

Data Processing Agreement

Global FullStack Service LLC | Version 2.0 | 2026-09-22

Applies under publication and acceptance of the document

1. Parties and priority

The Business is controller of its customers' data. Global FullStack Service LLC, 304 S Jones Blvd, Ste 8900, Las Vegas, NV 89107, United States, is processor and the platform provider. This DPA forms part of the Terms of Service and prevails on personal-data processing. Contact: gfullstackservice@gmail.com.

2. Instructions and purpose

We process data only on documented instructions to answer inquiries, manage appointments, maintain records, and produce operational information for the contracted service. Instructions comprise this DPA, the contract, configuration, and authorized requests. We report instructions we consider unlawful and may suspend them. We do not use data for unrelated purposes of our own, another business, sale, or training our own or third-party AI models.

3. Processing schedule

People: customers and prospective customers of the Business. Data: names, phone numbers, language, appointments, services, prices, history, messages, transcripts if voice is contracted, consents, and technical logs. Operations: receipt, recording, consultation, use, updating, disclosure to necessary providers, retention, return, anonymization, and deletion. Unnecessary sensitive data are not requested; volunteered data remain subject to the same restrictions. Duration: contract term and authorized retention.

4. Confidentiality and security measures

Authorized staff are bound by confidentiality and access limited to their roles. Measures include separation of data by business; least-privilege operational and reporting permissions; encryption in transit to databases and third parties; restricted infrastructure access; authorization independent of AI responses; data minimization in links and reports; and deletion or anonymization of identifiers and conversation history on valid requests. We maintain risk-appropriate measures and do not materially reduce protection without notice.

5. Authorized subprocessors

Depending on enabled features: Twilio for messaging and voice (phone numbers, messages, calls); Meta/WhatsApp for accounts and messaging network (identifiers, phone numbers, messages, metadata); Google Gemini for responses (conversation and necessary context); Railway for applications and databases (platform data); Netlify for legal pages (published documents and technical access data). Not all participate in every configuration. We require appropriate written obligations and remain accountable to the Business for subprocessors.

6. Provider changes

The Business authorizes the listed providers within the necessary scope. We notify additions or replacements at least 30 days in advance. The Business may object on reasonable data-protection grounds within that period; if unresolved, either party may terminate without penalty. When a provider ceases service, it must cease processing and return or delete the relevant data.

7. Rights and assistance

We reasonably assist with access, correction, deletion, objection, restriction, portability, impact assessments, and regulatory consultations where applicable. Direct requests are routed to the Business unless law requires otherwise. We do not disclose another business's data or follow instructions without verified authority.

8. Incidents

We notify the Business without undue delay and within 48 hours of becoming aware of a breach of data processed on its behalf. Available information includes nature, approximate categories and volume, consequences, measures, and contact, with subsequent updates. The Business determines notices to individuals and authorities required in its controller role.

9. Retention and termination

Customer data, conversations, and appointments are kept during the relationship or until a valid deletion request. Appointments may be retained anonymized. Execution logs may contain phone numbers and conversations and are kept for 14 days. Consent evidence is kept during the relationship and the applicable legal period.

On termination, the Business has 30 days to request a copy in a commonly used structured format or deletion. Without instructions, data are deleted or anonymized except for disclosed legal retention. Backups retained through their cycle are restricted; deletions must be reapplied if restored. We disclose relevant timing and do not reuse them for ordinary operations.

10. Transfers and audit

Platform infrastructure is hosted in the United States; providers may process data in other countries depending on configuration. Required international safeguards are established before the relevant processing. We provide information to demonstrate compliance. The Business may audit once annually on 30 days' notice, subject to confidentiality and without affecting other businesses; it bears costs unless substantial Provider noncompliance is found. This does not limit mandatory supervisory rights.