SERVEGUARD

ServeGuard Data Processing Addendum

Effective date: August 15, 2026

This Data Processing Addendum ("DPA") forms part of the agreement between ServeGuard LLC, a Delaware limited liability company ("ServeGuard"), and the restaurant, caterer, or other food-service customer identified in an Order Form or account ("Customer") for the ServeGuard Restaurant Service (the "Agreement"). It applies when ServeGuard processes Personal Data on Customer's behalf.

By accepting the Agreement, signing an Order Form that incorporates this DPA, or continuing to use the Restaurant Service after this DPA becomes effective, each party agrees to this DPA. If this DPA conflicts with the Agreement concerning Processing of Personal Data, this DPA controls. Capitalized terms not defined here have the meanings in the Agreement or applicable Data Protection Law.

1. Definitions

1. "Consumer Health Data" means Personal Data that identifies or is reasonably linkable to a consumer and identifies the consumer's past, present, or future physical or mental health status, and analogous regulated health data under applicable law.
2. "Data Protection Law" means privacy, data-protection, security, breach-notification, and consumer health-data laws applicable to a party's Processing under the Agreement, including applicable provisions of the California Consumer Privacy Act as amended ("CCPA"), other United States comprehensive state privacy laws, Washington's My Health My Data Act, and Nevada consumer health-data law.
3. "Personal Data" means information Processed by ServeGuard on Customer's behalf that is defined as personal data, personal information, or analogous protected information under Data Protection Law.
4. "Process," "Processing," "Controller," "Processor," "Business," "Service Provider," "Consumer," and "Sale" have the meanings given by applicable Data Protection Law.
5. "Security Incident" means a confirmed breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Personal Data in ServeGuard's possession or control. It does not include unsuccessful attempts that do not compromise Customer Personal Data, such as blocked probes, pings, scans, or login attempts.
6. "Subprocessor" means a third party engaged by ServeGuard to Process Customer Personal Data on Customer's behalf.

2. Scope, roles, and instructions

1. Customer is the Controller or Business, and ServeGuard is the Processor or Service Provider, for Customer Personal Data, except when ServeGuard independently determines the purposes and means of Processing for account security, fraud prevention, billing administration, legal compliance, or its internal business operations.
2. Customer appoints ServeGuard to Process Customer Personal Data only to provide, secure, maintain, and support the Restaurant Service; follow Customer's documented instructions; comply with the Agreement; and comply with law. The Agreement, Customer's configuration and authorized use of the Restaurant Service, and written support instructions constitute documented instructions.
3. ServeGuard will inform Customer if it reasonably believes an instruction violates Data Protection Law, unless prohibited by law, and may suspend the affected Processing until the parties resolve the issue. ServeGuard is not required to perform legal analysis on Customer's behalf.

4. Customer is responsible for the lawfulness, fairness, accuracy, quality, and necessity of Customer Personal Data and instructions; providing notices; obtaining required consents; honoring consumer choices; maintaining a lawful basis; and using the Restaurant Service consistently with Data Protection Law and the Agreement.
5. Customer will not instruct ServeGuard to collect or use more Personal Data than reasonably necessary, to sell or share Personal Data for cross-context behavioral advertising, to discriminate unlawfully, or to use identifiable Consumer Health Data for advertising, data brokerage, or general-purpose AI-model training.

3. Processing details

Subject matter and purpose

Provision of restaurant account administration, business and location management, QR and diner check-in workflows, allergy and dietary communications, records, menus, reviews, training support, notifications, security, customer support, and related functionality described in the Agreement.

Duration

For the term of the Agreement and the limited retention and deletion periods stated in the Agreement, this DPA, and applicable law.

Nature of Processing

Collection, receipt, organization, structuring, hosting, storage, separation, retrieval, consultation, transmission, display, access control, support review, correction at Customer's instruction where permitted, aggregation, deidentification, restriction, deletion, and other operations necessary to provide and protect the Restaurant Service.

Categories of data subjects

Restaurant owners, managers, employees, contractors, business contacts, diners, guests of diners, catering attendees whose information is submitted, support contacts, and authorized users.

Categories of Personal Data

Names, business and account contact information, account and authentication identifiers, roles and permissions, location and operational data, staff assignments and training records, device and security data, support communications, diner allergy and dietary submissions, diner-entered notes, response identifiers, table or event context, timestamps, consent and safety acknowledgments, review display names, category ratings, calculated rating averages, and related records. Restaurant-facing reviews do not include written comments or a diner's account email.

Sensitive data

Consumer Health Data, allergy and dietary information, authentication and security data, and other information treated as sensitive under applicable law. Customer must not submit complete medical records, payment-card data, government identifiers, or other unnecessary highly sensitive data in free-text fields.

Frequency

Continuous or event-driven as Customer and its users use the Restaurant Service.

