ZEGIT Tech Solutions VoIP Services

The ZEGs Corp | Zimmerman, Minnesota

HIPAA / GDPR Compliance Addendum & Data Handling Agreement

⚠ **IMPORTANT NOTICE: Provider's standard VoIP service is not certified as HIPAA-compliant or GDPR-compliant. This addendum documents the specific data handling commitments Provider makes and the obligations Customer accepts. This addendum does NOT make Provider a fully HIPAA-covered entity. Customer must consult their own legal counsel regarding HIPAA, GDPR, and other privacy law compliance for their specific use case.**

Provider (Legal Name):	The ZEGs Corp d/b/a ZEGIT Tech Solutions, a Minnesota corporation, Sherburne County, Minnesota
Customer (Legal Business Name):	
Customer Entity Type:	☐ Corporation ☐ LLC ☐ Partnership ☐ Sole Proprietorship ☐ Other: _____
Effective Date:	
Applicable Regulation(s):	☐ HIPAA ☐ GDPR ☐ State Privacy Law (specify): _____ ☐ Other: _____

This Addendum is entered into by and between The ZEGs Corp d/b/a ZEGIT Tech Solutions ("Provider") and the Customer identified above ("Customer"), and is incorporated into and subject to the Master Service Agreement ("MSA") between the Parties. In the event of a conflict between this Addendum and the MSA, this Addendum controls with respect to data privacy matters.

1. Nature of Provider's Role

Customer acknowledges that Provider functions as a telecommunications service provider, not as a healthcare provider, business associate (as defined under HIPAA), or data processor (as defined under GDPR) by virtue of the standard VoIP service alone. Provider transmits and routes voice and data communications and maintains call records (CDRs) for billing and regulatory purposes.

If Customer is a Covered Entity or Business Associate under HIPAA and wishes to transmit Protected Health Information (PHI) via Provider's VoIP network, Customer acknowledges that: (a) standard VoIP is not encrypted end-to-end; (b) call recordings stored on Provider's infrastructure may contain PHI; and (c) Customer bears primary responsibility for HIPAA compliance in their use of the service.

2. Provider's Data Handling Commitments

Provider commits to the following data handling practices:

- Call Detail Records (CDRs): CDRs will not be disclosed to any third party except as required by valid legal process (court order, subpoena, or lawful law enforcement request), regulatory requirement, or with Customer's prior written consent.
- Call Recordings: If Customer has enabled call recording, Provider will NOT access, listen to, copy, transcribe, or disseminate call recordings under any circumstances, except when compelled by a court order signed by a judge of competent jurisdiction or other lawful legal process. Provider will notify Customer of any such request to the extent permitted by law.

- Account Data: Customer account information (contact details, configuration, billing records) is maintained securely and is not sold or shared with third parties for marketing purposes.
- Employee Access: Access to Customer account data and CDRs is restricted to Provider personnel who require such access for operational or billing purposes. Provider personnel are trained on confidentiality obligations.
- Breach Notification: In the event of a data breach affecting Customer's account data or CDRs, Provider will notify Customer within 72 hours of discovery to the extent practicable.
- Retention: CDRs are retained for a minimum of 12 months for billing and regulatory purposes. Customer may request CDR exports at any time.

3. Customer's Obligations

Customer is solely responsible for:

- Ensuring their use of Provider's VoIP service complies with all applicable privacy laws, including HIPAA, GDPR, state wiretapping laws, and two-party consent recording laws.
- Obtaining all required consents from call participants before enabling call recording, transcription, or CNAM lookup features.
- Implementing appropriate technical and administrative safeguards on their own PBX, IP phones, and network equipment to protect PHI or personal data transmitted via VoIP.
- Not transmitting PHI via unencrypted channels unless they have independently assessed and accepted the risk.
- Notifying Provider immediately if they become aware of any unauthorized access to their account or VoIP credentials.
- Ensuring their GDPR-required Data Processing Agreement (DPA) obligations are met through their own legal counsel — Provider does not execute DPAs as a standard offering.

