Security Overview

How BlaBlea protects restaurant and caller data, what a POS integration can and cannot do, and how we respond when something goes wrong.

Last updated January 1, 2026 · Badcompadres LLC · 4539 N 22nd St #4611, Phoenix, AZ 85016, USA

1. Summary

BlaBlea is operated by Badcompadres LLC (Phoenix, Arizona). The platform is a multi-tenant web application hosted on managed cloud infrastructure in the United States. Every restaurant's data is isolated at the database level, all traffic is encrypted, and the POS integration is scoped to reading the menu and creating orders — it never touches payment card data.

2. Infrastructure and hosting

- Application and API run on Cloudflare's edge network; static assets are served over HTTPS only.
- Database, authentication and file storage run on Supabase (PostgreSQL) in a US region.
- Voice, telephony and call recording run on Retell AI.
- All providers are SOC 2 audited at the infrastructure layer; we rely on their controls for physical and hypervisor security.
- No customer data is stored on employee laptops or on unmanaged servers.

3. Encryption

- In transit: TLS 1.2+ for every browser, API, webhook and POS request.
- At rest: AES-256 disk encryption provided by the database and storage layer.
- Secrets, API keys and POS tokens are stored in the platform secret store, never in source code.

4. Tenant isolation and access control

- Every table that holds tenant data enforces PostgreSQL row-level security keyed to the organization, so one restaurant cannot read another's calls, orders or menu.
- Roles are owner, admin, manager and staff, stored separately from user profiles so a role cannot be escalated from the client.
- Platform administrators are a distinct, explicitly granted role with an audited list of holders.
- Internal access follows least privilege; production access is limited to the engineers who need it.

5. Authentication

- Sign-in uses one-time codes sent by email; there are no reusable passwords to leak.
- Sessions are short-lived and refreshed with rotating tokens.
- Team members are added by invitation from an owner or admin, and can be removed immediately.

6. Voice and POS integration scope

- Inbound and outbound voice webhooks are verified per agent, and each location has its own signing key for the tools the agent may call.
- The Clover integration is limited to reading the menu catalog, creating orders, assigning the order-taker employee and sending print events.
- BlaBlea never collects, transmits or stores payment card numbers. Payment is taken by the restaurant on its own POS at pickup.
- POS tokens can be revoked by the restaurant at any time from its POS dashboard, which immediately stops all access.

7. Data handling and retention

- Call audio and transcripts are retained 90 days, then deleted.
- Orders, caller phone numbers and configuration are kept while the account is active.
- Customer data is deleted within 30 days of account termination; an export can be requested before closing.
- Backups are managed by the database provider with point-in-time recovery and expire on their normal schedule.
- We do not sell data and do not allow model providers to train on Customer or caller content.

8. Logging and monitoring

- Application, webhook and POS errors are logged with timestamps and correlation IDs.
- Failed kitchen tickets are queued durably and retried with backoff, so an order is never silently lost.
- Automated monitoring flags authentication failures, POS rejections and abnormal call volumes for review.
- Logs are scrubbed of secrets and are not used for advertising or profiling.

9. Secure development

- Changes are reviewed before release and deployed through an automated pipeline; there is no manual editing of production servers.
- Dependencies are scanned for known vulnerabilities and updated on a regular cadence.
- Preview and production environments are separated, with distinct credentials and databases.
- Security findings are triaged by severity, with high-severity issues addressed as a priority.

10. Incident response

We investigate suspected incidents immediately, contain the issue, and assess what data was affected. If Customer or caller personal information is compromised, we notify affected Customers without undue delay and no later than 72 hours after confirming the breach, with what we know, what we are doing and what you should do. Report a suspected vulnerability or incident to security@blablea.com; we do not pursue legal action against good-faith researchers who report responsibly.

11. Sub-processors

- Supabase — database, authentication, storage (USA).
- Cloudflare — hosting, delivery, network security (global edge, US data residency for application data).
- Retell AI — voice, telephony, recording (USA).
- OpenAI and other LLM providers — language understanding (USA), no training on our data.
- Stripe — payments (USA).
- Resend — transactional email (USA).
- Clover and other POS providers — order push and printing, on the Customer's instruction.
- VoiceMonkey / Amazon Alexa — kitchen announcements, only when enabled by the Customer.

12. Shared responsibility

- BlaBlea secures the platform, the data, the integrations and the release process.
- The restaurant controls who has access to its account, keeps staff accounts current, discloses call recording on its line, and secures its own POS credentials and devices.

13. Documentation and requests

We can provide a signed data processing addendum, complete a standard vendor security questionnaire, and walk your team through the POS scope on a call. Write to security@blablea.com. We are not currently SOC 2 certified as a company; we build on SOC 2 certified infrastructure and are happy to discuss what your procurement process needs.