4. ServeGuard obligations

ServeGuard will:

1. Process Customer Personal Data only on documented instructions and as permitted by this DPA and Data Protection Law;
2. ensure that personnel authorized to Process Customer Personal Data are subject to confidentiality obligations and receive appropriate privacy and security guidance;

3. implement and maintain the safeguards described in Schedule 1, taking into account the nature, scope, context, and purposes of Processing and the risk to individuals;
4. not Sell Customer Personal Data, share it for cross-context behavioral advertising, retain, use, or disclose it outside the direct business relationship with Customer, or combine it with personal information received from another person or collected from ServeGuard's own consumer interaction, except as permitted for a Service Provider under applicable law;
5. not use Customer Personal Data for advertising, data brokerage, or training a general-purpose artificial-intelligence model;
6. notify Customer if ServeGuard can no longer meet an applicable obligation under this DPA and allow Customer to take reasonable steps to stop and remediate unauthorized use;
7. provide the assistance described below for rights requests, assessments, incidents, and deletion; and
8. maintain records reasonably sufficient to demonstrate compliance with this DPA.

5. Consumer Health Data

1. ServeGuard will Process Consumer Health Data only to provide the diner-requested check-in and the Restaurant Service, maintain security and integrity, comply with law, and carry out other purposes for which the required consent was obtained.
2. ServeGuard will require a separate affirmative consent for collection and a separate affirmative consent for sharing a diner submission with the applicable restaurant or caterer. Customer will not use the data beyond the disclosed purpose unless it independently obtains any additional consent required by law.
3. ServeGuard will not Sell Consumer Health Data, use geofencing to identify or track a consumer seeking health-related services, or use Consumer Health Data for unrelated advertising or profiling.
4. Customer acknowledges that it may be an independent regulated entity with respect to Consumer Health Data it receives. Customer is responsible for its own consumer health-data policy, notices, consents, safeguards, personnel access, and response to rights requests to the extent required by law.

6. Confidentiality and access

ServeGuard will limit access to Customer Personal Data to personnel and Subprocessors who need access to perform the Agreement, protect the Restaurant Service, or comply with law. ServeGuard will use role-based and least-privilege controls appropriate to the environment. Authorized support personnel may access a specific submission when reasonably necessary to fulfill a Customer-authorized support request, investigate a Security Incident, comply with law, or resolve a documented dispute. ServeGuard does not routinely inspect individual allergy submissions for unrelated purposes.

Customer will configure roles appropriately and limit exported records, screenshots, downloaded files, and other copies. Customer is responsible for security and use after Personal Data is exported from the Restaurant Service by an authorized Customer user.

7. Subprocessors

1. Customer gives ServeGuard general authorization to engage the Subprocessors identified in the current ServeGuard Subprocessor List. ServeGuard will impose written data-protection obligations appropriate to the services provided and remains responsible for each Subprocessor's performance of its obligations to the extent required by Data Protection Law.

2. ServeGuard will update the Subprocessor List before a new Subprocessor begins materially different Processing of Customer Personal Data. Customer may object on reasonable data-protection grounds by emailing privacy@serveguardapp.com within 15 days after notice. The parties will work in good faith on a commercially reasonable alternative. If none is available, ServeGuard may discontinue the affected feature or Customer may terminate the affected Service; any refund is limited to prepaid fees for the unused affected period.
3. Customer authorizes ServeGuard and its Subprocessors to Process Customer Personal Data in the United States. Customer must notify ServeGuard before using the Restaurant Service to transfer Personal Data subject to international transfer restrictions.

8. Assistance with individual rights

Taking into account the nature of Processing, ServeGuard will provide reasonable technical and organizational assistance for Customer to respond to verified requests for access, correction, deletion, portability, consent withdrawal, restriction, appeal, or disclosure information under Data Protection Law. ServeGuard may make self-service tools available. If ServeGuard receives a request relating primarily to Customer-controlled Personal Data, ServeGuard may direct the requester to Customer and notify Customer when appropriate, unless prohibited. Customer is responsible for responding and for determining whether an exception applies.

If assistance requires materially disproportionate work beyond standard functionality, the parties may agree to reasonable fees in advance, except where law prohibits charging.

9. Security Incidents

1. ServeGuard will notify Customer without undue delay after confirming a Security Incident affecting Customer Personal Data. Notification will include information reasonably available concerning the nature of the incident, categories of information and individuals affected, likely consequences, measures taken or proposed, and a contact for follow-up. Information may be provided in phases.
2. ServeGuard's notification is not an admission of fault or liability. ServeGuard may withhold information that would compromise security, violate law, or breach another person's rights, while providing information necessary for Customer's obligations.
3. ServeGuard will take reasonable steps to contain, investigate, remediate, and mitigate the Security Incident and will reasonably cooperate with Customer. Customer is responsible for notices arising from Customer's role as Controller or Business, but ServeGuard will provide assistance required by Data Protection Law.
4. Customer will notify ServeGuard promptly of suspected compromise of Customer accounts, credentials, devices, QR codes, exports, or Customer-controlled systems affecting the Restaurant Service.

