technical and organisational measures to protect personal information against loss, unauthorised access, misuse, alteration, disclosure and destruction.

Depending on the information and system involved, these measures may include access restrictions, authentication controls, security monitoring, protected communications, infrastructure safeguards, backups and procedures for responding to suspected security incidents.

Access to personal information should be restricted to authorised individuals and service providers who require it for a legitimate function.

However, no online service, database, electronic communication or storage system can be guaranteed to be completely secure.

Users are responsible for maintaining the confidentiality of their account credentials, using appropriate device security and promptly notifying Vyler if they suspect that their account has been compromised.

Where a security compromise affects personal information, Vyler will take appropriate steps to investigate, contain and address the incident and comply with applicable notification obligations.

13. CROSS-BORDER PROCESSING

Some of Vyler's service providers may process or store information outside South Africa.

Where personal information is transferred to or accessed from another country, Vyler will take reasonable steps to ensure that the transfer complies with applicable legal requirements, including the relevant provisions of POPIA.

Depending on the circumstances, this may involve assessing the destination country's protections, contractual safeguards, the recipient's obligations and any applicable exceptions or authorisations under law.

The location and terms of processing by Didit, TradeSafe and other providers depend on their actual infrastructure and contractual arrangements.

Vyler does not represent that all information processed in connection with the Platform is necessarily stored exclusively within South Africa.

14. COOKIES AND TECHNICAL TRACKING

Vyler may use cookies, session identifiers, local storage or similar technologies where required to operate the website, maintain sessions, support authentication, remember relevant preferences, improve reliability or protect against misuse.

Where analytics or optional tracking technologies are used, they should be disclosed and configured in accordance with applicable law and the relevant privacy requirements.

Users may be able to manage certain cookies through their browser settings. Disabling essential technologies may affect the operation of parts of the Platform.

The specific technologies used depend on Vyler's current technical configuration.

15. USER RIGHTS

Subject to applicable law, users may have rights concerning their personal information, including the right to:

- **Request confirmation of whether Vyler holds personal information about them.**
- **Request access to personal information in accordance with applicable law.**
- **Request correction of information that is inaccurate, incomplete, misleading or outdated.**
- **Request deletion or destruction of information where the applicable legal requirements are satisfied.**
- **Object to certain forms of processing where permitted by law.**
- **Withdraw consent where processing relies on consent.**
- **Raise concerns about how their information is collected, used, stored or shared.**
- **Lodge a complaint with the Information Regulator of South Africa where appropriate.**

These rights are subject to applicable legal limitations. For example, Vyler may be unable to delete particular records immediately where continued retention is required by law, necessary for a legitimate legal claim or otherwise lawfully justified.

A request concerning information processed by Didit or another independent service provider may need to be directed to that provider, depending on the provider's role and the nature of the request.

Vyler will assess requests concerning information within its responsibility and respond in accordance with applicable legal requirements.

16. HOW TO SUBMIT A PRIVACY REQUEST

For privacy enquiries, requests to access or correct information, or concerns about the handling of personal information, contact:

Email: support@vyler.co.za
Website: https://vyler.co.za
Organisation: CLEARHOLD (Pty) Ltd

Please provide enough information for us to understand and assess the request. We may need to verify your identity before disclosing, correcting or deleting personal information.

Do not send complete identity documents or sensitive financial information by ordinary email unless we have provided an appropriate and secure method for doing so.

If your request concerns identity documents processed directly by Didit, we may direct you to the appropriate channel or assist with identifying the relevant service provider, as appropriate.

17. COMPLAINTS AND THE INFORMATION REGULATOR

If you believe that Vyler has processed your personal information unlawfully or has failed to respect your rights under POPIA, you may contact us using the details above.

You may also lodge a complaint with the Information Regulator of South Africa through its official channels:

Information Regulator of South Africa
Website: https://inforegulator.org.za/

This does not limit any other rights or remedies available under applicable law.

18. INFORMATION RELATING TO OTHER PEOPLE

Users must not submit another person's personal information unless they have an appropriate lawful basis or authority to do so.

Where a user provides information about a business representative, beneficial owner, delivery recipient or other third party, the user is responsible for ensuring that the information is accurate and that its provision is lawful.

Users must not impersonate another person, submit false verification information, misuse identity documents or attempt to access information they are not authorised to obtain.

Vyler may take appropriate action where information appears to have been obtained unlawfully or supplied in connection with fraudulent activity.

19. AUTOMATED CHECKS AND HUMAN REVIEW

Vyler may use automated tools or third-party services to assist with identity verification, business checks, sanctions screening, risk assessment, fraud detection and security monitoring.

These tools may generate verification results, matches, alerts or risk indicators that require further review.

An automated match or alert does not necessarily establish fraud, wrongdoing or legal liability.

Where appropriate, a result may be reviewed in context, additional information may be requested, or a decision may be escalated for further examination.

Where applicable law provides rights concerning automated decision-making, those rights will be respected.

20. CHANGES TO THIS PRIVACY POLICY

We may update this Privacy Policy to reflect changes in the Platform, the information we process, our service providers, our security measures or applicable legal requirements.

The latest version will be made available through the relevant Vyler website or platform interface, together with an updated effective date.

Where a change requires notification or consent under applicable law, we will take the appropriate steps.

Continued use of the Platform does not override any legal requirement to obtain consent or provide notice for a particular change.

21. CONTACT DETAILS AND RESPONSIBILITY

CLEARHOLD (Pty) Ltd operates Vyler and is responsible for the personal information it processes in connection with the Platform, to the extent that it acts as the responsible party under POPIA.

The roles and responsibilities of Didit, TradeSafe, payment providers and other service providers depend on the particular processing activity and the applicable contractual arrangements.

Where another organisation independently determines the purposes and means of its own processing, that organisation may have separate privacy responsibilities.

For general privacy enquiries or requests relating to information processed by Vyler, contact:

CLEARHOLD (Pty) Ltd
Company registration number: 2026/035423/07
Email: support@vyler.co.za
Website: https://vyler.co.za

22. FINAL STATEMENT

Vyler is committed to handling personal and business information responsibly, limiting its use to legitimate purposes, protecting confidential account and transaction records, and working with relevant service providers to support secure and accountable transactions.

We do not sell users' personal information, and we do not make private identity documents or confidential verification records publicly available through Vyler's ordinary escrow platform.

Information may nevertheless be processed, reviewed or disclosed where reasonably necessary for verification, transaction administration, payment processing, dispute resolution, security, authorised audits, the investigation of suspected suspicious activity or compliance with applicable law.

All such processing remains subject to the applicable legal requirements, the purposes described in this Privacy Policy and the responsibilities of the relevant parties.

End of Privacy Policy