# ServeGuard Consumer Health Data Privacy Policy

Effective date: August 15, 2026

This Consumer Health Data Privacy Policy supplements the ServeGuard Diner Privacy Policy and applies to "Consumer Health Data" Processed by ServeGuard LLC, a Delaware limited liability company ("ServeGuard," "we," "us," or "our"). It is intended to provide the disclosures and rights required by applicable United States consumer health-data laws, including Washington's My Health My Data Act and Nevada consumer health-data law. If this policy and the Diner Privacy Policy conflict concerning Consumer Health Data, this policy controls.

"Consumer Health Data" means personal information that identifies or is reasonably linkable to a consumer and identifies or permits an inference concerning the consumer's past, present, or future physical or mental health status, as defined by applicable law. "Process" includes collecting, using, storing, analyzing, sharing, disclosing, or deleting data.

This policy applies whether you use the ServeGuard diner application with an account or submit a web QR form without an account. It does not govern a restaurant's independent Processing after the restaurant receives information you directed us to share. The restaurant's own consumer health-data or privacy notice may apply.

## 1. Consumer Health Data we collect

Depending on what you choose to provide and the feature used, we may collect:

- allergies, allergen selections, dietary restrictions, dietary preferences, sensitivities, and custom allergen descriptions;
- preparation, ingredient, cross-contact, accommodation, or safety notes that may reveal or permit an inference about health;
- whether the information concerns you, another person, or multiple people;
- an optional saved allergy or dietary profile;
- reservation, attendee, or event name when required for a catering or event workflow;
- restaurant, caterer, location, table, event, visit, date, and time context associated with a submission;
- consent choices, safety acknowledgments, response identifiers, and records of when and how the submission was made;
- support communications, deletion requests, or dispute details that include or relate to allergy or dietary information;
- downloaded response records you ask us to generate; and
- technical and security information that can be associated with a Consumer Health Data submission, such as account identifier, one-time form-session identifier, Internet Protocol address, authentication event, device or application identifier, and app-integrity or anti-fraud signal.

We do not intentionally collect diagnoses, laboratory results, prescriptions, genetic data, biometric identifiers, complete medical records, or healthcare-provider records through ordinary ServeGuard allergy forms. Do not enter unnecessary medical records, government identifiers, payment-card data, or unrelated sensitive information in free-text fields.

## 2. Sources of Consumer Health Data

We collect Consumer Health Data:

- directly from you when you create or edit an optional profile, complete a QR or in-app submission, contact support, or make a privacy request;
- from a parent, legal guardian, dining companion, or other person who represents that the person is authorized to submit information for you;
- from a restaurant or caterer only to the limited extent it configures the location, table, event, menu, or service context linked to your submission;
- automatically from the application, browser, device, authentication, and security systems when you use a health-data feature; and
- from service providers acting on our behalf to host, secure, transmit, or support the Diner Service.

We do not purchase Consumer Health Data from data brokers, advertising networks, social-media platforms, or public-record vendors.

## 3. Why we collect and use Consumer Health Data

We collect and use Consumer Health Data only as reasonably necessary to:

- provide the allergy or dietary check-in you request;
- transmit your submission to the restaurant or caterer you selected after separate sharing consent;
- store an optional saved profile after separate consent and allow you to update or delete it;
- maintain your diner-owned allergy and visit history when you are signed in;
- generate a temporary download of your submitted record at your request;
- display the submitted information to authorized restaurant personnel for the applicable visit or event;
- maintain consent, response, and security records; prevent duplicate or replayed web submissions; and protect against fraud, QR tampering, or unauthorized access;
- provide support that you or an authorized restaurant requests concerning a specific record;
- comply with law, respond to valid legal process, protect rights and safety, or establish or defend legal claims; and
- create aggregate or deidentified information and maintain it in deidentified form.

ServeGuard does not use Consumer Health Data for unrelated advertising, cross-context behavioral advertising, data brokerage, employment or insurance eligibility, or training a general-purpose artificial-intelligence model on identifiable submissions. ServeGuard does not make medical, diagnostic, treatment, or restaurant food-safety decisions.

## 4. Consent for collection

Before an in-app or web QR allergy or dietary submission is sent, we request your affirmative consent to collect and use the Consumer Health Data for the check-in and related records described in this policy. That collection consent is separate from:

- consent to share the submission with the selected restaurant or caterer;
- the safety acknowledgment stating that direct communication with restaurant personnel remains necessary; and
- acceptance of the Diner Terms and confirmation that you are an eligible user or are using ServeGuard with required supervision.

