

Taskbase Sales Coach

Terms of Service, DPA & TOMs

The contractual and security documentation for **Taskbase Sales Coach**: the General Terms and Conditions, the Data Processing Agreement (Annex 6), the Technical and Organizational Measures (Annex 7) and the Sub-processor list (Annex 8).

01	General Terms and Conditions of Taskbase	Version Date: 9.09.2026
02	Annex 6 – Taskbase Data Processing Agreement (DPA)	Version: 10.9.2026
03	Annex 7 – Technical and Organizational Measures (TOM)	Version: 17.9.2026
04	Annex 8 – Sub-processors	Version: 3.9.2026

Contents

General Terms and Conditions of Taskbase

1. Subject Matter
2. Taskbases' Services
3. Customer's duties of cooperation
4. Duty to provide information
5. Fees, payment and expenses
6. Default by Taskbase
7. Acceptance procedure for one-time Services
8. Warranty
9. Liability
10. Force majeure
11. Intellectual property rights
12. Confidentiality and data protection
13. Compliance with laws and regulations
14. Suspension of Services by Taskbase
15. Term, termination and effects of termination
16. Changes
17. Miscellaneous
18. Dispute resolution, applicable law and place of jurisdiction

Annex 6 – Taskbase Data Processing Agreement (DPA)

Information on Taskbase
Data Processing
General
Location of Data Processing
Assistance to the Controller
Notification of Data Breaches
Security of Processing

Annex 7 – Technical and Organizational Measures (TOM)

How to read the status column

1. Governance
2. People
3. Physical and Environmental
4. Identity and Access
5. Network and Communications
6. Systems and Applications
7. AI and Agent Processing
8. Data and Information
9. Suppliers and Third Parties
10. Operations and Resilience
11. Compliance and Audit

Mapping to statutory and legacy control categories

Annex 8 – Sub-processors

General Terms and Conditions of Taskbase

Version Date: 9.09.2026

1. Subject Matter

These General Terms and Conditions of Taskbase (“GTC”) are applicable to all services (“Services”) that Taskbase AG, Zahnradstrasse 22, 8005 Zürich, Switzerland (“Taskbase”) provides to its customers (“Customer”) (Taskbase and the Customer each individually a “Party” and jointly the “Parties”).

The Customer agrees to the application of these GTC by accepting Taskbase’s offer or by signing a service agreement or any other agreement with Taskbase in which reference is made to these GTC (such offer, service agreement or other agreement together with all further contractual documents, including these GTC, the “Service Agreement”), whereby a contract is concluded between the Parties.

The application of any general terms and conditions of the Customer is herewith expressly excluded unless stated otherwise in the Service Agreement.

2. Taskbases’ Services

Taskbase shall provide the Services in accordance with the Service Agreement (including its annexes).

Taskbase shall be free to organize the manner in which it provides the Services, unless specified otherwise in the Service Agreement. It shall however be obliged to consult with the Customer and other parties involved, as required for the applicable project.

Taskbase is entitled to engage third parties and auxiliary persons (in particular subcontractors) for the purpose of providing the Services and meeting its contractual obligations.

3. Customer’s duties of cooperation

The Customer shall, by all reasonable means, to the extent necessary, and in a timely manner, actively support Taskbase, its employees and any third parties engaged by Taskbase for the purpose of providing the Services, cooperate in taking the necessary preparatory and provisioning actions (including the procurement of all requisite rights and authorizations), provide all relevant information and grant the necessary access to its systems and resources.

In addition, the specific duties of cooperation as set out in the Service Agreement apply.

The Customer shall bear all costs incurred by it in the course of fulfilling its duties of cooperation.

Taskbase shall attempt to perform the Services even if the Customer fails to comply with its duties of cooperation as agreed upon in the Service Agreement. Should this occur, Taskbase shall inform the Customer promptly and set a reasonable grace period in order to comply with the relevant duties that the Customer has not or not been properly complied with, and Taskbase shall state the consequences that may be expected for the Customer in the event of failure to comply with the relevant duties of cooperation within the grace period. If, upon expiry of the grace period, compliance has not been restored by the Customer, Taskbase has the right to suspend the Services with immediate effect and/or to terminate the Service Agreement for cause.

In the event of non-fulfilment or improper fulfilment of the Customer's duties of cooperation, in addition to the remedies stated above, the Customer shall compensate Taskbase for the resulting additional efforts at the standard hourly rates of Taskbase as stated in the Service Agreement.

4. Duty to provide information

Each Party shall inform the other Party promptly of any circumstances, developments, incidents and findings that may be relevant for the other Party in connection with the performance of the Service Agreement or with the contractual relationship as such, unless prohibited by statutory or contractual confidentiality obligations.

5. Fees, payment and expenses

The fees for the provision of the Services are specified in the Service Agreement.

Invoices are payable net within 30 days net as of receipt. The Customer shall be in default upon expiry of the payment period without further ado. The statutory rate of default interest shall apply. If the Customer defaults on a payment, Taskbase has the right to suspend the provision of the Services until receipt of payment in full of all outstanding invoices. All fees are exclusive of value added tax (VAT) and any other taxes, duties and charges.

Unless otherwise agreed, any expenses (i.e. all necessary and reasonable out-of-pocket expenses, including, but not limited to travel, lodging, meals, and other business expenses incurred by Taskbase in the provision of the Services, all together the "Expenses") shall be borne by the Customer.

If the Customer does not agree with the prices or expenses invoiced (the "Billing Dispute"), it must notify Taskbase in text form within 10 days of receipt of the respective invoice, stating the reasons and the type and amount of the disputed prices (the "Billing Dispute Notice"). The Customer shall cooperate with Taskbase to promptly address and attempt to resolve any Billing Dispute submitted in accordance herewith. The Customer acknowledges and agrees that in the event that the Customer does not submit a Billing Dispute Notice in accordance with the foregoing, the Customer waives all rights to dispute such invoice, and all fees and Expenses set forth in such invoice will be considered correct and binding on the Customer. In case of a Billing Dispute, the Customer shall remain obligated to pay all undisputed fees and Expenses.

6. Default by Taskbase

Contractually agreed deadlines shall be deemed met upon provisioning of the relevant Services by Taskbase.

If Taskbase fails to comply with a material contractual deadline set forth in the Service Agreement (hard milestone, performance obligation with a defined deadline), Taskbase shall be in default upon expiry of a reasonable grace period set by the Customer in a written reminder (e-mail sufficient). If Taskbase fails to fulfil its performance obligation by the expiry date of this grace period, the Customer has the right to withdraw from the Service Agreement. Any Services (or parts thereof) that have already been provided substantially in accordance with the Service Agreement and that can be used by the Customer as such in an objectively reasonable manner must be paid for in full. Any withdrawal from the Service Agreement shall not affect these Services and they shall remain subject to the relevant provisions of the Service Agreement.

7. Acceptance procedure for one-time Services

7.1. General

In case the Parties agree in the Service Agreement on specific results of performance and the corresponding acceptance criteria (contract for work and services, “Werkvertrag”), then Taskbase’s duty to deliver shall be met upon the Customer’s acceptance of such work results in accordance with the acceptance criteria. The Customer shall declare acceptance in text form (e-mail sufficient). The work results shall, in the absence of any express written declaration to the contrary by the Customer, be deemed to have been accepted following operational use of the work results by the Customer during at least 30 days.

If the Parties agree to the acceptance of partial work results, the acceptance thereof shall be subject to final acceptance. Upon successful final acceptance, the warranty periods shall commence.

7.2. Failure of acceptance

Acceptance shall be deferred, if acceptance testing by the Customer identifies major defects. The Customer is obliged to provide Taskbase with evidence of any such major defects claimed by it and to reproduce them if possible. Taskbase shall rectify the defects within a reasonable time period, taking into account the cause and nature of the defect, and once again provide the relevant deliverable for acceptance by the Customer.

If the defect cannot be remedied within a time period appropriate to the cause and nature of the defect, the Customer shall set a reasonable grace period for the remedying of the defect. If the remedying definitely fails, the Customer is entitled to (a) demand an appropriate reduction of the respective fees, or (b) withdraw from the Service Agreement in the case of a substantial defect that prevents the Customer from using the deliverable in its entirety. Those Services or parts thereof which have already been provided substantially in accordance with the Service Agreement and which can be used by the Customer as such in an objectively reasonable manner must be paid in full. Any withdrawal from the Service Agreement shall not affect these Services and they shall remain subject to the relevant provisions of the Service Agreement.

Minor defects shall not entitle the Customer to refuse acceptance, but such defects must be rectified by Taskbase within a reasonable grace period set by the Customer.

8. Warranty

8.1. Recurring/operational Services

Taskbase will provide the Services in a professional and diligent manner. If a Service Level Agreement (SLA) forms part of the Service Agreement, then the relevant provisions of the SLA apply. In the absence of any agreement to the contrary in the Service Agreement (including the SLA), there are no representations or warranties as to the availability, quality, security, operation or support of the Services. The Services are provided on a “best effort” basis. In the event of failures, malfunctions and delays, Taskbase shall use its available resources in a reasonable and customary manner to provide the Services or remedy the failures or malfunctions, without, however, giving any assurances in this respect.

8.2. One-time Services

Taskbase warrants that the Services conform to the contractually agreed specifications. The warranty period is 12 months as of the date of acceptance (in accordance with section 7 of these GTC).

Defects must be stated in text form (e-mail sufficient) in a comprehensible form with evidence of the relevant defects and all information useful for identifying the defects. The Customer is obliged to reproduce the defects if possible.

In case of a defect covered by the warranty, the Customer may first demand that the defect shall be remedied free of charge. The Customer shall support Taskbase in the remedying of defects to the extent necessary. If the defect cannot be remedied within a time period appropriate to the cause and nature of the defect, the Customer shall set a reasonable grace period for the remedying of the defect. If the remedying definitely fails, the Customer is entitled to (a) demand an appropriate reduction of the respective fees, or (b) withdraw from the Agreement in the case of a substantial defect that prevents the Customer from using the deliverable in its entirety. Those Services or parts thereof which have already been provided substantially in accordance with the Service Agreement and which can be used by the Customer as such in an objectively reasonable manner must be paid in full. Any withdrawal from the Service Agreement shall not affect these Services and they shall remain subject to the relevant provisions of the Service Agreement.

In the event of defects that cannot be remedied in the short term, Taskbase has the right to provide the Customer with a temporary solution (workaround).

8.3. Warranty of title

Taskbase warrants that the Services do not infringe any intellectual property rights of third parties which exclude or restrict the contractual use of the Services by the Customer.

