Zowie Data Processing Agreement

concluded between

Customer (hereinafter referred to as: „Controller")

and

Zowie (hereinafter referred to as: „Processor")

hereinafter jointly referred to as „Parties"

1. this agreement (hereinafter: „DPA") is an integral part of the agreement between the Customer and Zowie governing the Customer's access to and use of the Services, including any applicable order form, statement of work, or other agreement incorporating this DPA (the "Agreement");
2. DPA specifies the rules for the processing of personal data of people using Zowie's services ("Services") and for whom the Customer acts as the controller of the personal data;
3. Zowie is an entity that processes personal data of those people collected as part of the provision of Services on behalf of the Customer;
4. DPA regulates the principles of processing personal data by Zowie on behalf of the Customer in such a way that they comply with the provisions of the data protection laws, including GDPR (that is Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data - General Data Protection Regulation);

5. terms used in this DPA, which are capitalized and are not defined in this DPA, have the meaning specified in the Agreement;
6. in the event of a conflict between this DPA and the Agreement with respect to the processing of personal data, this DPA will prevail to the extent of the conflict.

1. General Provisions

1. Controller entrusts Processor with the processing of personal data described in the Agreement, on the terms and for the purpose specified in the DPA and Agreement.
2. The processing of personal data is entrusted to the Processor for the duration of the Agreement and for the additional period referred to in section 3.
3. In the event of termination of the Agreement, DPA remains in force and expires after the data collected by Processor regarding the use of the Services (Customer Materials) is deleted, on the terms described in the Agreement.
4. Processor processes personal data only in accordance with the Controller's documented instructions. DPA and its annexes constitute such documented processing instructions.
5. To ensure compliance with the requirements of GDPR, Processor participates in the EU-U.S. Data Privacy Framework (DPF), the Swiss-U.S. DPF, and the UK Extension to the EU-U.S. DPF. Processor adheres to the DPF Principles concerning the transfer of personal data from the European Economic Area (EEA), Switzerland, and UK to the United States under the DPF. To the extent applicable to a transfer, Processor may rely on its participation in the EU-U.S. DPF, the UK Extension to the EU-U.S. DPF, or the Swiss-U.S. DPF as a lawful transfer mechanism.

2. Nature and Purpose of Processing

1. Processor will process personal data as necessary to provide, operate, maintain, secure, and support the Services in accordance with the Agreement, this DPA, and Controller's documented instructions. Processor will not process personal data for any other purpose except as required by applicable law.

3. Type of Data and Categories of Persons

1. The entrusting of processing applies to all personal data collected from individuals in connection with their use of the Services. The categories of personal data processed under this DPA may include, depending on Controller's use of the Services: names, business contact details, account and company information, email and message content, calendar and meeting information, audio and video recordings, transcripts, call metadata, and other personal data submitted to or generated through the Services by or on behalf of Controller.
2. Data subjects may include Controller's Authorized Users, customers, prospective customers, contacts, meeting participants, and other individuals whose personal data is submitted to or processed through the Services by or on behalf of Controller.

4. Rights and Obligations of Processor

1. Processor undertakes to implement DPA with the utmost care and in accordance with the data protection laws binding the Parties.
2. Processor:

a. may transfer personal data outside the EEA, including to the United States, in connection with the provision of the Services;
b. may engage Subprocessors that process personal data outside the EEA. Where such processing constitutes a restricted transfer under applicable data protection laws, Processor will ensure that an appropriate transfer mechanism is in place, including, as applicable, an adequacy decision of the European Commission, the EU-U.S. Data Privacy Framework, or the Standard Contractual Clauses adopted by the European Commission;
c. will inform Controller if Processor is required by applicable law to transfer or otherwise process personal data outside Controller's documented instructions before the relevant processing, unless applicable law prohibits such notice on important grounds of public interest;
d. will ensure that persons authorized to process personal data in connection with the implementation of DPA shall be obliged to maintain confidentiality;
e. will implement and maintain appropriate technical and organizational measures designed to ensure a level of security appropriate to the risk, in accordance with Article 32 GDPR and, where applicable, the security measures described in the Agreement;
f. will engage Subprocessors only in accordance with section 7 of this DPA.

3. If Processor has doubts as to the legality of the instruction given to it by Controller, then Processor shall immediately inform Controller about the doubts raised.

