> **ENTWURF — ANWALTLICHE PRUEFUNG ERFORDERLICH**
>
> Dieses Dokument ist ein **technischer Erstentwurf** der Solvevo-IT-Solutions GmbH und gibt den Stand der bei solvevo ONE umgesetzten technisch-organisatorischen Massnahmen wieder. Es **ersetzt keine anwaltliche Pruefung** und ist nicht zur direkten Vertragsverwendung freigegeben. Vor Veroeffentlichung als Vertragsbestandteil ist eine Pruefung durch eine datenschutzrechtlich qualifizierte Kanzlei verbindlich.
>
> **Status:** ENTWURF v0.1 · Stand 2026-04-30 · Verantwortlich: Geschaeftsfuehrung

Technisch-organisatorische Massnahmen (TOM)

Verantwortlicher: Solvevo IT-Solutions GmbH

Anlage zum Auftragsverarbeitungsvertrag gemaess **DSGVO Art. 32** (Sicherheit der Verarbeitung) und **Art. 28 Abs. 3 lit. c**.

Geltungsbereich: Plattform „solvevo ONE" (`one.solvevo-it.com`), inklusive optionaler On-Prem-Agent-Komponente fuer Microsoft-365- und Active-Directory-Anbindung beim Auftraggeber.

Stand: 2026-04-30

1. Pseudonymisierung (DSGVO Art. 32 Abs. 1 lit. a)

Massnahme	Umsetzung
Trennung Stammdaten / Verarbeitungsdaten	Mehrfach-mandantenfaehige Architektur — jede Verarbeitung ist auf den Mandanten des Auftraggebers begrenzt.
Pseudonyme IDs	Interne Datensaetze werden ueber UUIDv4-Identifikatoren referenziert; Klarnamen-Querverweise nur dort, wo der Geschaeftszweck es erfordert.
Pseudonymisierung bei AI-Verarbeitung	Personenbezogene Daten werden vor Uebermittlung an externe AI-Provider regelbasiert maskiert (E-Mail, Telefon, IBAN, Kreditkarten, IP-Adressen).
Audit-Spuren ohne Klartext	Audit-Eintraege fuer privilegierte Operationen enthalten SHA-256-Hashes statt Klartext (z. B. PowerShell-Skripte).

2. Verschluesselung (DSGVO Art. 32 Abs. 1 lit. a)

2.1 Verschluesselung im Ruhezustand (At-Rest)

Datenklasse	Verfahren	Schluessel-Verwaltung
Sensible Anwendungs-Felder (M365-Secrets, MFA-Geheimnisse, Cloud-Zugangsdaten, SSH-Keys, OAuth-Tokens, SAML-Zertifikate)	AES-256-GCM	Separater `ENCRYPTION_KEY` (256 Bit), getrennt vom Sitzungs-Schluessel; jaehrliche Rotation moeglich
Datenbank-Backups (off-site)	XChaCha20-Poly1305 (libsodium)	Client-seitige Verschluesselung vor Uebertragung an den Backup-Anbieter (zero-trust gegenueber Storage-Anbieter)
Audit-Log-Archive (Cold-Storage)	gzip + SHA-256-Fingerprint in der Hash-Kette	identisch wie operatives Audit-Log

2.2 Verschluesselung in der Uebertragung (In-Transit)

Verbindung	Verfahren	Mindestversion
Browser ↔ Plattform	TLS	1.3 (TLS 1.2 als Fallback fuer Legacy-Clients)
On-Prem-Agent ↔ Plattform	mTLS mit Cloud-eigener Plattform-CA, Session-Token mit 1h-TTL	TLS 1.3
Outbound zu E-Mail- und AI-Providern	TLS	1.2+

Schluessel-Hierarchie: Vier voneinander getrennte Schluesselbereiche (Anwendungs-Verschluesselung, Sitzungs-Authentifizierung, Backup-Verschluesselung, Code-Signatur). Eine kompromittierte Schicht eskaliert nicht in andere.

Schluessel-Recovery: Master-Schluessel werden ueber ein **Shamir-2-of-3-Verfahren** an drei unabhaengige Verwahrstellen verteilt (Bankschliessfach + Wirtschaftspruefer-Kanzlei + Notar). Jaehrliche Pruefung der Plomben.

---

3. Vertraulichkeit (DSGVO Art. 32 Abs. 1 lit. b)

3.1 Zutrittskontrolle

Massnahme	Umsetzung
Rechenzentrums-Standort	Frankfurt am Main (Deutschland), Tier-III- bis Tier-IV-zertifiziert
Hoster	IONOS Cloud GmbH (BSI C5 Type 2 testiert, ISO 27001 zertifiziert)
Physischer Zutritt	Vom Hoster verantwortet — biometrisch / Mehr-Augen-Prinzip
Backup-Standort	Hetzner Online GmbH (Deutschland), zertifiziert nach ISO 27001 + DIN EN 50600