If a third party attempts to prevent the Customer from using the Services in accordance with the Service Agreement on the basis of allegedly superior proprietary rights, the Customer shall notify Taskbase of this in text form without delay (e-mail sufficient). Provided that the Customer notifies Taskbase without delay and provides reasonable assistance, Taskbase shall, at its own discretion, either (i) modify the relevant Services in such a way that they do not infringe the proprietary rights of the respective third party while however, fulfilling all material requirements of the Customer, (ii) procure a license for the Customer from the third party at its own expense or (iii) dispute the third party claim. In the event that a legal action is brought against the Customer by the third party, the Customer shall transfer to Taskbase exclusive control regarding the conduct of the lawsuit and take all actions necessary for this purpose. Subject hereto, Taskbase shall bear the costs of litigation (including reasonable attorneys' fees) and shall compensate the Customer for any direct damage resulting from a final judgment against the Customer. The Customer shall forfeit its claims under this provision if it withdraws or fails to give Taskbase control over the conduct of the lawsuit, in particular if it deals with third-party claims in whole or in part by means of settlement or recognition without the express consent of Taskbase.

8.4. Exclusion of warranty

Taskbase's warranty shall be excluded in case of incidents or circumstances, the causes of which are beyond Taskbase's control and/or which are attributable in whole or in part to the Customer and/or to third parties not engaged by Taskbase (e.g. modifications of software or improper use of systems or other Services). Further, the warranty shall be excluded in case of incidents or circumstances related to force majeure events. No warranties apply to resources provided by the Customer (e.g. software licenses). In addition and in the absence of any agreement to the contrary in the Service Agreement, Taskbase makes no warranty that the Services can be used uninterruptedly and flawlessly in all combinations desired by the Customer, with any possible data or with any other IT systems or programs.

9. Liability

Taskbase shall be liable for proven direct damages in case of a breach of contract, unless Taskbase proves that it is not at fault. The liability shall be limited to the amount of the remuneration owed under the Service Agreement for the year in which the damage occurs. The liability shall be unlimited

for any damages caused intentionally or through gross negligence, as well as for personal injury.

Taskbase's liability for any indirect or consequential damages, including but not limited to lost profits, loss of data, loss of reputation and third-party claims, shall be excluded.

10. Force majeure

Neither Party shall be liable for any damage, loss or delay resulting from any force majeure event, including but not limited to natural disaster (e.g. avalanches, flooding, landslides, etc.), acts of war, terrorism, riots, labor strike, pandemics, DDOS attacks, hacking, malware, ransomware, unforeseeable official restrictions and criminal acts of third parties, and any delivery date shall be extended to the extent of any delay resulting from any such force majeure event.

However, if performance of a contractual obligation is prevented by such a circumstance for a period of 90 days or more, each Party shall be entitled to terminate the Service Agreement subject to 90 days' prior notice. In case of termination by the Customer, all fees under the Service Agreement are due and payable immediately pro rata up to the date of termination.

11. Intellectual property rights

11.1. In general

Unless otherwise agreed upon in the Service Agreement, no rights are transferred to the Customer in connection with the provision of the Services by Taskbase and the use of the Services by the Customer.

11.2. Recurring/operational services

Taskbase grants the Customer a non-exclusive, non-transferable, non-sublicensable right, limited to the term of the Service Agreement, to use the recurring Services in compliance and to the extent agreed upon in the Service Agreement.

11.3. One-time services

11.3.1. Newly created intellectual property rights

Insofar as agreed in the Service Agreement, all intellectual property rights newly and specifically created for the Customer in connection with the provision of one-time Services under the Service Agreement, in the case of software newly developed specifically for the Customer including the source code and the complete documentation, shall transfer to the Customer at the time of their creation. Taskbase undertakes to take all required actions for this purpose and issue the appropriate legal declarations in the requisite form to the extent required, and to ensure that any third parties involved do the same.

11.3.2. Pre-existing intellectual property rights

Unless otherwise specified in the Service Agreement, the Customer shall acquire a non-exclusive right, unlimited in time, to use any pre-existing intellectual property rights that are contained in the one-time Services provided by Taskbase. The Customer may create copies of such Services protected by pre-existing intellectual property rights for backup and archival purposes.

12. Confidentiality and data protection

12.1. Contractual confidentiality obligations

Both Parties undertake to treat as confidential any information that is not obvious or generally accessible concerning the other Party, or the customers and business relationships of the other Party, that may come to their attention in connection with their performance of the Service Agreement or with

their contractual relationship in general.

The Parties undertake to make such information accessible to their staff, other auxiliary agents and third parties involved or other third parties only to the extent permitted to the Parties under the Service Agreement or where approved in advance by the other Party. Taskbase shall be entitled to pass on the information to third parties (e.g. subcontractors) engaged by it in Switzerland and abroad as well as to group companies (parent, sister or daughter companies of Taskbase) to the extent necessary in connection with the conclusion and performance of the Service Agreement.

The Parties confidentiality obligations shall not apply to information that:

- was already in the public domain at the time of its disclosure by the disclosing Party;
- was already known to the other Party before it was made accessible by the disclosing Party;
- was lawfully provided to the other Party by a third party without any restrictions on disclosure;
- was developed internally by the other Party without using or referring to the confidential information of the disclosing Party.

The confidentiality obligations shall also extend to information exchanged prior to the conclusion of the Service Agreement and shall continue to apply after its termination, for so long as a Party has a legitimate interest in confidentiality but, as a rule, for a period of at least 3 years after the termination of the relevant contractual relationship.

