DATA PROCESSING AGREEMENT
within the meaning of Art 28 GDPR
(hereinafter the "**DPA"**)

Status: April 21, 2026

1. Scope of application

1.1 Kickscale GmbH with the address Stella-Klein-Löw-Weg 8, 1020 Vienna, registered in the Commercial Register of the Commercial Court of Vienna under FN 535151 m (hereinafter "**Processor"**), performs all processing of personal data on behalf of its customer (hereinafter each the "**Controller**" and the Controller together with the Processor the "**Parties"**) on the basis of this DPA.

1.2 Within the framework of the main contract concluded between the parties for the use of the social media management software operated by Kickscale (hereinafter the "**Main Contract**"), the Processor shall carry out the processing of personal data described in Annex ./1 on behalf of the Controller (hereinafter the "**Data Processing**").

2. Place of processing

2.1 Data processing shall, as a matter of principle, take place in a Member State of the European Union (EU) or the European Economic Area (EEA). A transfer of personal data to third countries shall only take place subject to the requirements of Art. 44 et seq. GDPR. For transfers to sub-processors in third countries without an adequacy decision such as, for example, those not certified under the EU-U.S. Data Privacy Framework), the current Standard Contractual Clauses (SCC) of the EU Commission shall be concluded. In such cases, the Processor shall additionally perform a Transfer Impact Assessment (TIA) and, where necessary, implement additional technical or organisational measures to ensure an adequate level of data protection.

3 Obligations of the Processor

3.1. The Processor hereby undertakes to perform data processing exclusively on the basis of documented instructions from the Controller. The Controller shall have the right to issue supplementary instructions regarding the type, scope, and procedure of the data processing to the Processor at any time.

Instructions must be issued in text form (e.g., e-mail). The Processor shall inform the Controller immediately if it is of the opinion that an instruction violates the GDPR or other data protection provisions and shall suspend the execution of said instruction until it is confirmed or amended.
The Processor shall refrain from all acts that contradict its position as a Processor.
The use of personal data for the Processor's own purposes shall require prior written authorisation from the Controller.
Insofar as the Processor is required by the law of the Union or the Member States to which the Processor is subject to process personal data even without an instruction from the Controller, the Processor shall notify the Controller of the reason for processing and the corresponding legal

requirements in good time prior to processing, unless the relevant law prohibits such notification on grounds of important public interest.

3.2 The Processor is obliged to treat the personal data of which it becomes aware in connection with the data processing as confidential. The Processor shall impose a duty of confidentiality on all persons authorised by it to process the data, unless they are already subject to a statutory duty of confidentiality. The duty of confidentiality and non-disclosure shall continue to apply after termination of this DPA.

3.3 The Processor shall take all necessary technical and organisational measures within the meaning of Art 32 GDPR. These technical and organisational measures are data security measures and measures to ensure a level of protection appropriate to the risk with regard to the confidentiality, integrity, availability and resilience of the systems. The state of the art, the implementation costs and the nature, scope and purposes of the processing, as well as the varying likelihood and severity of the risk to the rights and freedoms of natural persons, must be taken into account. The technical and organisational measures taken by the Processor are set out in Appendix 2

3.4 The Parties agree that amendments to the technical and organisational measures may be necessary to adapt to technical and legal developments. The Processor shall coordinate with the Controller in advance regarding any material changesthat may affect the integrity, confidentiality, or availability of the personal data. Measures involving only minor technical or organisational changes that do not adversely affect the integrity, confidentiality, and availability of the personal data may be implemented by the Processor without prior coordination with the Controller. The Controller may request an up-to-date version of the technical and organisational measures implemented by the Processor at any time.

3.5 The Processor shall support the Controller with appropriate technical and organisational measures to the extent possible so that the Controller can fulfil the data subject rights under Chapter III of the GDPR within the statutory deadlines and shall provide the Controller with the necessary information for this purpose at the Controller's request, provided that the Processor has this information. If a data subject submits a request to the Processor to exercise data subject rights, the Processor is obliged to forward this to the Controller if the request relates to data processing by the Controller.

