
Data Processing Agreement

Between ShockwaveHQ ('Processor') and Client ('Controller')

Version 1.0 | Effective Date: Upon execution of Services Agreement

Section 1: Definitions

- 1.1 "**Agreement**" means this Data Processing Agreement and any annexes attached hereto.
- 1.2 "**Client**" or "**Controller**" means the entity that has entered into a Services Agreement with ShockwaveHQ for AI automation services.
- 1.3 "**Client Data**" means any data provided by or on behalf of the Client to ShockwaveHQ in connection with the Services, including configuration data, business contact information, and service preferences.
- 1.4 "**End-Customer Data**" means data relating to the Client's customers, patients, or contacts that is processed transiently by ShockwaveHQ in the course of providing the Services.
- 1.5 "**Data Protection Laws**" means all applicable data protection and privacy legislation, including the General Data Protection Regulation (EU) 2016/679 ("GDPR"), the California Consumer Privacy Act as amended by the CCPA ("CCPA"), and the Telephone Consumer Protection Act ("TCPA").
- 1.6 "**Personal Data**" has the meaning given in the GDPR, or the equivalent term under applicable Data Protection Laws.
- 1.7 "**Processing**" has the meaning given in the GDPR and includes any operation performed on Personal Data.
- 1.8 "**Services**" means the AI automation services provided by ShockwaveHQ under the Services Agreement.
- 1.9 "**Subprocessor**" means any third-party entity engaged by ShockwaveHQ to process data in connection with the Services.
- 1.10 "**Services Agreement**" means the primary service agreement between ShockwaveHQ and the Client governing the provision of AI automation services.

2. Scope of Processing

2.1 ShockwaveHQ processes data solely for the purpose of providing the Services, including but not limited to automated messaging (SMS, voice, email), appointment scheduling, lead qualification, and workflow automation.

2.2 ShockwaveHQ acts as a Processor for End-Customer Data and as a Controller for data related to the business relationship between the parties.

3. Data Processing Details

Element	Description
Categories of Data Subjects	Client's customers, patients, leads, and contacts
Types of Personal Data Processed	First name, last name, phone number, appointment date/time, service type booked
Purpose of Processing	Automated communication delivery, appointment scheduling, reminder workflows, lead qualification
Duration of Processing	For the duration of the Services Agreement, plus retention period in Section 7
Nature of Processing	Real-time, transient processing via authenticated API. End-Customer Data processed in memory and discarded upon task completion.

4. Controller Obligations

4.1 The Client shall be responsible for ensuring a lawful basis for processing, including obtaining all necessary consents from data subjects.

4.2 The Client shall be responsible for all aspects of TCPA consent management. ShockwaveHQ provides tools to assist, but the Client maintains full responsibility for compliance.

4.3 The Client shall ensure that it has the right to transfer End-Customer Data to ShockwaveHQ for processing.

5. Processor Obligations

5.1 ShockwaveHQ shall process End-Customer Data only on documented instructions from the Controller, unless required by applicable law.

5.2 ShockwaveHQ shall ensure that persons authorized to process End-Customer Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

5.3 ShockwaveHQ shall implement appropriate technical and organizational security measures as described in Section 6 to protect End-Customer Data.

5.4 ShockwaveHQ shall assist the Controller by appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of the Controller's obligation to respond to requests for exercising the data subject's rights.

5.5 ShockwaveHQ shall assist the Controller in ensuring compliance with the obligations pursuant to security, breach notification, and data protection impact assessments (DPIAs), taking into account the nature of processing and the information available to the Processor.

