SERVEGUARD

ServeGuard Restaurant Privacy Policy

Effective date: October 12, 2026

This Restaurant Privacy Policy explains how ServeGuard LLC, a Delaware limited liability company ("ServeGuard," "we," "us," or "our"), collects, uses, discloses, retains, and protects personal information in connection with the ServeGuard Restaurant application, restaurant administrative tools, websites, support, and related services (collectively, the "Restaurant Service"). It applies to restaurant and catering owners, managers, employees, contractors, business contacts, and other individuals who use or interact with the Restaurant Service on behalf of a food-service business.

This policy does not replace the Diner Privacy Policy or Consumer Health Data Privacy Policy, which apply to diners and consumer health data. When ServeGuard processes personal information solely on a restaurant's documented instructions, the restaurant generally determines the purposes and means of processing and ServeGuard acts as its service provider or processor under the Data Processing Addendum ("DPA"). The restaurant's privacy notices and instructions may also apply. ServeGuard acts independently for its own account administration, security, fraud prevention, billing, legal compliance, and business operations.

Current menu experience

ServeGuard currently provides restaurant menu discovery, guest-controlled allergy and dietary filters, and restaurant menu-management and training tools. Menu QR codes identify a restaurant location, not a table, diner, check, or order. Available menus follow the restaurant’s active-menu and scheduling settings. Selecting filters does not submit an allergy report, notify staff, request a food modification, create a review, or confirm that food is safe.

When you continue to a menu, the web QR page or updated diner app sends the selected filter names to ServeGuard to increment the restaurant location’s aggregate totals: menu opens, opens with allergies, and counts for each allergy or dietary preference. No individual menu response, name, account identifier, table, reservation, or per-visit selection record is saved for these totals. Detailed selections are not shown to restaurant staff. Requests still involve ordinary technical information processed by hosting providers; this is not a promise of completely anonymous browsing. Changing filters after opening the menu does not add another count, and repeat menu entries may count again.

In the updated iOS diner app, optional saved allergy profiles remain account-linked and stored with the existing affirmative storage consent. Detailed menu history and the filters used are stored on the device, separated by signed-in account and excluded from app cloud backup. The detailed history is not uploaded; the separate aggregate-count request described above carries no account authentication token or history record. They do not sync between devices. You can delete a menu visit in History. Completing account deletion on a device also clears its local menu history; local copies on other devices must be removed on those devices or by deleting the app.

Table and event check-ins, staff allergy notifications, new reviews, and table assignments are paused in this experience. Their code and prior records are retained, subject to the existing deletion schedules and rights. References below to submissions, sharing with restaurants, response downloads, and reviews describe earlier records and the retained legacy workflow; they do not mean that choosing menu filters activates those features. Any future restoration requires a new product and privacy review and appropriate notice and consent before new collection or sharing.

1. Information we collect

Depending on how the Restaurant Service is used, we may collect the following categories.

Account and identity information

Names, business email addresses, business telephone numbers, job titles, role and permission information, authentication provider identifiers, account status, profile information, invitation records, ownership-verification information, and multifactor or device-verification status. We do not receive or store a user's raw password from Firebase Authentication.

Business, location, and operational information

Restaurant or catering business name, entity and ownership details, addresses, locations, hours, cuisine, contact details, subscription status, table and event configurations, QR-code assignments, staff assignments, internal workflow status, and information submitted during onboarding, verification, or support.

Menu, training, and content information

Menus, menu-source files, menu items, ingredients and allergen information, dietary options, photos, logos, training materials and completion records, notes, and other content a restaurant chooses to provide. Restaurant-app camera or photo-library access is used only when a user chooses to upload restaurant, menu, or related content. ServeGuard does not use the Restaurant app to collect precise location data.

Earlier diner-submission and review information processed for restaurants

Allergy or dietary selections, diner-entered notes, a response identifier, table or event context, timestamps, safety acknowledgments, and limited diner identifiers needed for the visit or event. Allergy-response content and identifying information are separated within the Restaurant Service. Restaurant-facing reviews include a diner's chosen display name; one-to-five ratings for Service, Food, Allergy Communication, and Atmosphere; and a calculated overall average. Reviews do not include written comments. A diner's account email is not included in restaurant-facing review records. Owners and authorized managers may view restaurant-facing reviews; other staff access is restricted according to role.

ServeGuard does not seek complete medical records, diagnoses, government identifiers, or payment-card information in allergy free-text fields, and users should not submit them.

Billing and commercial information

Plan, subscription, invoice, payment status, transaction identifiers, tax and billing contact information, and limited payment-method details provided by the payment processor. Stripe or another disclosed processor handles full payment-card credentials; ServeGuard does not store full card numbers in the Restaurant Service.

Device, usage, and security information

Internet Protocol address, device and application identifiers, operating-system and app version, push-notification token, session and authentication events, approximate network-derived region where made available by infrastructure providers, logs, crash and diagnostic information, timestamps, actions taken, security signals, and records needed to prevent abuse or investigate incidents. We do not use the Restaurant app to collect GPS or precise device location.

Communications and support information

Emails, support requests, demo requests, deletion-cancellation requests, feedback, survey responses, attachments, call or meeting details if arranged, and records of our responses. We may review a specific allergy submission only when reasonably necessary to provide authorized support, investigate security, comply with law, or address a documented dispute. ServeGuard does not routinely inspect individual submissions for unrelated purposes.

2. Sources of information

We collect information:

- directly from restaurant owners, managers, staff, contractors, diners, and business contacts;
- from the restaurant or another authorized user who creates an account, sends an invitation, assigns a role, or uploads content;
- automatically from devices, applications, websites, and infrastructure used to access the Restaurant Service;
- from authentication, payment, email, push-notification, cloud-hosting, and security providers;
- from public business sources and information a restaurant makes public; and
- from referrals, signed agreements, and business partners when lawful.

3. How we use information

We use personal information to:

- create, authenticate, secure, and administer accounts, roles, sessions, invitations, and locations;
- provide Menu QR codes, menu management, training, authorized historical records, account and security notifications, and support;
- process subscriptions, invoices, taxes, refunds, and account deletion or restoration requests;
- verify businesses, ownership, authorization, and compliance with our terms;
- detect, prevent, investigate, and remediate fraud, abuse, tampering, unauthorized access, and security incidents;
- maintain, debug, measure, and improve reliability, accessibility, and product performance using data minimized for the purpose;
- communicate about service, security, billing, legal, and support matters;
- enforce agreements, protect rights and safety, comply with law, and establish or defend legal claims; and
- create aggregated or deidentified information that is not reasonably linkable to an individual and maintain it in deidentified form.

ServeGuard does not use identifiable allergy submissions or other consumer health data to train general-purpose artificial-intelligence models. We do not make medical decisions, employment decisions, or food-safety decisions for restaurants.

4. How we disclose information

We may disclose information as follows.

At the restaurant's direction

We make restaurant account, staff, operational, diner-submission, and review information available to authorized users of the applicable restaurant or catering organization according to configured roles and the restaurant's instructions. Restaurants are independently responsible for their authorized use and for notices they give personnel and diners.

Service providers and subprocessors

We disclose information to vendors that provide cloud hosting, databases, authentication, storage, serverless processing, security, email, communications, app distribution, push notifications, support, and payment processing. They may process information only to perform contracted services, protect the service, or comply with law. Current core subprocessors are identified in the ServeGuard Subprocessor List.

Professional advisers and business administration

We may disclose information to auditors, insurers, lawyers, accountants, and consultants subject to appropriate confidentiality duties, and in connection with financing, diligence, merger, acquisition, reorganization, or sale of assets. A recipient must use personal information consistently with this policy and applicable law.

Legal, security, and safety disclosures

We may disclose information when we reasonably believe disclosure is required by law, legal process, or a valid government request; needed to investigate fraud, misuse, security incidents, or threats; or necessary to protect the rights, safety, and integrity of ServeGuard, restaurants, diners, or others. We evaluate requests and disclose only information reasonably necessary where practicable.

With consent

We may disclose information for another purpose clearly described when we obtain the required consent.

ServeGuard does not sell personal information or consumer health data for money. ServeGuard does not share personal information for cross-context behavioral advertising, use sensitive information to infer characteristics for advertising, or permit data brokers to use Restaurant Service data. We do not provide identifiable diner data for a restaurant's unrelated marketing.

5. Consumer health and allergy data

Allergy and dietary information can be sensitive and may be regulated as consumer health data even when it is not protected by the Health Insurance Portability and Accountability Act ("HIPAA"). ServeGuard is not a healthcare provider or health plan merely because it offers the Restaurant Service, and information in the Restaurant Service may not receive HIPAA protections. Other federal and state privacy, consumer health, breach-notification, and consumer-protection laws may apply.

ServeGuard requires separate diner consent for collection and for sharing a submission with the scanned restaurant or caterer. Restaurants may process that submission only for the visit or event and other authorized, disclosed purposes. Additional details and consumer health rights appear in the Consumer Health Data Privacy Policy.