12.2. Statutory or regulatory confidentiality obligations

Taskbase shall be obliged to treat as confidential any information concerning the Customer that is protected by statutory or regulatory confidentiality obligations insofar as Taskbase has been informed about the Customer being subject to such obligations in the Service Agreement or otherwise in text form. This shall apply in particular with regard to information protected by the banking secrecy, official secrecy, telecommunications secrecy, and non-disclosure duties under social insurance law.

12.3. Data protection

The Parties shall comply at all times with applicable data protection laws, in particular the provisions of the Swiss Data Protection Act (nDSG) and the EU-GDPR, when handling personal data. This also includes the implementation of appropriate technical and organizational security measures.

The Parties enter into a separate Data Processing Agreement (DPA) (Annex 6 to the Service Agreement).

Further data protection-related information can be found in Taskbase's privacy policy, which the Customer acknowledges when concluding the Service Agreement. The Customer shall observe the current version, available at: taskbase.com/privacy-policy

12.4. Common provisions

Notwithstanding the foregoing, each Party may disclose confidential information and personal data if and to the extent such disclosure is required pursuant to a court order or in accordance with a statutory or regulatory obligation. To the extent permitted by law, the other Party shall be informed of such disclosure in advance, and the disclosing Party shall cooperate with the other Party with respect to the manner of the disclosure and shall take all reasonable measures and avail itself of all reasonable legal remedies in order to prevent the disclosure and to achieve the confidential treatment of the information to be disclosed.

Any information and personal data that is no longer required for the performance of the Service Agreement or in the context of the business relationship as such shall be erased, subject to any mandatory statutory retention obligations or legitimate interests of the relevant Party, as provided for by law, in further retention.

Each Party shall take reasonable technical and organizational security measures within its respective sphere of responsibility in order to protect the confidential information and personal data (including information and data retained).

13. Compliance with laws and regulations

The Parties shall comply with all laws and regulations applicable to them. Taskbase will thus comply with all laws and regulations applicable to Taskbase generally as a provider of the Services agreed upon in the Service Agreement. The Customer is responsible for determining and specifying the requirements of laws and regulations applicable to the Customer's business, in particular those relating to the Services that the Customer procures under the Service Agreement.

14. Suspension of Services by Taskbase

Taskbase is entitled to suspend or restrict access of the Customer to the Services immediately and without further notice:

- if the Customer is in default with the payment of fees due under the Service Agreement;
- if the Customer breaches any clause of the Service Agreement, any terms of license and use (software) or any specifications or instructions by Taskbase (e.g. instructions for the use of systems);
- if Taskbase terminates the Service Agreement for good cause;
- if the undisturbed operation of Taskbase is endangered on the basis of circumstances within the Customer's responsibility.

The suspension of the Services shall not affect the right to terminate for cause according to section 15.2 of these GTC.

15. Term, termination and effects of termination

15.1. Term and ordinary termination

The Service Agreement enters into force as of the relevant effective date as specified therein and, subject to earlier termination as provided below, be concluded for the term as specified therein.

15.2. Termination for cause

Either Party shall be entitled to terminate the Service Agreement with immediate effect for cause where:

- the other Party materially breaches its obligations under the Service Agreement (including, with respect to the Customer, the failure to pay any agreed fees or the breach of essential terms of license and use) and has failed to remedy the breach within 30 days after written notice from the other Party;
- the other Party dissolved or otherwise ceased operations;
- the other Party is placed into bankruptcy, commences composition proceedings, or is insolvent.

15.3. Effects of termination

Upon any termination of the Service Agreement, the Customer shall, as of the effective date of such termination, immediately cease accessing and otherwise utilizing the Services (except during an agreed transition period, if any) and any confidential information of Taskbase (as defined in section 12.1).

If Taskbase terminates the Service Agreement for the Customer's uncured material breach, all fees under the Service Agreement shall become immediately due and payable within 10 days of the effective date of termination.

Termination of the Service Agreement will not affect any accrued rights (in particular Taskbase's right to demand payment of all fees that the Customer is obliged to pay until the date of termination), claims and/or liabilities of either Party at the date of termination and shall be without prejudice to any other rights and/or remedies that either Party may have under the Service Agreement.

Further, the termination of the Service Agreement shall have no effect on the clauses which, by their nature, shall survive termination of the Service Agreement, particularly but not exclusively the clauses relating to intellectual property rights, liability, confidentiality and applicable law and place of jurisdiction.

16. Changes

16.1. Changes to Services and fees

Should the Customer wish to make any changes to any contractually pre-defined Services, it shall inform Taskbase thereof in text form (change request). Taskbase shall promptly state whether the change is possible along with any implications that it will have, in particular on the Services to be provided as well as on the fees and contractual deadlines (if any). The changes to the Taskbase Services as requested by the Customer, along with any adjustment of the fees, contractual deadlines (if any) and other terms of the Service Agreement, shall be agreed on in text form prior to execution and, if requested by a Party, signed by both Parties (e.g. by means of an addendum to the Service Agreement).

With respect to recurring Services (e.g. operating and maintenance services), Taskbase may adapt the Services at any time (e.g. due to further developments), provided that this does not impair the Customer's use of the Services. Further, Taskbase reserves the right to make changes to the Services that affect the Customer's use, as well as adjustments to the fees. Taskbase will inform the Customer of such changes in an appropriate manner (e.g. via e-mail). If Taskbase increases fees in such a way that they lead to a higher total charge for the Customer, or if Taskbase significantly changes the Services to the detriment of the Customer, then Taskbase will inform the Customer sufficiently in advance and the Customer may terminate the Service Agreement as of the effective date of the changes. If the Customer fails to do so, the changes are deemed approved. Adjustments to the fees as a result of a change in legal requirements (e.g. increase of the value-added tax rate), as a result of an adjustment to inflation (in accordance with the Consumer Price Index (CPI) of the Swiss Federal Statistical Office) and increases of the fees by service partners or other third party providers of Taskbase are not considered increases of the fees and do not entitle the Customer to terminate the Service Agreement.