4. Processor will maintain records of the categories of processing activities carried out on behalf of Controller to the extent required by Article 30(2) GDPR.

5. Controller's Rights and Obligations

1. Controller is responsible for ensuring that it has a valid legal basis and all necessary rights, notices, consents, and authorizations required to provide personal data to Processor and to instruct Processor to process such Personal Data in accordance with the Agreement and this DPA.
2. Controller undertakes to cooperate with Processor to the extent that it is necessary for the implementation of DPA and compliance with the provisions of the GDPR.
3. If Processor informs Controller that, in Processor's reasonable opinion, a documented instruction may infringe applicable data protection laws, Controller will provide such clarification or revised instructions as are reasonably necessary to address the issue.

6. Controller and Processor's Cooperation

1. Controller and Processor will cooperate to the extent that it is necessary to comply with the provisions of the GDPR.
2. Taking into account the nature of the processing, Processor will assist Controller, by appropriate technical and organizational measures, insofar as this is possible, in fulfilling Controller's obligation to respond to requests from data subjects exercising their rights under applicable data protection laws.
3. Taking into account the nature of the processing and the information available to Processor, Processor will provide reasonable assistance to Controller in

fulfilling Controller's obligations under Articles 32-36 GDPR, including with respect to security of processing, personal data breaches, data protection impact assessments, and prior consultation with supervisory authorities.

4. Controller will reimburse Processor's reasonable costs for assistance that requires material effort beyond the ordinary operation of the Services or Processor's obligations under the applicable data protection laws, unless the assistance is required because Processor breached this DPA.
5. Processor will make available to Controller all information reasonably necessary to demonstrate its compliance with the obligations set out in the DPA and art. 28 of GDPR.

7. Subprocessing

1. Controller grants Processor general authorization to engage Subprocessors to process Personal Data on behalf of Controller in connection with the Services. "Subprocessor" means any third party, including an affiliate of Processor, engaged by Processor to process personal data on behalf of Controller in connection with the Services.
2. The list of current Subprocessors used by the Processor constitutes an appendix to this DPA.
3. Processor will enter into a written agreement with each Subprocessor imposing data protection obligations that are no less protective, in all material respects, than those imposed on Processor under this DPA, to the extent applicable to the services provided by that Subprocessor. Processor remains responsible for the performance of its Subprocessors to the extent required by applicable data protection laws.

4. Processor will provide Controller with at least seven (7) days' prior notice of any intended addition or replacement of a Subprocessor, thereby giving Controller an opportunity to object to the change on reasonable data protection grounds. If Controller objects within the notice period, the Parties will cooperate in good faith to address the objection. If the Parties cannot resolve the objection within a reasonable period, Controller may terminate the affected portion of the Services to the extent the use of the relevant Subprocessor is necessary to provide those Services. No amendment to this DPA is required solely because Processor adds or replaces a Subprocessor in accordance with this Section 7.

8. Data Security

1. Processor declares that the processing of the entrusted data takes place in accordance with appropriate technical and organizational measures, in particular those indicated in art. 32 of GDPR.
2. Processor, taking into account the nature, scope, context, purposes of processing and the risk of violation of the rights or freedoms of data subjects, has implemented the necessary measures to ensure the security of personal data being processed.
3. Processor ensures that the level of security is appropriate and takes into account, in particular, the risk associated with the processing, including the risk resulting from accidental or unlawful destruction, loss, modification, unauthorized disclosure or unauthorized access to personal data transmitted, stored or otherwise processed.

9. Procedure in the Event of Breach

1. Processor will notify Controller without undue delay after becoming aware of a Personal Data Breach affecting personal data processed under this DPA. “Personal Data Breach” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed under this DPA. For clarity, a Personal Data Breach does not include unsuccessful attempts or activities that do not compromise the confidentiality, integrity, or availability of personal data, including unsuccessful login attempts, pings, port scans, blocked or unsuccessful denial-of-service attacks, or other unsuccessful network attacks.
2. To the extent reasonably available to Processor, such notification will include information regarding the nature of the Personal Data Breach, the categories and approximate number of affected data subjects and personal data records, the likely consequences of the Personal Data Breach, and the measures taken or proposed to address and mitigate its effects. Processor may provide this information in phases as additional information becomes available.
3. Processor will provide Controller with reasonable assistance and cooperation in connection with Controller’s investigation, assessment, and any notification or communication obligations arising from the Personal Data Breach under the applicable data protection laws.

