

Annex 6 – Taskbase Data Processing Agreement (DPA)

Version: 10.9.2026

This Annex 6 describes the data processing carried out by Taskbase under the data processing agreement (DPA) within the scope of the contract for the Sales Coach.

Information on Taskbase

Taskbase contact details (responsible recipient of instructions):

Taskbase AG, Samuel Portmann, CEO, Zahnradstrasse 22, 8005 Zurich, Switzerland

Email: samuel@taskbase.com

Contact details of the contact point at Taskbase responsible for data protection issues (also Data Protection Consultant or Data Privacy Contact Point):

Taskbase AG, Samuel Portmann, CEO, Zahnradstrasse 22, 8005 Zurich, Switzerland

Email: privacy@taskbase.com

Contact details of Taskbase's data protection representative in the European Union, who can be contacted by supervisory authorities and data subjects for all questions relating to EU data protection law:

Jetro Capiaghi, Hammerweg 8, 83022 Rosenheim, Germany

Email: jetro@taskbase.com

Data Processing

General

Within the scope of the contract, the customer entrusts Taskbase with confidential data for processing, at its own discretion and on its behalf. The customer acts as Controller and Taskbase as Processor.

1.1 Purpose of Processing

Taskbase processes the personal data entrusted to it by the customer only for the purposes set out below. By entering into this DPA, the customer instructs Taskbase to carry out the processing described in each of them:

(a) Provision of the Services.

Delivering, operating, maintaining and supporting the Sales Coach product, including the capture and transcription of business conversations where configured by the customer, and the generation of coaching content, learning progress, development feedback as well as user-configured sales

productivity outputs that support the customer's users in their day-to-day work, such as call prioritisation lists, daily activity summaries and pre-meeting briefings.

(b) Configuration and tailoring for the customer.

Configuring, adapting and improving the Services for the customer, including the adaptation of coaching skills, playbooks, prompts and evaluation logic to the customer's own context, and the review of processing results by authorised Taskbase personnel for that purpose.

(c) Integrity, security and support.

Securing the Services, diagnosing and remedying faults and errors, investigating security incidents, and maintaining availability.

(d) Administration of the contractual relationship.

Customer relationship management, invoicing and archiving.

1.2 Instructions

(a) Taskbase processes personal data only on documented instructions from the Controller, unless there is an obligation to process under Swiss law or Union law. In such a case, Taskbase shall inform the customer of these legal requirements prior to processing, unless the relevant law prohibits this due to an important public interest. The customer may issue further instructions throughout the duration of the processing of personal data. These instructions must always be documented.

(b) Taskbase shall inform the customer without delay if it is of the opinion that instructions issued by the customer violate applicable data protection provisions.

1.3 Duration of Processing

Processing runs for the duration of the contract.

Personal data will be handled by Taskbase as follows after the end of the contract:

Live customer data is deleted within 30 days of termination. Backup data containing customer information is expired after at most 65 days after termination. Log information is kept for up to 12 months for forensic purposes.

Transfer of data to the customer before deletion of live data upon request of the customer.

Deletion will take place unless there are longer statutory retention obligations or legitimate interests in relation to certain personal data.

1.4 Categories of Data Subjects

Taskbase processes personal data of:

- ☒ Internal or external employees/auxiliary personnel of the customer
- ☒ End customers of the customer
- ☒ Internal or external employees/auxiliary personnel of the customer's business clients
- ☐ End customers of the customer's business clients
- ☐ Internal or external employees/auxiliary personnel of the customer's suppliers/partners

1.5 Categories of Personal Data

Taskbase processes the following categories of personal data:

- ☒ Private and professional contact and identification data as well as (work) organization data (Name, first name, email address)
- ☒ Data on personal/professional circumstances and characteristics (job title, professional career, company affiliation, tasks, activities, coaching content)
- ☒ Image and/or sound recordings (e.g. audio, video, photos) of business meetings.
- ☒ Contract data (e.g. purchased products, (financial) services, date of purchase contract, purchase price, special equipment, guarantees, etc.)
- ☒ IT usage data (User ID)
- ☐ Payroll and time management data (e.g. payroll, special payments, garnishment, daily attendance times, reasons for absence, etc.)
- ☐ Creditworthiness and bank data (e.g. IBAN, card number, payment behavior, balance sheets, data from credit agencies, score values, financial circumstances, bank account, credit card number, etc.)
- ☐ Particularly sensitive personal data (e.g. racial and ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the unique identification of a natural person, social assistance measures, health data or data on sexual life or sexual orientation, and data relating to criminal offences or the suspicion thereof)

Taskbase does not intentionally process special categories, the customer must not instruct it to, unstructured content may incidentally contain such data, and no special-category attributes are derived from it.

1.6 Special Statutory Confidentiality Obligations

- ☐ Taskbase processes personal data as an auxiliary person of the customer which is additionally subject to a special statutory confidentiality obligation:

(Multiple selection possible)

- ☐ Official secrecy
- ☐ Banking secrecy
- ☐ Professional secrecy (e.g. trustees, tax experts, lawyers)
- ☐ Telecommunications secrecy
- ☐ Federal Act on the General Part of Social Security Law (ATSG)
- ☒ Taskbase, as an auxiliary person of the customer, does not process any personal data which is subject to a special statutory confidentiality obligation.

1.7 Confidentiality of Authorised Personnel

Taskbase grants access to the personal data processed on behalf of the customer only to those employees and other persons acting under its authority who require such access in order to carry out the purposes set out in section 1.1. Taskbase ensures that these persons are bound by a contractual or statutory obligation of confidentiality which continues to apply after the end of their engagement, that they are instructed in the lawful handling of personal data, and that they process the personal data only on the instructions of Taskbase and within the scope of this DPA.

Location of Data Processing

2.1 Location of personal data processing

The personal data is processed in the EU/EEA and Switzerland. All processing countries are listed in Annex 8 (Sub-Processors).

2.2 Guarantees for Subprocessors outside the EU/EEA

Taskbase ensures an adequate level of protection for personal data when processing is performed in the EU/CH by an entity located outside EU/CH by concluding data processing agreements with the relevant sub-processors, in which these sub-processors are obliged to take sufficient technical and organizational measures to protect the processed personal data and/or to ensure data security appropriate to the risk, and which contain the EU Standard Contractual Clauses (SCC) or are adequate according to the EU commission.

2.3 Disclosure of Personal Data to Sub-processors

The third parties listed in Annex 8 (Sub-processors) have access to and process personal data as sub-processors, or personal data is disclosed to these third parties.

Taskbase shall explicitly inform the customer at least 14 days in advance of intended changes to this list by adding or replacing sub-processors, thereby giving the customer sufficient time to raise objections to these changes before commissioning the relevant sub-processor(s).

Taskbase ensures that the sub-processor fulfills the obligations to which Taskbase is subject in accordance with these clauses, the Swiss Data Protection Act (nDSG), and Regulation (EU) 2016/679 (EU GDPR).

Assistance to the Controller

(a) Taskbase shall provide the customer with all information necessary to demonstrate compliance with the obligations set out in these clauses and arising directly from the Swiss Data Protection Act (nDSG) and/or Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725. At the customer's request, Taskbase shall also permit and contribute to audits of the processing activities falling under these clauses at reasonable intervals or where there are indications of non-compliance. When deciding on a review or audit, the customer may take into account relevant certifications of Taskbase.

(b) The customer can carry out the audit themselves or commission an independent auditor. Audits may also include inspections of Taskbase's premises or physical facilities and will be carried out with reasonable prior notice if applicable.

(c) Taking into account the nature of the processing, Taskbase shall assist the customer in fulfilling its obligation to respond to requests from data subjects to exercise their rights. Where a data subject addresses such a request directly to Taskbase, Taskbase shall not respond on its own account but

shall forward the request to the customer without undue delay.

(d) Apart from the obligation to assist the customer pursuant to clause (c), Taskbase shall also assist the customer in complying with the following obligations, taking into account the nature of the data processing and the information available to it:

(1) Obligation to carry out an assessment of the consequences of the planned processing operations for the protection of personal data (“Data Protection Impact Assessment”) if a form of processing is likely to result in a high risk to the rights and freedoms of natural persons;

(2) Obligation to consult the competent supervisory authority(ies) prior to processing if a data protection impact assessment shows that the processing would result in a high risk, unless the customer takes measures to mitigate the risk.

Notification of Data Breaches

Taskbase shall notify the customer without undue delay, and at the latest within 36 hours of becoming aware of a personal data breach involving personal data processed on behalf of the customer. This timeline is designed to ensure that the customer retains sufficient time to fulfil its own notification obligations to the competent supervisory authority within the 72-hour period prescribed by Art. 33 GDPR.

The initial notification shall be made in text form (email sufficient) to the customer’s designated contact and shall include, to the extent available at the time of notification:

- (a) a description of the nature of the breach, including the categories and approximate number of data subjects and personal data records affected;
- (b) the name and contact details of Taskbase’s data protection contact point;
- (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 its possible adverse effects.

Where all required information cannot be provided at the time of the initial notification, Taskbase shall provide it in phases without further undue delay. Taskbase shall additionally notify the customer by telephone if the breach is of a severity that warrants immediate escalation, as assessed by Taskbase in good faith.

Taskbase shall document all personal data breaches, including those not requiring notification to a supervisory authority, and make this documentation available to the customer upon request.

Where the customer is subject to the Swiss Federal Act on Data Protection (nDSG), Taskbase shall notify the customer without undue delay upon becoming aware of a data breach involving a likely high risk to the personality or fundamental rights of affected data subjects, in accordance with Art. 24 nDSG. The above notification timelines and content requirements apply correspondingly. Where both the GDPR and the nDSG apply, Taskbase shall fulfil whichever obligation is more stringent in the circumstances.

Security of Processing

3.1 Taskbase implements and maintains the technical and organisational measures set out in Annex 7 (Technical and Organisational Measures) in order to ensure a level of security appropriate to the risk, in accordance with Art. 32 GDPR and with Art. 8 nDSG together with Art. 3 of the Swiss Data

Protection Ordinance (DSV).

3.2 The measures reflect the state of the art at the time of conclusion of this DPA and are subject to technical development. Taskbase may replace individual measures with alternative or additional measures, provided that the level of protection agreed in Annex 7 is not reduced. Taskbase reviews the protection requirement of the personal data, the risk, and the effectiveness of the measures over the entire duration of the processing, in particular upon material change to the processing or to the measures and following a security incident, and adapts the measures where necessary.