SERVEGUARD

ServeGuard Diner Privacy Policy

Effective date: October 12, 2026

This Diner Privacy Policy explains how ServeGuard LLC, a Delaware limited liability company ("ServeGuard," "we," "us," or "our"), collects, uses, discloses, retains, and protects personal information when you use the ServeGuard diner mobile application, web QR menus, restaurant discovery, saved allergy profile, visit history, reviews, websites, and related support (collectively, the "Diner Service").

Because allergy and dietary information may be regulated as consumer health data, please also read our Consumer Health Data Privacy Policy. It describes consumer health-data categories, sources, purposes, sharing, consent, and additional rights. This policy does not govern a restaurant's independent practices after it receives information you directed us to share; the restaurant's privacy notice may also apply.

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

Account and profile information

If you create an account, we may collect your name, email address, account identifier, sign-in provider, profile preferences, optional phone number, phone- or email-verification status, account-security settings, and authentication events. Firebase Authentication, Apple, or Google processes credentials used for supported sign-in methods. ServeGuard does not receive or store your raw Apple or Google password, and Firebase Authentication does not provide us your raw email-account password.

If you use Sign in with Apple and choose Hide My Email, Apple may provide a private relay email address. ServeGuard treats that relay address as your account email and does not require separate ServeGuard email verification solely because you used Apple authentication.

Saved profiles and earlier allergy records

We may collect allergy and dietary selections, custom allergens, preparation or cross-contact notes, whether the information concerns you or another person, reservation or event name, optional saved allergy profile, safety acknowledgments, consent choices, and the restaurant, caterer, location, table, or event associated with a submission. This information may reveal or permit an inference about health status and is treated as sensitive.

Saving an allergy profile is optional. We request consent before saving it, and declining does not block other Diner Service features. A saved profile can prefill editable menu filters. It is not shared with a restaurant, and changing filters does not change the saved profile.

Earlier visits, reviews, and restaurant interactions

We may collect visit identifiers and dates, scanned restaurant and location, table or event context, review eligibility, one-to-five ratings for Service, Food, Allergy Communication, and Atmosphere, a calculated overall rating, chosen display name, cuisine and recommendation preferences, saved or featured restaurant interactions, and requests to bring ServeGuard to a restaurant. ServeGuard reviews do not accept written comments.

When you submit a review, the restaurant's owners and authorized managers may receive your chosen display name, the four category ratings, the calculated overall rating, visit context, and limited service details. Your diner account email is not included in the restaurant-facing review record. Public users may see only eligible aggregate ratings after ServeGuard's minimum threshold, currently five reviews; they do not see your account email.

Web Menu QR information

No account, name, phone number, table, or reservation identifier is requested for web menu filtering. Filters remain in the page’s memory for menu display and are sent once when continuing for the aggregate counters described above. ServeGuard does not put filters in request URLs, cookies or browser storage, and does not save the request as an individual response. Closing or reloading the page clears its choices. Infrastructure providers may process technical request information; the aggregate counter does not store IP addresses or device identifiers.

Earlier web check-ins collected the form content, collection and sharing consents, restaurant or event context, submission-session information, response identifiers and timestamps. Those earlier records remain governed by their original retention and deletion rules.

Device, camera, usage, and security information

We may collect Internet Protocol address, app and device identifiers, operating-system and application version, push-notification token, session identifiers, authentication and verification events, app-integrity signals, error and diagnostic data, timestamps, and interactions needed to provide, secure, and troubleshoot the Diner Service.

When you choose to scan a QR code, the application uses the camera to read QR-code metadata. ServeGuard does not store the camera image as part of normal QR scanning. You can decline camera access and use another supported method when available. The Diner Service does not collect GPS or precise device location for restaurant discovery. We may receive coarse network or security-region information from infrastructure providers, but we do not use it to track your physical movements.

Communications and requests

We collect information you send in support, privacy, account-deletion, restaurant-request, security, feedback, or legal communications. This may include attachments and account or submission details needed to resolve the request. Authorized support may cross-reference a specific allergy submission when reasonably necessary for your request, security, law, or a documented dispute, but ServeGuard does not routinely inspect individual submissions for unrelated purposes.

2. Sources of information

We collect information:

- directly from you or a parent, guardian, or other authorized person using the Diner Service;
- from restaurants and caterers that configure locations, tables, events, menus, review eligibility, or service records;
- automatically from your device, browser, application, and use of the Diner Service;
- from authentication, cloud-hosting, email, push-notification, application-integrity, and security providers; and
- from public restaurant information and lawful business sources.

3. How we use information

We use information to:

- create, authenticate, secure, and administer diner accounts and sessions;
- provide QR scanning, allergy and dietary submissions, saved profiles, visit history, reviews, recommendations, and support;
- transmit a submission to the restaurant or caterer you select after your separate sharing consent;
- produce a temporary diner-requested download of a submitted record;
- send service, authentication, security, and support communications;
- maintain consent and Terms-acceptance records;
- detect, prevent, investigate, and remediate fraud, abuse, QR tampering, unauthorized access, errors, and security incidents;
- operate, maintain, debug, measure, and improve performance, accessibility, and reliability using information minimized for the purpose;
- enforce our Terms, comply with law, protect rights and safety, and establish or defend legal claims; and
- create aggregate or deidentified information that is not reasonably linkable to you and maintain it in deidentified form.

We do not use identifiable allergy submissions to train general-purpose artificial-intelligence models. We do not use consumer health data for unrelated advertising, eligibility decisions, or data brokerage, and we do not make medical or restaurant-safety decisions for you.

4. When and why we disclose information

Restaurants and caterers you select

After your separate affirmative sharing consent, we disclose your submission to the restaurant or caterer associated with the scanned QR code, in-app location, or event. Authorized restaurant personnel may access it for the visit or event, safety and service follow-up, and appropriate recordkeeping. Restaurant-facing allergy content and identifying information are separated within the system. The restaurant may be an independent Controller or regulated entity and is responsible for its authorized access and practices.

Restaurant owners and authorized managers may receive reviews as described above. Your account email is not included in restaurant-facing review records. ServeGuard does not provide your account email to a restaurant for review follow-up or marketing.

Service providers

We disclose information to providers that perform cloud hosting, database, storage, authentication, application integrity, email, app distribution, push notification, security, logging, and customer-support functions. They may use information only to perform contracted services, protect the service, or comply with law. Principal providers are identified in the ServeGuard Subprocessor List.

Other people you authorize

If you submit information for another person or share a downloaded record, the people you choose may receive it. You are responsible for having authority and for securely handling downloads.

Professional advisers and business transactions

We may disclose information to lawyers, auditors, insurers, accountants, and consultants under confidentiality obligations, and in connection with financing, diligence, merger, acquisition, reorganization, or sale of assets. A successor must handle personal information consistently with this policy and applicable law.

Legal, security, and safety reasons

We may disclose information when reasonably necessary to comply with law or valid legal process; investigate or prevent fraud, misuse, security incidents, or threats; protect ServeGuard, diners, restaurants, or others; or establish or defend legal claims. We evaluate requests and limit disclosure where practicable.

With consent

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

ServeGuard does not sell personal information or consumer health data for money. We do not share personal information for cross-context behavioral advertising, use sensitive information to infer characteristics for advertising, or allow data brokers to use Diner Service data.

5. Legal bases and consent

Depending on applicable law, we process information to provide the Diner Service you request, carry out our Terms, protect the Diner Service and users, comply with law, pursue legitimate operational interests that do not override your rights, and act with your consent.

The retained legacy submission workflow used separate affirmative controls for the following purposes. The current menu experience does not collect or share a restaurant-facing submission, so those submission controls are inactive. Saved-profile storage still uses its own affirmative consent:

- consent to collect and use allergy or dietary information for a submission;
- consent to share that submission with the selected restaurant or caterer;
- acknowledgment that ServeGuard is supplemental and direct restaurant communication remains necessary;
- agreement to Diner Terms and confirmation of eligibility or supervised use; and
- consent to store an optional saved allergy profile.

You may withdraw consent for future processing through available controls or by contacting privacy@serveguardapp.com. Withdrawal does not invalidate processing already completed and may prevent the requested health-data feature from functioning. We do not condition unrelated features on consent to save an optional profile.

6. Retention and deletion

We use the following general retention periods, subject to legal exceptions:

- 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;
- a signed-in diner's separate account copy of an allergy response and visit remains until the diner deletes it or deletes the account;
- an optional saved allergy profile remains until the diner changes it, withdraws the storage choice, or deletes the account;
- one-time web-form sessions expire after five minutes if unused; limited consumed-session and security records may remain briefly to prevent replay, and temporary download authorization expires after 30 minutes;
- category ratings and calculated review averages remain until the review or diner account is deleted or deletion is otherwise required;
- account, authentication, consent, device-security, and access records remain while the account is active and for limited security, legal, or dispute periods afterward; relevant security and audit logs may be retained for up to 24 months or longer for an active investigation or legal obligation;
- support and privacy-request records remain as needed to complete the request, document compliance, prevent abuse, or resolve disputes; and
- deidentified or aggregate information may be retained without time limit if it is maintained in deidentified form.

When you complete verified diner account deletion, ServeGuard initiates deletion immediately rather than using the restaurant-account recovery archive. Diner-owned profile, allergy, visit, and private-rating records, restaurant-facing visit-review records, and the Firebase Authentication user are deleted. Aggregate review statistics are recalculated after the review is removed. Restaurant-facing allergy submissions retain their original 90-day expiration unless an earlier verified deletion right applies.