We request a separate optional consent before storing an allergy or dietary profile. Declining saved-profile consent does not block other features. A saved profile is not automatically shared with a restaurant.

Where law permits Processing without consent because it is necessary to provide a product or service you specifically requested, protect security and integrity, prevent fraud, or comply with law, we limit Processing to that permitted purpose.

## 5. Consumer Health Data we share

"Share" in this policy means disclosing Consumer Health Data to a third party or affiliate as defined by applicable consumer health-data law; it is broader than "share" for cross-context behavioral advertising under some general privacy laws.

We may share the categories listed in Section 1 as follows:

### The restaurant or caterer you select

After your separate affirmative sharing consent, we share the submission content, response identifier, table or event context, relevant timestamps, and limited identifying information needed for the visit or event with the restaurant or caterer associated with the QR code or in-app selection. Authorized personnel may access it for the check-in, service and safety follow-up, and appropriate recordkeeping. Restaurant-facing allergy content and identifiers are separated in the ServeGuard workflow.

The restaurant or caterer is the specific recipient you selected and may be an independent Controller or Consumer Health Data Regulated Entity. It is not permitted under its ServeGuard agreement to use the submission for unrelated advertising, marketing, profiling, data brokerage, or AI-model training. Its independent legal duties and privacy notice may also apply.

### Processors and service providers

We share Consumer Health Data with providers only as needed to host, store, secure, transmit, support, and delete it. Current relevant categories and entities include:

- Google Cloud Platform and Firebase, for database, storage, serverless processing, authentication, hosting, application integrity, logging, and security;
- Google Workspace or Gmail, only when necessary for an authorized support communication that includes health-related context; and
- Apple or Google authentication and app-distribution services for account authentication and security metadata, although the substance of an allergy submission is not ordinarily sent to Apple or Google merely because you use their sign-in service.

Stripe processes restaurant billing and does not receive diner Consumer Health Data for diner payments because the Diner Service is free.

### Legal, security, and professional recipients

We may share Consumer Health Data with lawyers, forensic or security advisers, insurers, auditors, courts, regulators, law enforcement, or other recipients when reasonably necessary and permitted or required by law to respond to legal process, investigate an incident, protect rights or safety, or establish or defend legal claims. We limit the data and require confidentiality where practicable.

### Business transactions

We may disclose Consumer Health Data in a merger, acquisition, financing, reorganization, bankruptcy, or sale of relevant assets, subject to confidentiality and continued compliance with this policy and applicable law. We will provide additional notice or consent if required.

### At your direction

We share Consumer Health Data with another person or service when you direct us, such as when you save or send a downloaded record. You are responsible for securely handling and directing those copies.

ServeGuard does not share Consumer Health Data with corporate affiliates for independent marketing and currently has no affiliate receiving Consumer Health Data for a separate purpose.

## 6. Consent for sharing

Before sharing a submission with a restaurant or caterer, we request affirmative consent separate from collection consent. The form identifies the recipient using the restaurant, caterer, or venue information linked to the QR code or in-app location. If the intended recipient is wrong, do not submit; notify restaurant personnel or support and scan the correct code.

Your consent applies only to that submission and recipient. It does not authorize the restaurant to use the data for unrelated marketing or authorize ServeGuard to share it with another restaurant. A new visit or recipient requires a new submission and sharing choice.

You may withdraw consent for future sharing by not making a new submission or by contacting privacy@serveguardapp.com. Withdrawal cannot undo a disclosure already completed, but you may request deletion from ServeGuard and the recipient as provided by law.

## 7. Sale and geofencing

ServeGuard does not Sell Consumer Health Data and does not exchange it for money or other valuable consideration in a manner treated as a Sale under applicable consumer health-data law. Because we do not Sell it, we do not request a consumer health-data sale authorization.

ServeGuard does not use geofencing around a healthcare facility or other location to identify, track, collect data from, or send messages to a person related to the person's health status or healthcare services. The Diner Service does not collect GPS or precise device location for restaurant discovery.

If ServeGuard proposes to Sell Consumer Health Data in the future, we would first update this policy, provide required notice, and obtain a separate signed authorization containing the legally required terms. A general acceptance of Terms or privacy policy would not be treated as that sale authorization.

