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

Status: January 15, 2025

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 The provisions of this DPA may be amended by the Processor at any time without giving reasons, whereby such amendments shall be announced on the Processor's website and by sending the text of the contract to the last e-mail address provided by the Customer at least 30 days before they come into force. If the customer does not object to the changes in writing by e-mail to privacy@kickscale.com within 30 days of receipt of the aforementioned announcement, the changes shall be deemed accepted. In the event of a timely objection by a customer, the contractual relationship between this customer and the processor shall continue to exist in accordance with the ADV in the version prior to the announced amendment.

1.3 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 As a rule, data processing takes place in a member state of the European Union or in another state party to the Agreement on the European Economic Area. Data may however also be processed outside the European Union in countries whose level of data protection may not correspond to that of Austria. However, the Processor shall only transfer the personal data to countries which, according to the EU Commission, have an adequate level of data protection. Alternatively, the Processor shall take measures to ensure that an adequate level of data protection is guaranteed in accordance with Art 44 et seq. of the GDPR.

3 Obligations of the Processor

3.1 The Processor undertakes to carry out data processing exclusively on the basis of documented instructions from the Controller. If the Processor considers an instruction from the Controller to be unlawful, the Processor shall be authorised to suspend implementation of the relevant instruction until it is confirmed or amended by the controller. The Processor must refrain from all actions that contradict its position as Processor. The use of personal data for the Processor's own purposes requires prior written authorisation from the Controller.

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 can be found in Appendix 2.

3.4 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.

3.5 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.

3.6 The Processor shall delete the personal data of the data processing after expiry of the retention periods provided for in the main contract and/or immediately at the request of the Controller. The Processor shall be obliged to hand over all processing results and documents containing personal data to the Controller in full after completion of the service provision. The Processor shall not be authorised to retain personal data, documents or parts thereof. Exceptions to this are those records and documents that the Processor is legally obliged to retain. The Processor shall be obliged to return or destroy the data to sub-processors accordingly.

3.7 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.

3.8 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 of any intended change with regard to the involvement or replacement of a Sub-Processor. The Controller may object to the planned change in writing by e-mail to privacy@kickscale.com within 30 working days from the date of notification. In the event of a timely objection, the processor is not authorised to use the services of the rejected sub-processor in the context of data processing. If the controller does not object within the aforementioned period, the intended change shall be deemed to have been authorised by the controller. In the event that the Controller authorises the use of a sub-processor, the Processor shall ensure that the Controller is granted access to the data related to the outsourced activities and to the relevant business premises and that the use of the sub-processor does not at any time jeopardise the fulfilment of the requirements of this Agreement.

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

8.1 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.

8.2 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.

8.3 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 data processing

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

During the term of the main contract and the retention periods provided for therein.

3. Nature and purpose of data processing

The data from sales meetings is automatically imported into the sales enablement platform operated by the Processor via the interfaces provide by the Processor and subsequently processed, displayed, and managed.

The purpose of the processing is the analysis and optimization of the customer's sales meetings and the management of the extracted information by the client.

4. Categories of personal data

First and last name, email addresses, profile pictures, user IDs and audio and video recordings of virtual conversations and meetings, including the content of these (sales) conversations.

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 transmission to a Third country
Google Cloud EMEA Limited	Hosting your own IT systems Backend and storage of recordings Database and authentication of users via Firecase	legitimate interests (Art 6 para 1 lit f GDPR): IT Infrastructure	USA (data storage: EU)	No third country transfer
Hyperdoc Inc / Recall AI	Recording of online meetings	for the implementation of (pre-)contractual measures (Art para lit b GDPR)	USA (data storage: EU)	No third country transfer
AssemblyAI	Transcription of sales calls	for the implementation of (pre-)contractual measures (Art para lit b GDPR	USA (data storage: EU)	No third country transfer
Microsoft Ireland Operations, Ltd.	Processing the transcripts	for the implementation of (pre-)contractual measures (Art para lit b GDPR)	EU (Ireland)	No third country transfer
Mailgun Technologies Inc	Marketing activities and product release notes	for the performance of (pre-)contractual measures (Art. 6 (1) (b) GDPR) and on the basis of legitimate interests (Art. 6 (1) (f) GDPR): Utilisation professional IT Infrastructure	USA (data storage: EU)	No third country transfer
Apideck bv	Integration for other platforms (especially CRM systems)	for the implementation of (pre-)contractual measures (Art para lit b GDPR)	EU (Belgium)	No third country transfer

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 an AI provider, Microsoft explicitly guarantees that it will not carry out any training on data processed via Azure AI Services (see https://learn.microsoft.com/en-us/legal/cognitive-services/openai/data-privacy?tabs=azure-portal and the DPA from Microsoft https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA)