

HVAC GrowthKit Privacy Notice

How we collect use disclose retain and protect personal information

Version 1 | Effective date 15 September 2026

This notice explains how HVAC GrowthKit handles personal information when someone visits our website, contacts us, buys or downloads a product, requests support, joins a mailing list or otherwise interacts with us. We process personal information only for identified and lawful purposes and take reasonable steps to keep it accurate, relevant and secure.

Responsible party	iLiso Digital Marketing, sole trader
Trading name	HVAC GrowthKit
Information Officer	Owner / Information Officer
Privacy email	support@ilisodigital.com
Physical address	58 Buitendag Street, Monte Vista, 7460

1 Who This Notice Applies To

This notice applies to website visitors, prospective customers, purchasers, authorised business users, support contacts and marketing subscribers. It also applies when a business provides us with the details of an employee or representative. The business providing those details must have a lawful basis for doing so and should make this notice available to that person.

2 Personal Information We May Collect

Depending on the interaction, we may collect:

- identity and contact information, such as name, business name, email address, telephone number and physical or billing address;
- order and transaction information, such as product, price, date, invoice details, payment status and refund history;
- account and delivery information, such as login identifier, download entitlement, access time and product version;
- communications and support information, including messages, attachments, feedback, survey responses and complaint records;
- technical and usage information, such as IP address, device or browser information, pages visited, referring source, cookie identifiers and security logs;
- marketing preferences, consent records, unsubscribe requests and campaign engagement; and
- information needed to prevent fraud, protect intellectual property, enforce the licence or comply with law.

We do not intentionally collect full payment-card details. Payment providers normally process those details under their own privacy notices. Do not send passwords, full card numbers or unnecessary sensitive information through support channels.

3 How We Collect Information

We may collect information directly from the person, from an authorised business representative, automatically through the website or digital delivery system, and from service providers involved in payment, hosting, analytics, email, customer support, fraud prevention or product delivery. We may also receive information from public business sources where lawful and relevant.

4 Why We Use Personal Information

Purpose	Typical activities
Orders and contracts	Process payment status, confirm orders, deliver files, administer licences, provide updates and manage refunds.
Customer service	Answer enquiries, troubleshoot access, respond to complaints and keep service records.
Security and enforcement	Authenticate access, prevent fraud and abuse, investigate unauthorised sharing and protect systems and intellectual property.
Business operations	Maintain accounting, tax, audit, supplier, performance and product-improvement records.
Marketing	Send product news or offers where permitted, manage preferences and measure campaign performance.
Legal compliance	Meet legal duties, respond to lawful requests and establish, exercise or defend legal claims.

5 Lawful Grounds

We process personal information where it is necessary to conclude or perform a contract, comply with a legal obligation, protect a legitimate interest of the person, pursue our legitimate business interests in a lawful and proportionate way, or where valid consent has been given. The applicable ground depends on the activity. A person may withdraw consent at any time, but withdrawal does not make earlier lawful processing unlawful and may not affect processing based on another legal ground.

6 Direct Marketing

We will send electronic direct marketing only where permitted by applicable law. Where consent is required, we will request it before sending marketing. Existing customers may receive communications about similar products where the law permits, with a clear opportunity to object. Every marketing message should identify the sender and provide a simple way to unsubscribe. An opt-out request will be honoured and recorded so that further marketing can be suppressed.

7 Cookies and Similar Technologies

Our website may use necessary cookies for security, checkout, preferences and delivery. It may also use analytics or advertising technologies if these are configured. Before launch, the actual website tools must be audited and accurately described in a separate cookie notice or consent tool where required. Browser settings can block some cookies, but this may affect website functions.

8 Sharing Personal Information

We may share relevant information with carefully selected operators and service providers that support:

- payment processing and fraud prevention;
- website, cloud storage, cybersecurity and digital delivery;
- email, customer support, analytics and marketing administration;
- accounting, tax, audit, legal advice and debt recovery; and
- regulatory, law-enforcement or judicial processes where disclosure is lawful or required.

We require service providers to process information for authorised purposes and to apply appropriate safeguards. We do not sell personal information. If the business or relevant assets are reorganised or transferred, information may be disclosed under suitable confidentiality and legal protections.