6. Technical and Organizational Security Measures

- 6.1 Encryption: All data transmitted between Client systems and ShockwaveHQ encrypted using TLS 1.3 with forward secrecy. No End-Customer Data stored at rest on ShockwaveHQ-controlled infrastructure.
- 6.2 Access Control: API access authenticated via OAuth 2.0 scoped tokens. Tokens expire after 1 hour. Clients may revoke API access at any time from admin panel, with disconnection effective in under 60 seconds.
- 6.3 Zero-Persistence Architecture: End-Customer Data processed in memory only. No persistent storage layer, database, or backup system retains End-Customer Data after task completion. ShockwaveHQ does not maintain shadow copies, replicas, or archival storage of End-Customer Data.
- 6.4 Infrastructure Security: Workflow automation engine (n8n) hosted on Railway with infrastructure-level security controls. Voice AI processing (Vapi) operates under its own security and data handling commitments. CRM and communication delivery (GoHighLevel) operates within client-provisioned subaccounts.
- 6.5 Monitoring: ShockwaveHQ maintains monitoring of automation systems for availability, performance, and security anomalies. Security events are logged and reviewed.
- 6.6 Personnel Security: ShockwaveHQ personnel with access to systems processing Personal Data are subject to confidentiality obligations and access only the minimum data necessary for their role.
- 6.7 SOC 2 Type II: ShockwaveHQ is currently pursuing SOC 2 Type II certification, with estimated completion in Q2 2026. Upon certification, the audit report will be available to Clients under NDA upon request.

7. Data Retention

- 7.1 End-Customer Data: Processed transiently and discarded upon task completion. No End-Customer Data is retained on ShockwaveHQ infrastructure after processing.
- 7.2 Voice Interaction Recordings: Quality assurance recordings are retained for a maximum of 30 calendar days from the date of recording, then permanently deleted. Clients may request shorter retention windows or immediate deletion at any time.
- 7.3 Client Business Data: Account configuration, billing records, and service preferences are retained for the duration of the Services Agreement and for 90 days following termination to facilitate data export and transition.
- 7.4 Post-Termination: Upon termination of the Services Agreement, ShockwaveHQ shall, at the Client's election, return or delete all Client Data within 90 days. ShockwaveHQ shall initiate deletion requests with Subprocessors in accordance with their respective retention policies. A certificate of deletion is available upon request.

8. Subprocessors

8.1 General Authorization. Client hereby grants ShockwaveHQ broad general authorization to engage Subprocessors in connection with the provision of the Services. ShockwaveHQ will provide reasonable advance written notice to Client of any intended changes concerning the addition or replacement of Subprocessors, thereby giving Client the opportunity to object to such changes.

Subprocessor	Purpose	Location	Data Processed
Railway	Infrastructure hosting for workflow engine (n8n)	United States	Transient processing; no persistent End-Customer Data
Vapi	Voice AI conversation processing	United States	Voice interaction data; 30-day QA retention
GoHighLevel	CRM, SMS/voice delivery, communication management	United States	End-Customer contact data in client subaccount (client-controlled)
Twilio	SMS and voice carrier services (via GHL/Vapi)	United States	Phone numbers, message content (carrier-standard retention)
Google Workspace	Business email and internal correspondence	United States	Business correspondence only; no End-Customer Data
Stripe	Payment processing for ShockwaveHQ services	United States	ShockwaveHQ billing data only; no End-Customer Data

8.3 Obligations of Subprocessors. ShockwaveHQ will ensure that any Subprocessor it engages is bound by data protection obligations that are substantially similar to those set forth in this Agreement, particularly regarding data security measures.

8.4 Liability. ShockwaveHQ shall remain liable to the Client for any failure by its Subprocessors to fulfill their data protection obligations under their respective agreements with ShockwaveHQ.

8.5 Objection to Subprocessors. If Client objects to the appointment of a new Subprocessor within thirty (30) days of receiving notice, the parties will engage in good faith discussions to resolve the objection. If the parties are unable to resolve the objection, Client may terminate the Agreement without penalty.

9 Data Subject Rights

- 9.1 ShockwaveHQ shall assist the Client in fulfilling its obligations to respond to data subject requests under applicable Data Protection Laws, including requests for access, rectification, erasure, restriction, portability, and objection.
- 9.2 If ShockwaveHQ receives a request directly from a data subject, ShockwaveHQ shall promptly notify the Client and shall not respond to the request without the Client's instructions, unless required by law.
- 9.3 Response Timelines:
GDPR requests: Processed within 30 days of receipt.
CCPA requests: Processed within 45 days of receipt.
- 9.4 Requests should be directed to: privacy@shockwavehq.com