Taskbase can also change the names of its Services (e.g. product names) at any time. Taskbase will inform the Customer of such changes in an appropriate manner (e.g. via e-mail).

16.2. Contractual amendments

Any amendments or supplements to the Service Agreement (including amendments to this provision) shall only be legally valid if concluded in writing (with handwritten signatures) or in electronic form (e.g. an electronic file which contains a scan of the signature(s) or a signature with DocuSign, Skribble or any other reputable provider of electronic signatures).

However, Taskbase reserves the right to amend these GTC at any time. Taskbase will notify the Customer of such amendments in an appropriate manner (e.g. via e-mail). If Taskbase amends the GTC significantly to the detriment of the Customer, Taskbase will inform the Customer sufficiently in advance and the Customer may terminate the Service Agreement, which is affected by the amendments, as of the effective date of the amendments. If the Customer fails to do so, the amendments are deemed approved.

17. Miscellaneous

The Service Agreement sets forth the entire agreement between the Parties in relation to the subject matter thereof and shall replace all previous written or oral agreements or declarations of intention in this regard between the Parties.

The waiver of any contractual breach or the failure to enforce any of the rights thereunder shall not be construed as a waiver to enforce other rights or the same right in the future.

In the event that any term or part of any term of the Service Agreement is or becomes invalid or unenforceable, this shall not affect the remaining terms of the Service Agreement. An invalid or partially invalid or unenforceable or partially unenforceable clause shall be replaced by a valid clause (as the case may be by a court order), which comes as close as possible to the meaning and purpose of such clause, and the Parties undertake to sign all agreements and documents that may be necessary in that respect. The same procedure shall be followed should any gap become apparent in the Service Agreement.

The Parties undertake to refrain from transferring/assigning the Service Agreement or any rights or obligations thereunder to any third party without the prior written approval of the other Party.

No agency, partnership, joint venture, or employment is created as a result of the Service Agreement and neither Party has any authority of any kind to bind the other Party in any respect whatsoever.

All notices between the Parties under the Service Agreement must be made by e-mail or letter to the addresses stated in Annex 1 to the Service Agreement. This does not apply to notices and communications on operational matters.

18. Dispute resolution, applicable law and place of jurisdiction

Any disagreement arising out of or in connection with the Service Agreement shall be resolved by mutual agreement if possible. If this is not possible, a mediation proceeding shall be conducted by an independent lawyer. If the disagreement cannot be resolved within 60 days of the commencement of the mediation procedure, the Parties shall be free to bring the matter to the ordinary courts.

The Service Agreement shall be governed in all respects by the substantive laws of Switzerland, excluding the United Nations Convention on Contracts of International Sale of Goods of 11 April 1980 (CISG) and the provisions of international private law (which shall not apply).

All disputes arising out of or in relation to the Service Agreement, including those concerning its valid conclusion, legal validity, amendment or dissolution shall fall under the exclusive jurisdiction of the courts of Zurich 1, Switzerland.

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.

Annex 7 – Technical and Organizational Measures (TOM)

Version: 17.9.2026

This Annex 7 describes the technical and organizational measures taken by Taskbase for the Sales Coach under the data processing agreement (DPA) within the scope of the contract to protect the personal data processed and/or to ensure data security appropriate to the risk (Art. 8 nDSG and Art. 3 DSV, and Art. 32 GDPR).

The technical and organizational measures are subject to technical progress and continuous development. Alternative or additional measures may be implemented, provided that the agreed level of protection is not compromised.

This Annex 7 is focused on the description of the technical and organizational measures that Taskbase itself has taken. Taskbase has contractually obliged its appointed sub-processors (see Annex 8) to implement appropriate technical and organizational measures. The description of these technical and organizational measures can be found in the corresponding documentation of the sub-processors. Taskbase will provide detailed information on this upon request.

Taskbase operates no own server or data-centre infrastructure. All production systems run on AWS (EU) and cloudscale.ch (CH); physical, environmental and hypervisor-level security is provided by those sub-processors under their certifications (Annex 8).

How to read the status column

STATUS	MEANING
Implemented	Formally in place and consistently applied
Partial	In place, with the stated limitation
Planned	Committed and scheduled, not yet in place

1. Governance

Who is accountable for security, and how Taskbase knows the measures are working.

REF	MEASURE	STATUS
G1	A named internal information security owner is accountable for the security programme and reports to the CEO. A designated data protection contact point is in place.	Implemented
G2	A documented risk methodology is applied, and information security risks are recorded in a risk register with owner, likelihood, impact and treatment decision.	Implemented

REF	MEASURE	STATUS
G3	All measures in this annex correspond to entries in an internal control register with an owner, a status and a review date. This annex is derived from that register.	Implemented
G4	Security posture and roadmap are reviewed with company leadership on a recurring basis.	Implemented
G5	The full control set is reviewed at least annually.	Implemented

2. People

The staff who can reach customer data, and the obligations they are under.