6. Retention and deletion

We retain information only as long as reasonably necessary for the purposes described, subject to these general periods:

- restaurant-facing allergy-response content and associated identifiers are scheduled for automatic deletion 90 days after submission, unless deleted earlier or temporarily preserved when legally required;
- an original uploaded PDF or spreadsheet menu-source file is scheduled for deletion no later than 30 days after upload; parsed menu records and Customer-approved items remain until deleted or the applicable account is deleted;
- restaurant, owner, manager, employee, location, training, menu, and operational records generally remain until the restaurant deletes them, the account is finally deleted, or they are no longer needed;

- restaurant-facing category ratings remain until the review or diner account is deleted or deletion is otherwise required; affected aggregate ratings are recalculated when a review is removed;
- when an employee requests account deletion, operational access is removed immediately and permanent employee-account deletion is scheduled after seven days unless the employee cancels during that recovery window; an authorized manager may separately remove employee access and the linked account immediately;
- security, access, authentication, and audit logs may be retained for up to 24 months and longer when reasonably necessary for an active investigation, legal obligation, or dispute;
- billing, tax, contract, consent, and transaction records remain as required for financial, legal, and audit purposes; and
- support communications remain as needed to resolve the request, maintain an appropriate record, prevent abuse, or comply with law.

An authorized owner account-deletion request begins a 30-day recovery period. If an owner asks to cancel deletion, the request becomes a priority administrative review, the owner is directed to support, and the pending period is extended to 60 days. Allergy records continue to expire on their original schedule. After final deletion, limited records may remain where required by law, necessary for security or legal claims, or stored temporarily in isolated backups until ordinary rotation. We may retain deidentified information without time limit if we commit not to reidentify it.

7. Security

We use administrative, technical, and physical safeguards designed for the nature of the information and risks involved. Measures may include encrypted transport and provider-managed encryption at rest, authentication and session controls, role-based access, multifactor or device verification features, application integrity controls, logging, least-privilege practices, secure development and review, retention controls, and vendor oversight. No safeguard can guarantee absolute security. Restaurant customers remain responsible for their own devices, networks, credentials, access assignments, exports, and physical QR codes.

If we confirm a security incident affecting personal information, we will investigate, contain, and notify affected customers, individuals, regulators, or others as required by contract and applicable law. Depending on the facts, federal or state breach-notification requirements, including rules applicable to certain health apps, may apply.

8. Privacy choices and rights

Depending on applicable law and the context in which information is processed, an individual may have rights to:

- know or confirm whether we process personal information;
- access and obtain a portable copy of certain information;
- correct inaccurate information;
- delete information;
- withdraw consent where processing relies on consent;
- opt out of a sale, targeted advertising, or certain profiling, although ServeGuard does not conduct those activities as described above;
- receive a list of certain third parties to which consumer health data was disclosed;
- restrict or object to certain processing; and
- appeal a refusal to act on a request.

To make a request, email privacy@serveguardapp.com with the subject "Privacy Request" and describe the request, the applicable restaurant or account, and the state of residence. We may verify identity and authority using account access, email, multifactor verification, business records, or other proportionate methods. An authorized agent may submit a

request where permitted, but we may require proof of authorization and direct identity verification. We will not discriminate for exercising a privacy right.

When we process information only for a restaurant, we may direct the requester to that restaurant or assist the restaurant under the DPA. We may deny or limit a request where permitted, including when identity cannot be verified, information must be retained by law, an exception applies, or disclosure would adversely affect another person's rights. Instructions for appeal will be included in our response. Consumer health-data requests are further described in the Consumer Health Data Privacy Policy.

9. Communications

Administrative, security, billing, and legal communications are part of the Restaurant Service and generally cannot be opted out of while an account remains active. Marketing communications, if any, may be unsubscribed from using the message instructions or by contacting support. Push notifications may be controlled in the application or device settings, although disabling them may reduce operational awareness. ServeGuard email uses serveguardapp.com addresses; replies are directed to support@serveguardapp.com or another stated serveguardapp.com address.

10. Children's information

The Restaurant Service is intended for businesses. Owner and administrator users must be at least 18. A restaurant may authorize staff who are at least 16 only when lawful and appropriate to their supervised job duties. The Restaurant Service is not directed to children under 13, and restaurants must not create accounts for them or instruct them to submit personal information through staff workflows.

11. United States processing

ServeGuard currently offers the Restaurant Service in the United States. Information may be processed and stored in the United States by ServeGuard and its providers. If Customer transfers information from another jurisdiction, Customer is responsible for ensuring a lawful transfer mechanism and notifying ServeGuard before doing so.

12. Third-party services and links

Third-party sites, authentication providers, app stores, and payment services have their own terms and privacy practices. This policy does not govern their independent processing. The Restaurant Service may link to them for convenience; a link is not an endorsement of their privacy practices.

13. Changes to this policy

We may update this policy to reflect legal, security, operational, or product changes. We will post the revised policy and update its effective date. We will provide additional notice and request renewed consent when required for a material change. We will not materially expand the use of previously collected consumer health data without the consent required by law.

14. Contact

ServeGuard LLC 335 Dunhill Way Dr Alpharetta, GA 30005 United States

Privacy requests: privacy@serveguardapp.com Support: support@serveguardapp.com Legal notices: legal@serveguardapp.com