3.6 The Processor shall support the Controller in fulfilling the Controller's obligations under Art. 32 to 36 GDPR, including, but not limited to, the implementation of security measures, the reporting of data breaches and, if necessary, the preparation of a data protection impact assessment. The Processor declares in a legally binding manner that it will inform the Controller immediately if the Processor becomes aware of a personal data breach or if data from a data application provided to it has been used systematically and seriously unlawfully and the data subjects are at risk of harm. The Processor shall take technical and organisational precautions to ensure that the Controller can comply with the provisions of Art. 33 and 34 GDPR ("Data Breach Notification") in particular within the statutory period.

3.7 Upon termination of the contract, the Processor shall, at the choice of the Controller, either return or delete all documents, data, and created processing or usage results in its possession that are related to the contractual relationship. Should no instruction be issued by the Controller within three months of the end of the contract, the data shall be deleted at the latest by that time. The deletion shall be documented in an appropriate manner.

The Processor may store personal data processed in connection with the mandate beyond the termination of the contract if and insofar as the Processor is subject to a statutory obligation of

retention. In such cases, the data may only be processed for the purposes of implementing the respective statutory retention obligations. After the expiry of the retention period, the data shall be deleted immediately.

3.8 The Processor is obliged to provide the Controller with information at the Controller's request in order to demonstrate compliance with the obligations under Art 28 GDPR. The Processor shall support the Controller in audits of the data processing and grant the Controller access to the documents and technical systems necessary for auditing the data processing in accordance with point 5 of this DPA. The Processor shall inform the Controller immediately if it discovers errors or irregularities in connection with the processing of personal data.

3.9 To the extent permitted by law, the Processor shall inform the Controller of inspection activities and measures taken by the supervisory authorities, insofar as this is permitted by law and they relate to the Controller's data processing activities.

4. Sub-processors

4.1 The Controller expressly authorises the use of the services of sub-processors by the Processor in the performance of the data processing governed by this DPA. The sub-processors named in Appendix ./1 shall be deemed authorised at the time the contract is concluded.

4.2 The Processor shall inform the Controller in text form of any planned replacement of a sub-processor or any planned engagement of a new sub-processor in a timely manner, but no later than 2 weeks prior to such replacement or new engagement ("Notice"). The Controller has the right to object to the replacement or new engagement of the sub-processor in text form, stating the reasons therefor, within 2 weeks of receipt of the "Notice". The objection may be withdrawn by the Controller in text form at any time. In the event of an objection, the Processor may terminate the contractual relationship with the Controller giving at least 14 days' notice to the end of a calendar month. The Processor shall give due consideration to the interests of the Controller when determining the notice period. If no objection is made by the Controller within two weeks of receipt of the "Notice", this shall be deemed to constitute the Controller's consent to the replacement or new engagement of the sub-processor concerned.

4.3 If the Processor utilises a sub-processor, the Processor shall be obliged to conclude an agreement with the sub-processor within the meaning of Art 28 (4) GDPR. This agreement must ensure that the sub-processor enters into the same obligations that apply to the processor on the basis of this DPA. If the sub-processor does not fulfil the obligations arising from the GDPR, the Processor shall be liable to the Controller for this.

5. Control and inspection rights

5.1 The Controller has the right, in agreement with the Processor, to carry out inspections of the data processing or to have them carried out by inspectors to be appointed in individual cases. Unless otherwise indicated for urgent reasons to be documented by the Controller, inspections shall take place after reasonable advance notice and during the Processor's business hours. Insofar as the Processor provides evidence of the correct implementation of the agreed data protection obligations of this DPA, checks shall be limited to random samples.

6. Running time

The term of this ADV corresponds to the term of the main contract. The cancellation, termination, expiry or dissolution of the main contract shall automatically result in the termination of this ADV.