3.2 Zugangskontrolle (Login)

Massnahme	Umsetzung
Passwort-Policy	Mindestlaenge 12 Zeichen, Komplexitaetsanforderungen, bcrypt-Hashing mit 12 Runden
Multi-Faktor-Authentifizierung	TOTP-basiert (kompatibel mit allen gaengigen Authenticator-Apps), 10 Backup-Codes
MFA-Pflicht	Pro Mandant einstellbar: optional / fuer Administratoren erzwungen / fuer alle erzwungen
Single-Sign-On	OpenID Connect 1.0 + SAML 2.0 (mit Audience-Restriction, Replay-Cache, signierten Assertions)
User-Provisioning	SCIM 2.0 verfuegbar
Brute-Force-Schutz	Rate-Limiting 5 Login-Versuche pro Minute pro IP, Account-Lockout
Session-Management	JWT mit 1 Stunde Gueltigkeit, 30-Minuten-Idle-Timeout, Token-Invalidierung bei Passwortaenderung

3.3 Zugriffskontrolle (Berechtigungen)

Massnahme	Umsetzung
Rollenmodell	4 hierarchische Rollen (PLATFORM_ADMIN > ADMIN > AGENT > ENDUSER) mit feingranularer Berechtigungspruefung pro Endpunkt
Mandanten-Isolation	Zwei-Schichten-Modell: (a) Anwendungsschicht prueft Mandanten-ID in jeder Anfrage, (b) Datenbank-Ebene erzwingt Row-Level Security auf 40 Tabellen
Privilegierte Operationen	Vier-Augen-Prinzip („Dual-Control") fuer kritische Aktionen (Impersonation, Tenant-Loeschung, User-Hard-Delete, Schluessel-Rotation) — bei Aktivierung muss ein zweiter Administrator zustimmen
Berechtigungs-Reviews	Vom Auftraggeber zu konfigurieren; Plattform stellt Reports und Export-Funktionen bereit
IP-Allowlist	Pro Mandant konfigurierbar (CIDR-basiert)

3.4 Trennbarkeit (Mandantenfaehigkeit)

Massnahme	Umsetzung
Datenbankebene	PostgreSQL Row-Level Security (RLS) auf 40 mandanten-bezogenen Tabellen
Anwendungsschicht	`TenantAwarePrismaService` setzt vor jeder Datenbank-Transaktion die Mandanten-ID; Verstoesse fuehren zu fail-fast Ausnahmen
AI-Embeddings	Tenant-isolierte pgvector-Tabellen mit `tenant_id`-Spalte + RLS — keine mandantenuebergreifenden Embedding-Suchen moeglich

3.5 Weitergabekontrolle

Massnahme	Umsetzung
Verschluesselter Transport	TLS 1.3 fuer alle externen Verbindungen (siehe §2.2)
API-Webhooks (ausgehend)	HMAC-SHA256-signiert, Empfaenger pruefen Signatur
API-Webhooks (eingehend)	Quellen-URL-Allowlist + HMAC-Verifizierung; SSRF-Schutz blockiert Aufrufe in private IP-Bereiche
Datenexport	Audit-Logs als CSV/PDF mit SHA-256-Fingerprint, Mandanten-Daten als JSON-Export auf Anforderung

---

4. Integritaet (DSGVO Art. 32 Abs. 1 lit. b)

Massnahme	Umsetzung
Audit-Log	90+ Aktionstypen, manipulationssicher per SHA-256-Hash-Kette zwischen aufeinanderfolgenden Eintraegen
Append-only	Datenbank-Trigger blockiert UPDATE und DELETE auf Audit-Tabellen
Hash-Kette-Verifizierung	Endpoint `GET /audit-logs/verify` prueft die gesamte Kette; taeglicher automatisierter Check 04:00 mit Prometheus-Metrik
Tagesanker	Taeglicher Anker-Eintrag um 04:00 als Forensik-Hilfsmittel
BSI-Meldungen	NIS2-Berichte werden mit CAdES-Basic-Signatur (PKCS#7) versendet, optional spaeter HSM-basiert
Code-Signatur	Agent-Releases mit Ed25519 signiert, Auto-Update prueft Signatur vor Anwendung
Container-Images	Signiert mit Cosign, Trivy-CVE-Scan im CI vor Build

5. Verfuegbarkeit + Belastbarkeit (DSGVO Art. 32 Abs. 1 lit. b + lit. c)

Massnahme	Umsetzung
Backup-Strategie	Kontinuierliches WAL-Streaming alle 15 Sekunden, taegliche Base-Backups, Aufbewahrung 30 Tage rolling + 4 Wochen + 6 Monate
Recovery-Punkt-Ziel (RPO)	< 15 Minuten
Recovery-Zeit-Ziel (RTO)	< 2 Stunden bei Datenbank-Restore, < 4 Stunden bei Hoster-Komplettausfall
Restore-Drill	Quartalsweise gegen ein Test-Postgres
Rate-Limiting	Drei Schichten (per IP / per User / per Agent) gegen DoS-Effekte
Health-Checks	Liveness, Readiness, Prometheus-Metriken
Auto-Restart	Docker-Compose-Restart-Policy bei Container-Crash
DDoS-Schutz	Cloudflare-Edge fuer Trust-Center; IONOS-Edge fuer Anwendung