## 8. Retention

We retain Consumer Health Data only as long as reasonably necessary for the purpose for which it was collected:

- 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 remains until the diner deletes it or deletes the account;
- an optional saved allergy or dietary profile remains until the diner changes it, withdraws the storage choice, or deletes the account;
- an unused web-form submission session expires five minutes after opening; limited consumed-session and security information may remain briefly to prevent replay, and a temporary response-download authorization expires after 30 minutes;
- consent records and limited security or audit records may remain as needed to demonstrate compliance, prevent fraud, investigate incidents, resolve disputes, or comply with law, with relevant security logs generally retained up to 24 months unless a longer period is reasonably necessary; and
- deidentified or aggregate information may be retained without time limit if we maintain it in deidentified form and do not attempt to reidentify it.

Verified diner account deletion begins immediately after successful reauthentication. Diner-owned Consumer Health Data is deleted, while a restaurant-facing submission remains on its original 90-day schedule unless an earlier verified deletion right applies. Isolated backups may retain a copy until ordinary rotation, subject to access restriction and no new use.

## 9. Your Consumer Health Data rights

Subject to verification, exceptions, and applicable law, you may request to:

- confirm whether we collect, share, or Sell your Consumer Health Data;
- access the Consumer Health Data we maintain about you, including a portable copy where required;
- receive a list of third parties and affiliates with which your Consumer Health Data was shared, where required;
- delete your Consumer Health Data, including data held by processors and, where required, notification to third-party recipients of the deletion request;
- withdraw consent for future collection or sharing;
- correct inaccurate Consumer Health Data where the applicable law provides that right; and
- appeal our refusal to act on a request.

To exercise a right, email privacy@serveguardapp.com with the subject "Consumer Health Data Request." Include your name, account email if applicable, the restaurant or event and approximate submission date if known, your state of residence, and the right you want to exercise. Do not email detailed medical information unless needed to locate the record. You may also use available in-app profile and account-deletion controls.

We will use commercially reasonable methods to authenticate your request. Depending on the request, this may include signed-in account confirmation, email or authentication-provider verification, phone verification, a response identifier, restaurant and date details, or another method proportionate to the sensitivity of the data. If you submitted without an account and we cannot reasonably link the request to a record without collecting disproportionate additional data, we will explain the limitation and available options.

An authorized agent may submit a request where permitted. We may require proof of authorization and direct verification with you. A parent or legal guardian may submit a request concerning a child or supervised teenager after we verify authority.

We will respond within the period required by applicable law. We may deny or limit a request when we cannot authenticate it, an exception applies, deletion would adversely affect another person's rights, or retention is reasonably necessary for security, fraud prevention, legal obligations, or claims. We will explain the reason and how to appeal.

## 10. Appeals

To appeal a denied or limited request, email privacy@serveguardapp.com with the subject "Consumer Health Data Appeal" within 45 days after our decision. Identify the original request and explain why you believe the decision should be reconsidered. A person not responsible for the initial decision will review the appeal where practicable. We will respond within the time required by applicable law and, when required, provide information about contacting the Washington Attorney General, Nevada Attorney General, or another appropriate regulator.

## 11. Security

We maintain administrative, technical, and physical safeguards designed for the sensitivity of Consumer Health Data, including provider-managed encryption in transit and at rest, authentication and session controls, role-based and least-privilege access, separation of allergy content from diner identifiers in restaurant workflows, application integrity controls, input validation, logging, secure development practices, retention controls, incident response, and service-provider restrictions.

No safeguard guarantees absolute security. Protect your device, sign-in method, downloaded records, response identifiers, and communications. Report suspected unauthorized access or QR tampering to support@serveguardapp.com. If a breach affects Consumer Health Data, we will provide notices required by applicable consumer health-data, general breach-notification, and, when applicable, federal health-breach law.

## 12. Children and supervised teenagers

A child under 13 may not create an account or submit Consumer Health Data directly. A parent or legal guardian may use the Diner Service in the adult's own name for the child and must provide the required consents. Users ages 13 through 17 may use the Diner Service only with parent or legal guardian supervision and permission. Contact privacy@serveguardapp.com if information was submitted contrary to this rule.

## 13. Changes to this policy

We may update this policy for legal, security, operational, or product reasons. We will post the revised policy and effective date and provide additional notice when required. We will not materially expand the collection, use, Sale, or sharing of previously collected Consumer Health Data without obtaining the consent or authorization required by law.

## 14. Contact

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

Consumer Health Data requests and appeals: privacy@serveguardapp.com Support and security reports: support@serveguardapp.com Legal notices: legal@serveguardapp.com