7. Final provisions

7.1 In the event of any conflict or inconsistency between the provisions of this DPA and the main agreement in relation to the parties' data protection obligations, the provisions of this DPA shall prevail.

7.2 Should individual provisions of this ADV be or become invalid, this shall not affect the remaining content of the ADV. The invalid provision shall be replaced by a valid provision that is legally valid and comes closest to the economic intentions of the parties. The same applies in the event of a contractual loophole.

7.3 This DPA shall be governed by Austrian law, unless the applicable data protection law provides otherwise. The place of jurisdiction for all disputes in connection with this DPA shall be determined by the main contract, unless the applicable data protection law provides otherwise.

Appendix ./1

Description of the Data Processing and Authorized Sub-processors

1. Object of data processing

Operation of a sales enablement platform that allows the customer to record, transcribe and analyse sales conversations.

2. Duration of data processing

Personal data shall be stored for the duration of the Main Contract. Upon termination of the contract, the return or erasure of data shall be governed by Section 3.6 of this Agreement.

3. Nature and purpose of data processing

Data from sales conversations shall be recorded (video and/or audio) and transcribed.

Data from sales conversations shall be automatically imported into the Sales Enablement Platform operated by the Processor via the interfaces provided by the same, and subsequently processed, displayed, and managed.

The purpose of the processing is the analysis and optimization of the Customer's sales conversations as well as the management of the extracted information by the Controller (Auftraggeber).

4. Categories of personal data

- First and last name, email addresses, profile pictures, user IDs.
- Audio and video recordings of virtual conversations and meetings, including the content of these (sales) conversations.
- Analysis results relating to the (sales) conversations.
- Where applicable, further platform content (comments, notes from sales representatives or supervisors).
- Information from connected interfaces regarding lead or customer data.

5. Categories of data subjects

Data subjects affected by the processing are:

- **End users:** The direct users of the platform who use the tools provided to organize, record, transcribe and analyse their sales conversations and meetings. The categories of personal data mentioned in point 4 are processed here.

- **Third parties:** This includes people who take part in the sales conversations and meetings conducted by our users, but who are not themselves users of our platform. The personal data processed here are email addresses, usernames on the respective meeting platform and audio and video recordings.

6. Authorised sub-processors

Receiver	Purpose	Legal basis of the Transmission	Registered office / place of data processing	Basis for Third Country Transfer
Google Cloud EMEA Limited	Hosting internal IT systems Backend and storage of recordings Database and user authentication via Firecase	Legitimate interests (Art 6(1)(f) GDPR): Use of professional IT Infrastructure	Data storage and processing in EU	No third country transfer; Participant in E.U.-U.S. Data Privacy Framework.
Hyperdoc Inc / Recall AI	Recording of online meetings	Performance of (pre-)contractual measures (Art 6(1)(b) GDPR)	Data storage and processing in EU	No third country transfer (EU data residency); In exceptional cases, transfer to the USA or access by US sub-processors cannot be fully excluded; SCCs pursuant to Art 46 GDPR have been concluded.
AssemblyAI	Transcription of sales calls	Performance of (pre-)contractual measures (Art 6(1)(b) GDPR)	Data storage and processing in EU	No third country transfer; Participant in E.U.-U.S. Data Privacy Framework.
Mailgun Technologies Inc	Emails to users regarding consent for recording.s	Performance of (pre-)contractual measures (Art 6(1)(b) GDPR)	Data storage and processing in EU	No third country transfer; Participant in E.U.-U.S. Data Privacy Framework.