REF	MEASURE	STATUS
P1	All employment and contractor agreements contain confidentiality obligations covering personal data, which continue to apply after the engagement ends.	Implemented
P2	Access to customer personal data is limited to personnel who require it for the purposes set out in Annex 6.	Implemented
P3	Security awareness training for all staff, with role-specific secure-development content for engineers.	Planned
P4	Documented joiner, mover and leaver process with access revocation on departure.	Partial lived but not documented
P5	A named internal escalation path for reporting suspected security incidents.	Implemented

3. Physical and Environmental

Where the hardware sits, and who can physically reach it.

REF	MEASURE	STATUS
PH1	Physical and environmental security of all processing facilities is provided by AWS (EU) and cloudscale.ch (CH) under their ISO 27001 and SOC 2 certifications.	Implemented by sub-process
PH2	No production customer data is stored on office infrastructure or on employee endpoints in the ordinary course.	Implemented
PH3	Entry to the office building requires a PIN code. The office is automatically locked outside business hours (17:00 to 08:00). Because building entry is credential-gated, visitors cannot enter unaccompanied and are accompanied throughout.	Implemented
PH4	Endpoints are personally owned and not centrally managed. At Rest encryption is mandated. Compensating control: production data access is cloud-side via VPN, centrally logged and centrally revocable rather than local, so loss of an endpoint does not expose customer data.	Partial as endpoints are not centrally managed

4. Identity and Access

Who is allowed in, to which systems, and with what privilege.

REF	MEASURE	STATUS
IA1	Multi-factor authentication is enforced on all business systems and administrative interfaces.	Implemented
IA2	Product user authentication runs through a central identity provider (ZITADEL) supporting enforced multi-factor authentication.	Implemented
IA3	Access to production customer data follows least privilege; access rights are granted per role and per need.	Partial Engineers have broad access rights in order to facilitate quick repairs. Improvements planned.
IA4	Copies of production data for development or diagnostic purposes are created only through a sanctioned script that records requester, purpose and time, runs server-side rather than on endpoints, enforces a time-to-live, and tears copies down automatically each night.	Implemented
IA5	Such copies default to masked or synthetic data; a copy containing real customer data is a justified, logged, time-limited exception confined to the requester.	Planned
IA6	Cloud infrastructure access is separated into normal and administrative access. Administrative access requires additional authentication.	Implemented
IA7	No long-lived static access keys for human or automated access; pipelines authenticate using short-lived federated credentials.	Planned
IA8	Service and infrastructure secrets are held in a managed secret store, never in source repositories or plaintext files, with secret detection in the pipeline.	Partial Secrets are currently part of CI/CD so not in source code but also not yet in a dedicated managed secret store.
IA9	Granted access rights are reviewed and recertified periodically.	Planned

5. Network and Communications

What data moves between systems, and whether it can be intercepted.

REF	MEASURE	STATUS
N1	TLS 1.2 or higher for all external traffic carrying customer data; no plaintext protocols.	Implemented
N2	Administrative access to production requires connection through the company VPN; production systems are not directly reachable from the internet outside defined ingress points.	Implemented
N3	SPF, DKIM and DMARC are configured on all company sending domains, with DMARC reports reviewed at least semi-annually.	Implemented

REF	MEASURE	STATUS
N4	A maintained overview records which systems exchange data, the data class carried by each flow, and every external recipient with its region.	Planned

6. Systems and Applications

How changes reach production, and how defects are found before they do.

REF	MEASURE	STATUS
S1	Production, staging and development environments are separated.	Implemented
S2	All production changes pass through a merge request; every change is attributable to an author and revertible.	Implemented
S3	An automated test suite gates deployment.	Implemented
S4	Human review is required for changes affecting authentication, authorisation, data access or infrastructure.	Partial Consistently applied but not formalized
S5	Static analysis, dependency scanning, secret detection and infrastructure-as-code scanning run in the pipeline, with high-severity findings tracked to closure under a remediation deadline.	Planned
S6	Automated dependency updating with review, and remediation deadlines by severity.	Planned
S7	Recurring automated vulnerability scanning of internet-facing services and infrastructure.	Partial Not all systems yet. Extension is planned.
S8	Independent external penetration test with tracked remediation.	Planned

7. AI and Agent Processing

How the models and agents handle customer content, and what they are prevented from doing.

REF	MEASURE	STATUS
AI1	Customer content is not used to train, fine-tune or otherwise adapt Taskbase models.	Implemented
AI2	Sub-processed model providers are contractually excluded from training on customer data. Inference runs in EU regions, and the primary inference path is configured for zero data retention at the provider.	Implemented
AI3	The Service produces coaching guidance for human use. It performs no automated decision-making producing legal effects or similarly significant effects on a data subject.	Implemented
AI4	Agent observability data (prompts, outputs and tool calls) is retained on Taskbase-operated infrastructure and is not transmitted to a third-party observability provider.	Implemented

REF	MEASURE	STATUS
AI5	Agent tool calls and data access are traced in sufficient depth to reconstruct what an agent did with customer data.	Implemented
AI6	Tenant and persona isolation is enforced in the retrieval, cache and execution layers.	Partial enforced in code, automated verification planned.
AI7	Agent permissions follow least privilege per tenant, with no access to data the requesting user could not see directly.	Partial Agent acts with rights of user so can in general not access more data. Additional measures planned.
AI8	Ingested content (transcripts, CRM text, uploads) is not treated as instruction, and tool calls are validated before execution.	Planned
AI9	Sensitive or irreversible agent actions require human confirmation.	Planned

8. Data and Information

Protection of the data itself, including how long it is kept and when it is deleted.

