

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-processors
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