6. Verfahren zur regelmaessigen Pruefung (DSGVO Art. 32 Abs. 1 lit. d)

Massnahme	Frequenz
Dependency-Audit (`npm audit`)	Pro Pull-Request + woechentlich automatisiert
Container-Vulnerability-Scan (Trivy)	Pro Pull-Request
Audit-Chain-Verifikation	Taeglich automatisch + manuell jederzeit
Patch-Day	Monatlich nach dokumentierter Routine (`docs/security/patch-day.md`)
Backup-Restore-Drill	Quartalsweise
Notfallhandbuch-Review	Quartalsweise (BSI DER.4 Compliance-Attestation)
Externe Penetration-Tests	Jaehrlich (in Vorbereitung — Beauftragung Q3 2026)
Compliance-Attestations	15 Kontrollen aus NIS2 Art. 21, BSI-Grundschutz, DSGVO; Geltungsdauer je 90/180/365 Tage
Awareness-Schulungen fuer Mitarbeiter	Mit Quiz + PDF-Zertifikat, Pflicht fuer Administratoren

7. Auftragskontrolle (Sub-Processoren)

Massnahme	Umsetzung
Sub-Processor-Liste	Live unter `https://trust.solvevo.one/subprocessors/` und in der Anwendung unter `/data-protection/sub-processors`
Aenderungs-Notifizierung	E-Mail an die hinterlegten Datenschutz-Empfaenger des Mandanten **7 Tage vor Wirksamkeit** der Aenderung
AVV mit Sub-Processoren	Mit allen Sub-Processoren wird eine DSGVO-konforme Verarbeitungsvereinbarung abgeschlossen
Standardvertragsklauseln	Wo erforderlich (z. B. Drittland-Transfer bei optional aktivierten US-AI-Providern)

8. Loeschung und Rueckgabe (DSGVO Art. 17 + Art. 28 Abs. 3 lit. g)

Massnahme	Umsetzung
Soft-Delete von Mandanten	30-Tage-Kulanzphase, danach automatischer Hard-Delete
Hard-Delete einzelner Nutzer (DSGVO Art. 17)	Anonymisierung der Stammdaten, Loeschung aller Auth-Geheimnisse, Audit-Spur bleibt referenziell erhalten (Forensik)
Backup-Loeschung	Aufbewahrungs-Ablaufpolitik (Retention) loescht Backup-Daten gemaess konfigurierter Frist; Recovery aus geloeschtem Zeitfenster nicht mehr moeglich
Daten-Export bei Vertragsende	JSON-Export aller Mandanten-Daten auf Anfrage; Loesch-Bestaetigung schriftlich nach erfolgter Vernichtung
Verschluesselungs-Loesung	`cryptsetup` auf Server-Volumes, RAM-Ueberschreibung mit `dd if=/dev/urandom` bei Container-Decommissioning

9. Logging und Monitoring

Massnahme	Umsetzung
Audit-Aktionen	90+ definierte Aktionstypen, alle sicherheitsrelevanten Vorgaenge erfasst
SIEM-Export	Optional aktivierbar pro Mandant — Webhook (ECS-JSON, HMAC-signiert) / Syslog RFC 5424 / CEF (Splunk, ArcSight, QRadar)
Strukturierte JSON-Logs	In Produktion zur Weiterverarbeitung im Log-System des Auftraggebers
Aufbewahrung	365 Tage in der Datenbank, danach komprimiertes Cold-Storage-Archiv mit verifizierter Hash-Kette
Personenbezug in Logs	Keine PII in Anwendungs-Logs (Anti-PII-Filter), nur fachliche IDs

10. Verantwortlichkeiten

Rolle	Funktion
Verantwortlicher	Auftraggeber (Mandant der Plattform)
Auftragsverarbeiter	Solvevo IT-Solutions GmbH
Datenschutzbeauftragter Solvevo	datenschutz@solvevo-it.com
Sicherheitskontakt Solvevo	security@solvevo-it.com
Vorfall-Meldung Solvevo → Auftraggeber	Innerhalb 24 Stunden nach Erkenntnis (NIS2 Art. 23 — Informationen ueber Sicherheitsvorfaelle)

Anlagen

- Sub-Processor-Liste: `https://trust.solvevo.one/subprocessors/`
- Loeschkonzept (Detail): auf Anfrage unter NDA via Trust Center
- Notfallhandbuch (Detail): auf Anfrage unter NDA via Trust Center
- Kryptokonzept (Detail): auf Anfrage unter NDA via Trust Center

> **HINWEIS ZUM VERSIONSMANAGEMENT**
>
> Materielle Aenderungen dieser TOM werden den Auftraggebern **30 Tage vor Wirksamkeit** angekuendigt. Der Auftraggeber hat bei wesentlichen Verschlechterungen ein **ausserordentliches Kuendigungsrecht**.

Dokument-Hash (SHA-256): wird beim PDF-Build generiert und auf der letzten Seite ausgewiesen.