

Security Audit Report

My Property Pages · mypropertypages.com · leads, storage and encryption

Prepared by

Softcado Pvt Ltd

Product

**My Property
Pages**

Review date

11 October 2026

Version

1.0

My Property Pages is a product of Softcado Pvt Ltd. This report sets out what the platform saves, which parts are encrypted, who can see a buyer lead and why another person cannot view or copy it. It is an internal review of the code and the live site, not a certificate from an outside auditor.

1. Summary

✓ **Leads are encrypted on disk**

AES-256-GCM, whole file. Confirmed in code and by the server log line written when the file was converted.

✓ **No customer can read another customer's leads**

Every lead query, edit, note and CSV export filters on the owning account.

✓ **Leads cannot be fetched without signing in**

Measured on the live site: lead list and lead export return 401; the raw data file returns 404.

✓ **All traffic is encrypted**

HTTP redirects to HTTPS (301). TLS 1.3 negotiated. TLS 1.1 refused. HSTS header set for 180 days.

✓ **Passwords are not stored**

bcrypt hashes only.

✓ **Leads are never sold, pooled or shared between agents**

There is no code path that copies a lead to a second account.

2. What was reviewed

The server code that stores and serves leads, the sign-in and admin access checks, the encryption module, the public forms, and the response headers and TLS configuration of mypropertypages.com as measured on 11 October 2026. The mobile apps use the same server and the same rules; they hold no separate copy of the leads database.

3. What is saved, and how it is protected

DATA	STATE	HOW IT IS PROTECTED
Buyer leads Name, phone, email, message, what the buyer is looking for, your notes, stage, follow-up dates, the log of WhatsApp messages sent	Encrypted	The whole leads file is one AES-256-GCM encrypted block. Opened on the server only, at the moment your dashboard or app asks for your leads.
Seller requests Owner name, phone, email, property address, asking price	Encrypted	Same AES-256-GCM encryption as leads.
Contact form messages Name, email, subject, message	Encrypted	Same AES-256-GCM encryption as leads.
Account passwords Your password	Hashed	Only a bcrypt hash (cost 10) is kept. The password itself is never saved and cannot be read back by anyone, including us.
Connected service keys Mail password, API keys for the services the platform uses	Encrypted	Each value encrypted with AES-256-GCM before it is saved.
Agent account record Name, email, plan, billing dates, brand kit	Not encrypted	Kept on the server behind the sign-in and the server firewall. Not encrypted at file level yet. See "Limits".
Property pages and agent profile Photos, price, address, description, the phone and WhatsApp number you publish	Public by design	This is what you choose to show buyers. A hidden or deleted page stops being served.
Page visits Property opened, time, the link that brought the visitor, a random visitor number	Not encrypted	No name, phone number or IP address is written to the visit record. Rows are deleted after 90 days.
WhatsApp taps Property and time only	Not encrypted	Records that someone opened WhatsApp from a page. No name and no number.
Card and bank details Card number, CVV, UPI PIN	Not stored by us	Payments are taken by Razorpay, Apple and Google. Card details never reach our server. We keep the order number, amount and date.

4. Who can see a lead

WHO	ACCESS	DETAIL
You, the account owner	Yes	All leads on your own pages.
Team members you add	Limited	Only leads assigned to them and leads not yet assigned.
Other agents and agencies on the platform	No	Every read, edit, note and export checks the account that owns the lead. A lead number from another account returns "not found".
Visitors and search engines	No	Lead addresses return 401 without a sign-in. The data folder is not served on the web (404).
Someone who obtains the disk or a backup	No	They get an encrypted block. The key is not stored with the data.
Our admin panel	Limited	Shows how many leads each agent received. It does not list buyer names or phone numbers. Seller requests sent to the platform itself, with no agent chosen, are visible so they can be passed to an agent.
Softcado Pvt Ltd engineers with server access	Limited	The server has to open the file to run your CRM and send your alerts, so a person with full server access could do the same. This is encryption at rest, not end-to-end. Access is limited to the operating team.