9 Artificial Intelligence Services

HVAC GrowthKit products may teach customers how to use third-party AI services, but the customer controls what information is submitted to those services. Customers should remove unnecessary personal, confidential and commercially sensitive information and review the AI provider's privacy terms. We will not submit a customer's support material to an AI service unless this is disclosed and there is an appropriate lawful basis and safeguard.

10 Cross Border Processing

Some technology or service providers may process information outside South Africa. Where this occurs, we will use a transfer mechanism permitted by applicable law and take reasonable steps to ensure an adequate level of protection, an appropriate agreement or another lawful basis. The final notice must name or describe the relevant countries or provider locations where reasonably practicable.

11 Retention

We keep personal information only for as long as reasonably needed for the purpose collected, a related lawful purpose, contractual administration, security, dispute handling or legal recordkeeping. Retention periods differ by record type. When information is no longer required, we will securely delete, destroy or de-identify it, subject to backup cycles and lawful holds. Before launch, the business should approve a retention schedule covering orders, invoices, support, marketing consent, access logs and complaints.

12 Security

We use reasonable technical and organisational safeguards appropriate to the information and risk. These may include access control, strong authentication, secure hosting, encryption where appropriate, backups, monitoring, staff confidentiality, provider due diligence and incident procedures. No system is completely secure, and customers must also protect their devices, accounts, passwords and downloaded files.

13 Security Incidents

If we reasonably believe that personal information has been accessed or acquired by an unauthorised person, we will investigate, contain the incident and notify the Information Regulator and affected data subjects where and as required by law, unless a competent authority directs otherwise. Notices will contain the information reasonably available and required by applicable law.

14 Your Rights

Subject to applicable law and appropriate identity verification, a data subject may ask us to:

- confirm whether we hold personal information about them;
- provide access to a record of their personal information;
- correct or update inaccurate, irrelevant, excessive, outdated, incomplete or misleading information;
- delete or destroy information that we are no longer authorised to retain;
- object to certain processing on reasonable grounds;
- withdraw consent where processing relies on consent;
- stop direct marketing; or
- explain or review a decision based solely on automated processing where applicable.

A request may be limited or refused where the law permits or requires this, including to protect another person's rights, privileged information, security or lawful recordkeeping. We will explain the applicable process and any lawful refusal.

15 How to Exercise Your Rights

Send a request to support@ilisodigital.com with enough information to identify the person, the relevant interaction and the requested action. We may request proof of identity or authority and will use it only to verify and process the request. We aim to respond within the time required by

law. Access requests may also be governed by the Promotion of Access to Information Act 2 of 2000 and the business's PAIA manual where applicable.

16 Children and Special Personal Information

Our products are intended for business users and not for children. We do not knowingly collect children's personal information or special personal information unless it is necessary, lawful and appropriately protected. If such information is submitted unnecessarily, contact us so that we can assess and remove it where appropriate.

17 Complaints

Please contact our Information Officer first so that we can investigate. A data subject may also lodge a complaint with the Information Regulator of South Africa using the current contact details and complaint process published at <https://inforegulator.org.za>. Nothing in this notice limits any other remedy available under applicable law.

18 Changes to This Notice

We may update this notice when our practices, providers, products or legal duties change. The current version and effective date should be published on the website. If a change materially affects existing processing, we will provide additional notice where reasonably required.

Privacy Launch Checklist

Complete these items before collecting customer information or accepting payment.

- Insert the responsible party's legal name, registration number, addresses and contact details.
- Appoint and register the Information Officer and any Deputy Information Officers where required.
- Create or update the PAIA manual and make it available where required.
- List every website form, cookie, analytics tag, payment provider, email platform, delivery system and support tool.
- Confirm the information collected, purpose, lawful ground, retention period, provider and processing country for each activity.
- Sign appropriate operator agreements and review provider security and breach-notification commitments.
- Configure consent and unsubscribe records for electronic direct marketing.
- Publish this notice before or when personal information is collected.
- Create procedures for access, correction, deletion, objection, marketing opt-out and identity verification.
- Approve an incident-response plan and maintain the Information Regulator's current contact information.
- Train anyone who handles orders, support requests, mailing lists or customer files.
- Have a qualified South African privacy professional or attorney review the completed notice and actual systems.

Important legal review

This document is a commercial template and not legal advice. It must be completed to match the actual website, payment, delivery, marketing and support systems before publication.