10. Assessments, audits, and compliance information

ServeGuard will make available information reasonably necessary to demonstrate compliance, such as relevant summaries, questionnaires, policies, certifications, or independent assessment reports when available. No more than once annually, unless required by a regulator or following a Security Incident, Customer may request a remote audit focused on Processing under this DPA. The parties will agree in advance on scope, timing, confidentiality, security, and allocation of reasonable costs. An audit must not expose another customer's data, compromise security, disrupt operations, or require disclosure of privileged information, source code, vulnerability details, or trade secrets beyond what is reasonably necessary. ServeGuard may satisfy an audit request through a qualified independent auditor's report where appropriate.

ServeGuard will reasonably assist Customer with a data-protection or consumer health-data assessment when the Processing requires one and the information is not otherwise available. Customer remains responsible for the assessment and its decisions.

11. Return, deletion, and retention

1. During the term, Customer may access or export Customer Personal Data through available functionality. On termination or final account deletion, ServeGuard will delete or return Customer Personal Data in accordance with the Agreement and Customer's documented instructions, unless law requires retention.
2. Restaurant-facing allergy-response content and associated identifiers are scheduled for deletion 90 days after submission. Original uploaded menu-source files are scheduled for deletion no later than 30 days after upload. A restaurant account-deletion request has the recovery periods described in the Agreement. These controls apply independently of Customer's general account status.
3. ServeGuard may retain limited billing, tax, consent, security, dispute, and legal records; deidentified information; and isolated backup copies until ordinary rotation. Retained Personal Data remains protected and is not used for another purpose.
4. Customer is responsible for deleting copies it exported or stored outside the Restaurant Service.

12. CCPA and analogous state requirements

For Customer Personal Data subject to the CCPA, ServeGuard is a Service Provider and Contractor. The business purposes and services are specified in Section 3. ServeGuard will not Sell or Share Customer Personal Data, retain, use, or disclose it outside the specific business purposes and direct business relationship, or combine it except as permitted by the CCPA. ServeGuard will comply with applicable CCPA obligations, provide the same level of privacy protection required of Customer for the Processing, allow reasonable monitoring, notify Customer if it determines it can no longer comply, and permit Customer to take reasonable steps to stop and remediate unauthorized use.

The parties intend these restrictions to satisfy analogous processor, service-provider, and contractor requirements under other applicable United States state privacy laws. If a new mandatory term applies, this DPA is deemed amended to include the minimum term necessary, and the parties will document it on request.

13. Liability

Each party's liability arising from this DPA is subject to the limitations, exclusions, and indemnification provisions in the Agreement. Nothing in this DPA limits liability that cannot lawfully be limited or changes the allocation for a party's independent legal obligations.

14. Order of precedence and changes

The order of precedence is: a signed amendment expressly identifying the provision it overrides; this DPA for Personal Data Processing; an Order Form; then the Restaurant Terms of Service. ServeGuard may update this DPA when required by law or to reflect equivalent or stronger safeguards. Material reductions in protection will not apply during a current paid term without Customer's agreement unless legally required.

15. Contact

Privacy and DPA requests: privacy@serveguardapp.com

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

Schedule 1 — Security measures

ServeGuard maintains a security program appropriate to the size and nature of the Restaurant Service and the information Processed. Measures may include the following, as applicable to the relevant system:

Governance and personnel

- designated responsibility for privacy, security, and incident response;
- confidentiality obligations and access appropriate to job duties;

- security and privacy guidance for personnel with access;
- documented incident-response, retention, and vendor-management procedures; and
- periodic review of risks and safeguards.

Identity and access management

- unique user accounts and prohibition on shared credentials;
- role-based access and least-privilege administration;
- email, phone, provider, multifactor, or device verification controls where offered or required;
- session revocation, sensitive-action reauthentication, and access removal processes; and
- restricted production administrative access.

Application and infrastructure security

- encrypted HTTPS/TLS transport and provider-managed encryption at rest;
- managed cloud database, storage, authentication, and serverless infrastructure;
- application integrity or attestation controls where supported;
- input validation, authorization enforcement, rate limiting or abuse controls where appropriate;
- separation of diner identifiers from restaurant-facing allergy-response content;
- secure secrets handling and prohibition on embedding production secrets in public client code;
- vulnerability remediation and dependency update practices proportionate to risk; and
- backups or provider resilience features appropriate to system needs.

Logging, monitoring, and response

- authentication, administrative, and security-event logging;
- monitoring for errors, abuse, and suspicious activity appropriate to the service;
- incident triage, containment, investigation, remediation, and required notification; and
- retention limits and access restrictions for logs.

Data lifecycle and vendors

- 90-day automatic expiration for restaurant-facing allergy records;
- 30-day source-file retention limit for menu imports;
- account-deletion and restoration controls;
- contractual restrictions and review for Subprocessors; and
- deletion or deidentification when data is no longer reasonably necessary, subject to law.

Customer understands that safeguards evolve and that ServeGuard may replace a measure with an alternative that maintains a materially equivalent or stronger level of protection.