REF	MEASURE	STATUS
D1	Encryption at rest for all persistent storage holding customer data, including databases and object storage.	Implemented
D2	Backups are encrypted and integrity-protected by cryptographic signing.	Implemented
D3	Customer data is processed and stored in the EU/EEA and Switzerland; per-sub-processor locations are listed in Annex 8.	Implemented
D4	Customer tenants are logically separated, with the tenant identifier enforced at the data access layer.	Implemented
D5	Retention is bounded and documented: live customer data including traces until end of contract plus 30 days, backups 65 days, operational and security logs up to 12 months.	Implemented
D6	Deletion on termination is executed rather than left to expiry; data export is available to the customer before deletion on request.	Implemented
D7	Alerting on bulk reads of customer data.	Planned
D8	A data classification scheme drives handling requirements per class.	Planned

9. Suppliers and Third Parties

The sub-processor chain, and the assurance obtained before a vendor is engaged.

REF	MEASURE	STATUS
SU1	A documented vendor risk assessment is completed before onboarding any vendor with access to customer data, covering certifications, data processing terms, breach notification, sub-processors and data residency.	Implemented
SU2	A data processing agreement is in place with each sub-processor, with Standard Contractual Clauses and Swiss addendum where required, and a transfer impact assessment where the importer is established outside the EEA and Switzerland.	Implemented
SU3	The sub-processor list is maintained and published as Annex 8, with advance notice of additions and replacements.	Implemented
SU4	Sub-processors are reassessed on material change and on a defined periodic cadence.	Implemented

10. Operations and Resilience

Detecting incidents, responding to them, and recovering from data loss.

REF	MEASURE	STATUS
O1	Central audit logging of authentication, privileged actions and infrastructure changes.	Implemented
O2	Security alerts are routed to a channel that is actively monitored.	Partial coverage currently narrower than O1
O3	All systems holding customer data are backed up.	Implemented
O4	At least one backup copy is immutable or isolated from production credentials.	Planned
O5	Recovery point and recovery time objectives are documented per system.	Implemented
O6	Restores are tested on a recurring schedule and the restore time is controlled.	Implemented
O7	A written disaster recovery plan covers roles, decision points, communication and per-system recovery order.	Partial Steps exist, comprehensive plan currently in construction
O8	A documented incident response process defines severity levels, roles, escalation, and the customer and regulator notification route.	Partial Process exists including escalation and notification routes. Severity levels still need to be formally defined
O9	Post-incident review with tracked follow-up actions.	Partial performed, not yet formalised

11. Compliance and Audit

Demonstrating that the measures operate, and meeting legal obligations.

REF	MEASURE	STATUS
C1	A register of applicable legal and regulatory obligations records, per entry, why it applies, the role held, status and owner.	Partial drafted, verification in progress
C2	This annex is derived from the internal control register and reviewed on material change to the control set and at least annually.	Implemented
C3	Records of processing activities as processor under Art. 30(2) GDPR are maintained and made available on request.	Planned
C4	Taskbase assists controllers with data protection impact assessments and prior consultation.	Implemented
C5	A documented process handles data subject requests forwarded by the customer, within a defined response time.	Partial CS has responsibility for customer data subject requests. Not fully formalized.
C6	A published security contact and vulnerability disclosure route.	Partial Main contact security@taskbase.com not yet exposed via security.txt Standard
C7	ISO 27001 certification.	Planned First steps initiated

Mapping to statutory and legacy control categories

This table maps the measures above to the control categories named in Swiss and EU data protection law, and to the legacy control categories used in the previous version of this annex. It adds no measures of its own; the sections above govern.

STATUTORY OR LEGACY CATEGORY	COVERED BY
DSV Art. 3(1) Zugriffskontrolle	IA1, IA3, IA4, IA5, IA9, P2, D4, AI6, AI7
DSV Art. 3(1) Zugangskontrolle	PH1, PH2, PH3
DSV Art. 3(1) Benutzerkontrolle	IA1, IA2, IA6, IA7, IA8, N1, N2
DSV Art. 3(2) Datenträgerkontrolle	D1, D2, PH1, PH4
DSV Art. 3(2) Speicherkontrolle	D1, D4, IA3, O1
DSV Art. 3(2) Transportkontrolle	N1, D1, D3
DSV Art. 3(2) Availability, integrity and recovery	D2, O3, O4, O5, O6, O7
DSV Art. 3(3) Eingabekontrolle (input logging)	O1, S2, AI5