5. Can a lead be copied?

- **By another customer:** no. Leads are tied to the account that owns the page, and the check is made on the server for every request, not in the app.
- **By export:** only the account owner and their team can download a CSV, and it contains only that account's leads. Cells are escaped so a buyer's name cannot run as a spreadsheet formula.
- **From the server disk or a backup:** the file is an encrypted block and cannot be read without the key.
- **In transit:** every page, the dashboard and the apps talk to the server over TLS.

A lead does leave the server in three cases, each one to deliver it to you or because you switched a feature on: the new-lead email sent to your address, the push notification sent to your phone, and WhatsApp follow-ups, which are sent through the WhatsApp Business Platform run by Meta. Analytics tags such as Google Analytics or the Meta Pixel run on your pages only if you add your own IDs.

6. How the encryption works

- **Algorithm:** AES-256-GCM, an authenticated cipher. Any change to the stored file makes it fail to open instead of opening as altered data.

- **Fresh random value every save:** a new 96-bit IV is generated each time the file is written, so the same data never produces the same output twice.
- **Key:** a 256-bit key derived with scrypt from a secret that exists only in the server configuration. It is not in the data folder, not in the source code and not in the database files.
- **Safe writes:** the file is written to a temporary name and swapped in, so a crash cannot leave a half-written file.
- **Wrong-key guard:** if the file ever fails to open, the server refuses every later write to it, so a configuration mistake cannot overwrite your leads with an empty file.

7. Connection security

- HTTP requests are redirected to HTTPS (301).
- TLS 1.3 with a certificate from Let's Encrypt; TLS 1.1 is refused.
- Strict-Transport-Security for 180 days, including subdomains.
- X-Content-Type-Options: nosniff, X-Frame-Options: SAMEORIGIN, Referrer-Policy: no-referrer.

8. Sign-in and abuse protection

- Passwords are stored as bcrypt hashes. Sign-in with Google, Apple or a one-time code is also available.
- One-time codes expire after 10 minutes and the number of sends and attempts is capped.
- Sign-in tokens are signed by the server. Admin routes also require an admin role, so a customer token cannot open them.
- The API allows 300 requests per 15 minutes per address.
- Public enquiry forms use a hidden trap field, a signed expiring form token, a minimum fill time and a per-form rate limit to keep bots out.

9. Deleting your data

- **Delete account** in the app or dashboard removes your account, pages, profile, agency website, team logins and every lead straight away. No archive copy is kept. Uploaded photo files are cleared in a later sweep.
- If a paid plan lapses, the website is switched off after 7 days and the Pages data is removed after 45 days, with a notice first.
- Page visit records are deleted after 90 days.
- Invoices that the law requires us to keep are retained for the statutory period.

10. Limits of this review

- **This is not end-to-end encryption.** The server holds the key so it can show your leads, send lead alerts and run follow-ups. Encryption at rest protects against a stolen disk or backup; it does not make the data unreadable to the operator.
- **The agent account record is not encrypted at file level.** Names, emails and plan details sit on the server in plain form, protected by the sign-in and server access controls. Passwords are hashed and are not affected.
- **No outside firm has tested the system yet.** This report is an internal review by Softcado Pvt Ltd. It is not a certification and not an independent penetration test.

- **The encryption key is on the same server as the data.** It is kept in the server configuration, outside the data folder and outside the code.
- **A Content-Security-Policy header is not enabled.** Other browser protections are on (HSTS, no-sniff, frame protection, referrer policy).
- **App sign-ins last a long time.** A sign-in stays valid for up to 400 days so agents are not logged out of the app. Keep your phone locked, and sign out on devices you no longer use.

11. Contact

Security questions and reports: mypropertypages.com/contact. My Property Pages is a product of Softcado Pvt Ltd.