4. Call Recording — Consent Laws

Federal law (18 U.S.C. § 2511) and many state laws regulate the recording of telephone calls. Customer is solely responsible for compliance with all applicable recording consent laws:

- One-Party Consent States: Federal law and many states require only one party to a call to consent to recording. If Customer is recording their own calls, this is generally sufficient in one-party states.
- Two-Party / All-Party Consent States: The following states (among others) require ALL parties to consent to call recording: California, Connecticut, Florida, Illinois, Maryland, Massachusetts, Michigan, Montana, Nevada, New Hampshire, Oregon, Pennsylvania, and Washington. Customer operating in or calling into these states must obtain consent from all parties.
- International: GDPR and other international frameworks impose strict requirements on recording of personal data. Customer calling internationally must comply with laws of both the originating and destination jurisdictions.

Provider recommends Customer consult legal counsel before enabling call recording features, particularly if operating in multiple states or internationally.

5. GDPR Applicability

The General Data Protection Regulation (GDPR) applies to processing of personal data of individuals in the European Union (EU) and European Economic Area (EEA), regardless of where the processing entity is located. If Customer's VoIP communications involve EU/EEA individuals (e.g., calling EU customers or employees), Customer may have GDPR obligations.

Provider's standard service is US-based and does not include GDPR data processing agreements. Customers with GDPR obligations must: (a) assess whether their use of VoIP service constitutes processing of EU personal data; (b) implement appropriate safeguards (e.g., Standard Contractual Clauses if transferring data outside EU); and (c) consult their own Data Protection Officer (DPO) or legal counsel.

6. Limitations of This Addendum

This Addendum does NOT constitute a Business Associate Agreement (BAA) under HIPAA. If Customer requires a formal BAA, additional services and security measures beyond Provider's standard offering would be required, and a separate negotiated BAA must be executed. Contact Provider to discuss availability and cost.

Provider makes no warranty that its standard VoIP service meets the technical safeguard requirements of the HIPAA Security Rule (45 CFR Part 164). Customer is responsible for their own HIPAA Security Rule compliance.

This Addendum does not create a data processing agreement (DPA) under GDPR Article 28. If Customer requires a formal GDPR DPA, contact Provider to discuss availability.

7. Legal Requests for Data

If Provider receives a subpoena, court order, or other lawful legal request for Customer data, CDRs, or call recordings, Provider will:

- Review the request for facial legal validity before complying.
- Notify Customer as soon as practicable, unless legally prohibited from doing so (e.g., by a gag order accompanying the legal process).
- Provide only the data specifically required by the legal process, and no more.
- Cooperate with Customer's legal counsel to contest or narrow overly broad requests, where feasible.

Customer acknowledges that Provider is legally required to comply with valid court orders and law enforcement requests and that compliance with such requests does not constitute a breach of this Agreement.

8. Governing Law

This Addendum is governed by the laws of the State of Minnesota. Any disputes shall be resolved in Sherburne County, Minnesota courts. Federal privacy law (HIPAA, ECPA, CALEA) supersedes state law where applicable.

9. Term & Termination

This Addendum remains in effect for the duration of the MSA. Upon termination of the MSA, Provider will retain CDRs as required by law or regulatory obligation and will destroy or return other Customer data upon written request, subject to legal hold obligations.

10. Acknowledgment

By signing below, both Parties acknowledge that they have read, understood, and agreed to the terms of this HIPAA/GDPR Compliance Addendum, and that Customer has had the opportunity to consult with legal counsel regarding their specific privacy law obligations.

Customer / Authorized Signer Signature	*Date*
Printed Full Name	*Title / Role*

Provider Representative Signature — The ZEGs Corp d/b/a ZEGIT Tech Solutions	*Date*
Printed Full Name	*Title / Role*

ZEGIT Tech Solutions VoIP Services — zegittech.cloud — 1-833-493-4832