10 Personal Data Breach Notification

- 10.1 ShockwaveHQ shall notify the Client without undue delay, and in any event within 72 hours, after becoming aware of a Personal Data breach affecting data processed under this Agreement.
- 10.2 Notification shall include, to the extent available: (a) A description of the nature of the breach, including categories and approximate number of data subjects and records affected; (b) The name and contact details of ShockwaveHQ's point of contact for further information; (c) A description of the likely consequences of the breach; (d) A description of the measures taken or proposed to address the breach, including measures to mitigate possible adverse effects.
- 10.3 ShockwaveHQ shall cooperate with the Client in investigating and remediating any breach and shall provide a written post-incident report within 14 days of breach resolution.
- 10.4 ShockwaveHQ shall document all breaches, including facts, effects, and remedial actions taken, regardless of whether notification to the supervisory authority or data subjects is required.

11 Data Protection Impact Assessments

- 11.1 ShockwaveHQ shall provide reasonable assistance to the Client in conducting data protection impact assessments and prior consultations with supervisory authorities, where required under Data Protection Laws, in relation to the processing of Personal Data under this Agreement.

12 International Data Transfers

- 12.1 All ShockwaveHQ Subprocessors are currently located in the United States. If End-Customer Data originates from the European Economic Area (EEA), United Kingdom, or Switzerland, ShockwaveHQ shall ensure appropriate safeguards are in place, which may include Standard Contractual Clauses (SCCs) as approved by the European Commission.
- 12.2 ShockwaveHQ shall notify the Client before making any changes to the location of data processing.

13 Audit Rights

- 13.1 ShockwaveHQ shall make available to the Client all information necessary to demonstrate compliance with this Agreement and shall allow for and contribute to audits, including inspections, conducted by the Client or an auditor mandated by the Client.
- 13.2 Audits shall be conducted with reasonable prior notice (minimum 30 days), during normal business hours, and shall not unreasonably interfere with ShockwaveHQ's operations.
- 13.3 Upon completion of SOC 2 Type II certification (estimated Q2 2026), the audit report shall serve as the primary compliance verification mechanism, supplemented by the Client's right to additional audit under this section for matters not covered by the SOC 2 report.
- 13.4 Audit costs shall be borne by the Client, unless the audit reveals a material breach by ShockwaveHQ, in which case ShockwaveHQ shall bear reasonable audit costs.

14 Term and Termination

- 14.1 This Agreement shall remain in effect for the duration of the Services Agreement and shall automatically terminate upon expiry or termination of the Services Agreement, subject to surviving obligations regarding data return, deletion, and confidentiality.
- 14.2 The obligations in Sections 7 (Data Retention), 10 (Breach Notification), and 13 (Audit Rights) shall survive termination of this Agreement for a period of 12 months or such longer period as required by applicable Data Protection Laws.

15 Limitation of Liability

- 15.1 Each party's total aggregate liability under this Agreement shall be subject to the limitation of liability provisions in the Services Agreement.
- 15.2 Nothing in this Agreement excludes or limits either party's liability for breaches of Data Protection Laws to the extent such limitation is prohibited by applicable law.

16. General Provisions

- 16.1 Governing Law:** This Agreement shall be governed by the laws of the state specified in the Services Agreement, without regard to conflict of law provisions.
- 16.2 Amendments:** This Agreement may be amended by ShockwaveHQ to reflect changes in Data Protection Laws or processing activities. Material changes shall be communicated to the Client with 30 days' notice.
- 16.3 Severability:** If any provision of this Agreement is held to be invalid or unenforceable, the remaining provisions shall continue in full force and effect.
- 16.4 Entire Agreement:** This Agreement, together with the Services Agreement, constitutes the complete agreement between the parties regarding data processing and supersedes all prior agreements on this subject.
- 16.5 Conflict:** In the event of conflict between this Agreement and the Services Agreement regarding data protection matters, this Agreement shall prevail.

17. Contact Information

Data Protection Contact:

ShockwaveHQ

Email: privacy@shockwavehq.com

Security Inquiries: security@shockwavehq.com

Web: shockwavehq.com/security

SIGNATURE BLOCK

For and on behalf of ShockwaveHQ (Processor):

Signature: _____

Name: _____

Title: _____

Date: _____

For and on behalf of Client (Controller):

Signature: _____

Name: _____

Title: _____

Date: _____