

SpotsOnSpots — Security & Privacy Overview

Prepared for property-management and IT review · spotsonspots.com · hello@spotsonspots.com

SpotsOnSpots is a resident-only, in-building parking marketplace operated by Varun Bhatia as a sole proprietorship based in Austin, Texas. This document summarizes how the Service collects, protects, and handles resident data. It is written to answer the questions a building's management or IT team asks before adopting a vendor. Everything here matches our public Security and Privacy pages and can be verified on request.

1. Scope and data minimization

We deliberately hold as little sensitive data as possible. **We never collect or store payment card numbers, bank account or routing numbers, Social Security numbers, dates of birth, or driver's-license numbers.** Payments are arranged directly between residents off-platform, which keeps SpotsOnSpots out of PCI scope entirely.

Data we do hold: resident name, unit, email, phone; vehicle make/model and license plate for an active rental; and the payment-app handle an owner chooses to display. Contact details are exchanged between two residents only after a rental is approved, and are never shown to anyone browsing listings.

2. Infrastructure and subprocessors

The Service runs on managed, industry-standard providers. We do not operate our own servers or data centers.

Provider	Purpose	Location
Supabase	Managed PostgreSQL database, authentication, file storage	United States (us-east-2)
Netlify	Static site hosting and serverless functions	United States / global CDN
Resend	Transactional email (rental notifications, password resets)	United States
SimpleAnalytics	Cookieless, privacy-friendly usage analytics (no personal identifiers)	European Union

3. Encryption

In transit: every connection uses HTTPS/TLS, and HTTP Strict Transport Security is enforced for one year so browsers never fall back to an unencrypted connection. **At rest:** resident data is stored in managed PostgreSQL on Supabase, encrypted at rest with AES-256.

4. Access control and tenant isolation

Authorization is enforced in the database itself using PostgreSQL Row-Level Security on every table, not only in the application interface. Each resident, owner, and building admin can read only the data their role and building permit. A resident of one building cannot access another building's spots, roster, or contact details, even by calling the API directly. Buildings can also be set to a private mode in which listings are visible only to signed-in residents of that building and pages are excluded from search-engine indexing.

5. Authentication

Sign-in is handled by Supabase Auth. Passwords are hashed with bcrypt and are never stored or transmitted in plain text. Sessions use an HTTP-only cookie. Multi-factor authentication for admin accounts is being rolled out (see Section 9, Current limitations).

6. Availability, patching, and backups

Hosting, database, and platform patching are managed by Netlify and Supabase. The database is backed up automatically by Supabase's managed platform. Application dependencies are monitored for known vulnerabilities via automated Dependabot alerts, and every change runs through an automated CI pipeline (linting, tests, an HTML/security check, and end-to-end tests) before release.

7. Data retention, portability, and deletion

A building's directory, listings, rentals, and complete admin action log can be exported to CSV from the dashboard at any time — the data is yours. If a building ends its subscription, its data remains exportable, and we delete personal data on request within 14 days, subject to legal retention obligations. Individual residents may request account deletion at hello@spotsonspots.com on the same terms.

8. Incident response

If we confirm a security incident affecting a building's data, we notify that building's administrator promptly — our target is within 72 hours of confirmation — with what we know and the steps we are taking, and we coordinate on any resident notification. Suspected issues can be reported at any time to hello@spotsonspots.com.

9. Current limitations (stated plainly)

SpotsOnSpots is an early-stage service operated by a single individual. In the interest of an honest review: we do **not** hold a SOC 2 or ISO 27001 attestation; no third-party penetration test has been performed to date; and multi-factor authentication for admin accounts is in progress, not yet enforced. Production database access is limited to the operator and is used only for support and maintenance. We are glad to discuss any of these directly and to complete a building's own security questionnaire.

Vendor security questionnaire — quick answers

Question	Answer
Where is resident data hosted?	Managed PostgreSQL on Supabase, United States (us-east-2).
Is data encrypted in transit and at rest?	Yes. TLS/HTTPS in transit (HSTS enforced); AES-256 at rest.
How is multi-tenant / per-building isolation enforced?	PostgreSQL Row-Level Security on every table, enforced at the database, not just the UI.
How are passwords stored?	Hashed with bcrypt via Supabase Auth; never stored or sent in plain text.
Is multi-factor authentication available?	For admin accounts: in progress, not yet enforced. Honest current state.
Do you store payment card or bank data?	No. Payments are off-platform between residents. Out of PCI scope.
Do you collect SSNs, DOBs, or license numbers?	No.
Who can access production data internally?	The sole operator only, for support and maintenance.
Are backups performed?	Yes, automatically by the managed Supabase platform.
How are vulnerabilities managed?	Automated Dependabot alerts on dependencies; platform patching by Supabase/Netlify; CI checks on every change.

Has a third-party penetration test been done?	Not to date.
Do you hold SOC 2 / ISO 27001?	No, not at this stage.
What is your breach-notification commitment?	Notify the affected building's admin, target within 72 hours of confirmation.
Can we export and delete our data?	Yes. CSV export any time; deletion on request within 14 days, subject to legal retention.
Who owns the data?	The building/its residents. SpotsOnSpots is a processor of it.

This overview is provided for vendor review and is not a contract. It reflects the Service as operated at the time of writing and may be updated. Questions: hello@spotsonspots.com