STATUTORY OR LEGACY CATEGORY	COVERED BY
DSV Art. 3(3) Bekanntgabekontrolle (disclosure traceability)	D3, N4, SU2, SU3, Annex 8
DSV Art. 3(3) Detection and remediation of breaches	O1, O2, O8, O9, S5, S7
DSV Art. 4 Protokollierung	O1, S2, AI5, D5
DSV Art. 7 Processor obligations	SU1, SU2, SU3, SU4, P1, P2
GDPR Art. 32(1)(a) Pseudonymisation and encryption	D1, D2, N1, IA5
GDPR Art. 32(1)(b) Confidentiality, integrity, availability, resilience	D1, D2, D4, O1, O2, O3, O4, AI6
GDPR Art. 32(1)(c) Restoration after an incident	O3, O4, O5, O6, O7
GDPR Art. 32(1)(d) Testing and evaluating effectiveness	G3, G5, C2, S5, S7, S8, O6
GDPR Art. 32(4) Personnel acting under authority	P1, P2
GDPR Art. 25 Data protection by design and by default	IA5, D4, D5, D8, AI1, AI2, AI7, AI8
Legacy: Access Control (Physical) / Zutrittskontrolle	PH1, PH2, PH3
Legacy: Access Control (System) / Zugangskontrolle	IA1, IA2, IA6, IA7, IA8, N1, N2, PH4
Legacy: Access Control (Data) / Zugriffskontrolle	IA3, IA4, IA5, IA9, P2, D4, D6, AI6, AI7
Legacy: Transfer and Transmission Control / Weitergabekontrolle	N1, N4, D3, SU2, SU3, Annex 8
Legacy: Input Control / Eingabekontrolle	O1, S2, AI5, D5, D6
Legacy: Order Control / Auftragskontrolle	SU1, SU2, SU3, SU4
Legacy: Availability Control / Verfügbarkeitskontrolle	D2, O3, O4, O5, O6, O7, PH1
Legacy: Separability / Trennungskontrolle	S1, D4, AI6
Legacy: Review, Assessment and Evaluation	G1, G2, G3, G4, G5, C1, C2, C4, S8, O6
Legacy: Incident Response Management	O1, O2, O8, O9, P5, C6
Legacy: Privacy by Design / Privacy by Default	IA5, D4, D5, D8, AI1, AI2, AI3, AI7, AI8

Annex 8 – Sub-processors

Version: 3.9.2026

This Annex 8 lists the sub-processors engaged by Taskbase. Processing location is where personal data is stored and processed. Additions and replacements are governed by the sub-processor clause of Annex 6.

SUB-PROCESSOR	SERVICE	PERSONAL DATA PROCESSED	PROCESSING LOCATION	TRANSFER SAFEGUARD
Amazon Web Services	Cloud infrastructure and application hosting; LLM inference via Amazon Bedrock	Name, email, CRM contact and activity data relating to the customer's employees and their business contacts, conversation and transcript content, application data	Germany (EU)	AWS GDPR DPA (part of AWS Service Terms); EEA-established processor with EU-region processing, so no third-country transfer for the engagement itself; the DPA's EU SCCs and Swiss Addendum would apply automatically to any onward transfer outside the EEA or Switzerland.
Supabase	Application platform: PostgreSQL database, object storage, authentication, realtime, edge functions	Name, email, CRM contact and activity data relating to the customer's employees and their business contacts, conversation and transcript content, application data	Switzerland (CH)	Signed DPA; EU Standard Contractual Clauses Modules Two and Three with Swiss Addendum (FDPIC); Transfer Impact Assessment completed
cloudscale.ch AG	IaaS hosting for parts of the application	Name, email, conversation data	Switzerland (CH)	DPA compliant with the GDPR and the nDSG; Swiss adequacy decision (EU) — no Standard Contractual Clauses required
Anthropic	Claude large language models, accessed through Amazon Bedrock	Prompts and model outputs, which may contain any customer content submitted to the Service	Germany (EU) — Bedrock EU region, zero-day retention	Accessed via Amazon Bedrock under the AWS DPA and Standard Contractual Clauses above; the model provider has no access to Bedrock prompts or completions. Anthropic's own DPA with Standard Contractual Clauses applies to any direct API use. No training on customer data

SUB-PROCESSOR	SERVICE	PERSONAL DATA PROCESSED	PROCESSING LOCATION	TRANSFER SAFEGUARD
Microsoft Azure	EU-region LLM inference (Azure OpenAI / Azure AI)	Prompts and model outputs, which may contain any customer content submitted to the Service	Germany (EU)	Microsoft Products and Services DPA (applies automatically under the Product Terms), including EU Standard Contractual Clauses; EU–US Data Privacy Framework; no training on customer data
Google Cloud	Gemini Enterprise Agent Platform (formerly Vertex AI) — agent hosting and inference	Prompts and model outputs, which may contain any customer content submitted to the Service	Belgium (EU)	Google Cloud DPA (applies automatically under the Cloud Terms), including EU Standard Contractual Clauses; EU–US Data Privacy Framework; prompts and outputs not retained for model training
Recall.ai* (* only relevant if Taskbase Recording Tool is used)	Meeting capture, transcription and meeting metadata	Meeting transcripts, participant names and email addresses, join and leave times, meeting titles. Audio and video as recorded and controlled by the customer.	Germany (EU)	DPA with EU Standard Contractual Clauses Modules Two and Three (Swiss modifications, FDPIC); Transfer Impact Assessment completed.
bliro GmbH* (* only relevant if Bliro is used as part of a partnership agreement)	AI meeting transcription and summarisation; no audio or video recording is stored	Name, email, meeting transcripts, audio transiently processed on device.	Germany (EU)	DPA under German law signed per customer order
ZITADEL	Identity and access management for Service users	First name, last name, email, language, gender, authentication data	Switzerland (CH)	ZITADEL DPA; SCC, US-EU and Swiss US Data Privacy Framework
iWay AG	Outbound transactional email (SMTP relay)	Email address, name, message content	Switzerland (CH)	DPA under Swiss law; Swiss adequacy decision (EU). Relay only — no mailbox or message storage
PostHog	Product analytics.	Device and browser data, product usage events, pseudonymous user identifier. No customer content beyond incidental info in URLs/browser data	Germany (EU)	PostHog DPA including EU Standard Contractual Clauses and nDSG adaptations; EU–US Data Privacy Framework + Swiss–US DPF