10. Liability of Parties

Each Party’s liability arising out of or relating to this DPA will be subject to the exclusions and limitations of liability set out in the Agreement, except to the extent such exclusions or limitations are prohibited by applicable data protection laws.

11. Data Deletion

Upon termination or expiration of the Agreement, Processor will, at Controller's choice, delete or return personal data processed on behalf of Controller, in accordance with the data return and deletion procedures set out in the Agreement, and will delete existing copies of such personal data, unless applicable law requires continued storage.

Notwithstanding the foregoing, Processor may retain personal data in backups, disaster-recovery systems, audit logs, security records, or pursuant to a legal hold until such personal data is deleted in accordance with Processor's ordinary retention cycles, provided that Processor continues to protect such personal data in accordance with this DPA and does not further process it except as required by applicable law or for the purposes for which it is retained.

Appendix: List of Subprocessors

Subprocessor	Purpose	Location
Google Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland	Hosting, Backups, LLM provider, TTS, ASR, Gmail and Google Calendar integrations where applicable	EEA / United States, as applicable
AWS Amazon Web Services, Inc., 410 Terry Avenue North, Seattle, WA 98109-5210, USA	Hosting, Backups, LLM provider	United States / applicable AWS region

Cloudflare Cloudflare Inc., 101 Townsend St., San Francisco, CA 94107, USA	Content Delivery Network, traffic routing, security and DDoS Protection	Global, including United States
Zowie Europe Zowie Europe sp. z o.o., Marszałkowska 107, 00-110 Warszawa, Poland	Customer support, helpdesk, product development, and hosting support	Poland / EEA
OpenAI OpenAI Ireland Limited, 1st Floor, The Liffey Trust Centre, 117-126 Sheriff Street Upper, Dublin 1, D01 YC43, Ireland	LLM processing where selected	EEA / United States, as applicable
Livekit Livekit Inc., 4285 Payne Avenue #9154, San Jose, CA 95157, USA	Real-time communications and voice infrastructure, including voice activity detection where enabled	United States
ElevenLabs Eleven Labs Inc., 169 Madison Ave #2484, New York, NY 10016, USA	Text-to-speech processing where selected	United States
Anthropic Anthropic Ireland, 6th Floor, South Bank House, Barrow Street, Dublin 4, D04 TR29, Ireland	LLM processing where selected	EEA / United States, as applicable

AssemblyAI Assembly AI Inc., 2261 Market Street #4577, San Francisco, California 94114, USA	Audio transcription, transcript generation, and speaker identification where selected	United States
Azure Microsoft Ireland Operations Limited, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, Ireland	Text-to-speech and applicable voice-processing services where selected	EEA / other configured regions
Sendgrid; Twilio Twilio Inc., 101 Spear Street, 5th Floor, San Francisco CA 94105, USA	Email delivery, telephony, SMS, call routing, call recording, and call metadata processing	United States
360Dialog 360dialog GmbH, Torstraße 61, 10119 Berlin, Germany	WhatsApp channel infrastructure	Germany / EEA
Clickhouse ClickHouse Inc., 601 Marshall St, Redwood City, CA 94063, USA	Analytics functionality where enabled	United States / configured hosting region
Vercel Vercel Inc., 440 N Barranca Ave #4133, Covina, CA 91723, United States	Hosting and operation of the CRM, including application traffic, server-side processing, logging, and deployment infrastructure	United States

Neon Neon Inc., 209 Orange Street, Wilmington, Delaware 19801, United States	Database hosting and persistent storage for CRM	United States
Recall.ai Hyperdoc Inc., 2261 Market Street #4339, San Francisco, CA 94114, United States	Meeting recording, transcription, and conversation-intelligence infrastructure	United States
FullEnrich FullEnrich Corp, 28 Geary St, STE 650, Suite #346, San Francisco, CA 94108, United States	Business-contact enrichment and work-email discovery	United States
Bouncer Bouncer Sp. z o.o., ul. Cypriana Kamila Norwida 24/1, 50-374 Wrocław, Poland	Email-address verification and deliverability services	Poland / EEA
Slack Slack Technologies Limited, Salesforce Tower, 60 R801, North Dock, Dublin, Ireland	Delivery of CRM notifications and collaboration messages in connection with the Services	Ireland / EEA; other processing locations as applicable