Limited information may remain in isolated backups until ordinary rotation or where needed for security, fraud prevention, consent records, legal obligations, or claims. We restrict retained information and do not use it for a new purpose.

7. Your privacy rights

Depending on your state and the information involved, you may have the right to:

- know or confirm whether we process your personal information;
- access and obtain a portable copy of certain information;
- correct inaccurate information;

- delete information, including verified earlier deletion of consumer health data where required;
- withdraw consent for future collection, sharing, or saved-profile storage;
- obtain information about certain third parties or affiliates that received consumer health data;
- restrict or object to certain processing;
- opt out of sale, targeted advertising, or certain profiling, although ServeGuard does not conduct those activities as described above; and
- appeal a refusal to act on a request.

To exercise a right, email privacy@serveguardapp.com with the subject "Privacy Request" and describe the request, your account email if applicable, and your state of residence. You may also use in-app controls for profile changes and account deletion. We may verify your identity using account access, email, authentication provider, phone verification, recent service details, or another proportionate method. Verification is designed to avoid collecting unnecessary information.

An authorized agent may act where permitted, but we may request signed authorization and direct verification with you. We will not discriminate against you for exercising a right. We may deny or limit a request where law permits, including when identity cannot be verified, disclosure would adversely affect another person's rights, an exception applies, or information is needed for security, fraud prevention, legal obligations, or claims. Our response will explain any appeal method. Consumer health-data rights are described more fully in the Consumer Health Data Privacy Policy.

8. Account deletion for Apple, Google, and password users

The in-app deletion process supports the authentication method linked to the account:

- Apple users reauthenticate with Apple, ServeGuard revokes the Sign in with Apple authorization, then deletes the account data and Firebase Authentication user;
- Google users reauthenticate with Google, ServeGuard deletes the account data and Firebase Authentication user, and the application disconnects the Google authorization; and
- email-and-password users enter their current password for recent reauthentication before deletion.

If an account has multiple linked providers, the application may require the provider selected by its security logic. If deletion cannot be completed in the app, contact privacy@serveguardapp.com. Deleting the app from a device does not delete the account.

9. Security

We use administrative, technical, and physical safeguards designed for the nature and sensitivity of the information. Measures may include HTTPS/TLS, provider-managed encryption at rest, role-based access, authentication and session controls, optional phone verification, application integrity controls, input validation, logging, secure development and review, separation of allergy content from identifiers, retention controls, and vendor oversight. No service can guarantee absolute security.

You can help by protecting your device, email, phone, sign-in provider, credentials, and downloaded records; reviewing QR destination information; using current software; and reporting suspicious activity. If we confirm a security incident affecting personal information, we will investigate, contain, and provide notifications required by applicable privacy, consumer health, or breach-notification law.

10. Children and teenagers

The Diner Service is not directed to children under 13. A child under 13 may not create an account or submit a form directly. A parent or legal guardian may use the Diner Service in the adult's own name to communicate information concerning a child.

Users ages 13 through 17 may use the Diner Service only with parent or legal guardian supervision and permission. We may request confirmation of age or supervised use where appropriate. A parent or guardian who believes a minor submitted information contrary to this policy should contact privacy@serveguardapp.com so we can review and delete it as required.

11. Communications and choices

Account, security, authentication, privacy, and service communications are part of the Diner Service and may continue while the account is active. Marketing communications, if any, can be unsubscribed from using the message instructions. Push notifications can be controlled in the application or device settings, but disabling them may reduce real-time awareness. ServeGuard messages use serveguardapp.com addresses; replies are directed to support@serveguardapp.com or another stated serveguardapp.com address.

You can control camera, notification, and related permissions through device settings. Denying camera access prevents in-app scanning but does not authorize ServeGuard to collect other location data.

12. United States processing

ServeGuard currently offers the Diner Service in the United States. Information is primarily processed and stored in the United States by ServeGuard and its providers. Provider support, security, or resilience operations may involve other locations as described by the provider and permitted by law.

13. Third-party services and restaurants

Restaurants, caterers, Apple, Google, app stores, and other third parties may independently process information under their own policies. This policy governs ServeGuard, not their independent activities. A restaurant is responsible for information in its own systems or exported by its authorized personnel after receipt, subject to applicable law and its agreement with ServeGuard.

14. Changes to this policy

We may update this policy for legal, security, operational, or product reasons. We will post the revision and effective date and give additional notice when required. We will request renewed consent before materially expanding collection or sharing of previously collected consumer health data when required by law.

15. Contact and appeals

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

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

For an appeal, use the subject "Privacy Appeal" and explain why you believe the request should be reconsidered. We will respond within the period required by applicable law and will identify any available regulator complaint method when required.