Apideck bv	Integration for other platforms (especially CRM systems)	Performance of (pre-)contractual measures (Art 6(1)(b) GDPR)	EU (Belgium)	No third country transfer
Langfuse	Tracking, prompt management, and metrics for LLM debugging/improvement.	Performance of (pre-)contractual measures (Art 6(1)(b) GDPR)	EU (Germany)	No third country transfer
Gladia	Transcription of audio and video calls.	Performance of (pre-)contractual measures (Art 6(1)(b) GDPR)	EU (France)	No third country transfer
Mongo DB	Primary database for storage of recordings and application data.	Performance of (pre-)contractual measures (Art 6(1)(b) GDPR)	Data storage and processing in EU	No third country transfer; Participant in E.U.-U.S. Data Privacy Framework.
Posthog	Platform monitoring	Performance of (pre-)contractual measures (Art 6(1)(b) GDPR)	Data storage and processing in EU	No third country transfer; Participant in E.U.-U.S. Data Privacy Framework.

Appendix ./2

Technical and organisational data security measures

1. Confidentiality

The **Processor** shall ensure that the confidentiality of personal data is guaranteed at all times. In particular, the following measures are taken for this purpose:

a) Access control to data processing systems, e.g. through regulated key management, security doors or security personnel;

b) Access control to data processing systems, e.g. through passwords, automatic locking mechanisms, two-factor authentication, encryption of data carriers, virtual private networks (VPN) or logging of user logins;

c) Access control to data within the data processing system, e.g. through standard authorisation profiles on a "need to know" basis, partial access authorisations or logging of accesses;

d) Pseudonymisation of personal data;

e) Classify data as secret, confidential, internal or public;

f) Separation of data processing for different purposes, e.g. through the use of separate databases, client separation, separation of customer servers.

2. Integrity

The **Processor** shall ensure that the integrity of the personal data is guaranteed at all times. In particular, the following measures are taken for this purpose:

a) Transfer control: Protection against unauthorised reading, copying, modification or removal during data transfers, e.g. through encryption, virtual private networks (VPN), ISDN wall, content filters for incoming and outgoing data or electronic signatures as well as lockable transport containers;

b) Input control: Ensuring that it is possible to check whether and by whom personal data has been entered, changed or deleted in data processing systems, e.g. by logging, using electronic signatures, regulating access authorisations.

3. Availability and resilience

The **Processor** shall ensure that its systems are available and resilient in accordance with the industry standard or the state of the art. In particular, the following measures are taken for this purpose:

a) Availability: Protective measures to prevent the destruction or loss of personal data, e.g. through storage in safes or security cabinets, storage networks, software and hardware protection, creation of backups.

b) Resilience: Measures to ensure that systems are protected in the event of technical attacks and that capacities are available to enable smooth operation despite unforeseeable loads.

4. Procedures for regular review, assessment and evaluation

The Processor shall regularly review, assess and evaluate its technical and organisational measures. It agrees to have its security measures reviewed by the RESPONSIBLE PARTY or an expert appointed by the latter.

5. Prevention of data leaks from the AI models

The **CONTRACTOR** shall implement the following measures to prevent data leaks:

a) Use of private cloud deployments on Azure AI
b) No training on customer data by the model provider (Microsoft)
c) Logically separated workspaces (data access control in the backend)
d) Encrypted transmission of data (SSL)

6. Model training

As AI providers Google Cloud and Amazon Web Services (AWS) explicitly guarantee that they will not conduct training on customer data processed via Google Cloud Vertex AI or Amazon Bedrock, respectively. Neither input prompts nor generated responses will be used for training or improving the underlying foundation models.

Google Cloud:

- Governance & Privacy für Vertex AI: Vertex AI and zero data retention | Generative AI on Vertex AI | Google Cloud Documentation
- Cloud Data Processing Addendum (DPA): Cloud Data Processing Addendum

Amazon Web Services:

- Privacy & Responsible AI für Amazon Bedrock: Amazon Bedrock security, privacy, and responsible AI
- Data Processing Addendum (DPA): AWS DATA PROCESSING ADDENDUM

Customer	**Kickscale FlexCo**
Signature: Customer Name: First name / Last name: Title: Date:	Signature: _____ Gerald Zankl, gerald.zankl@kickscale.com CEO _____ Markus Jenul, markus.jenul@kickscale.com CMO Date: