SCRUTARE

Auftragsverarbeitungsvertrag

DPA · revDSG + EU-GDPR-konform

1. Vertragsgegenstand

Dieser Auftragsverarbeitungsvertrag (DPA) regelt die Verarbeitung personenbezogener Daten durch **MProfi AG** (nachstehend "Auftragsverarbeiter") im Rahmen des Scrutare-SaaS-Vertrags mit dem Kunden (nachstehend "Verantwortlicher") gemäß Art. 9 revDSG sowie Art. 28 DSGVO.

2. Art und Zweck der Verarbeitung

Bereich	Beschreibung
Zweck	Bereitstellung der Scrutare-DD-Plattform (Document-Storage, AI-Analyse, IC-Memo-Generation, Workstream-Workflow)
Datenkategorien	Mitarbeiter-Stammdaten Target, LP-Kontaktdaten, Deal-Dokumente, Q&A-Konversationen
Betroffene	Mitarbeiter und Stakeholder des Targets, LP-Vertreter, GP-Team
Dauer	Laufzeit des SaaS-Vertrags + 30 Tage Datenexport-Window + 60 Tage Löschungsfrist

3. Sub-Processoren

Sub-Processor	Zweck	Hosting	DPA
Hetzner Switzerland	Server-Hosting (primär)	CH (Zürich)	✓
Infomaniak	Backup-Hosting	CH (Genf)	✓
Anthropic	AI-Doc-Analyse	EU/US (mit DPA)	✓
Mailjet	Transactional Emails	EU (FR)	✓
Adyen	Payment-Processing	NL (EU)	✓

Sub-Processor-Änderungen werden 30 Tage im Voraus an den Verantwortlichen kommuniziert. Widerspruch möglich innerhalb 14 Tagen.

4. Pflichten des Auftragsverarbeiters

- Verarbeitung ausschließlich nach dokumentierter Weisung des Verantwortlichen
- Vertraulichkeitsverpflichtung aller Mitarbeiter (NDA-Pflicht)
- Implementierung von TOM gemäß Abschnitt 6
- Unterstützung bei Auskunftsbegehren Betroffener (revDSG Art. 25)
- Meldung von Datenpannen innerhalb **24 Stunden** an Verantwortlichen
- Verantwortlicher meldet binnen 72h an EDÖB / DPA

- Audit-Recht 1× jährlich mit 30 Tagen Vorankündigung

5. Rechte des Verantwortlichen

- Auskunfts- und Korrekturrecht (revDSG Art. 25)
- Audit-Recht (siehe Abschnitt 4)
- Sub-Processor-Genehmigungs-/Widerspruchsrecht
- Datenexport in standardisiertem Format (CSV + JSON)
- Vollständige Löschung nach Vertragsende

6. Technische und Organisatorische Maßnahmen (TOM)

6.1 Vertraulichkeit

- AES-256-Verschlüsselung at-rest
- TLS 1.3 minimum für alle Verbindungen
- Granulare Access-Control (Role-Based)
- 2-Faktor-Authentifizierung (2FA) Pflicht
- Need-to-Know-Prinzip für alle Mitarbeiter

6.2 Integrität

- WORM-Audit-Trail (7 Jahre Retention)
- Hash-Chain für Tamper-Proof
- Tägliche Backup-Verifikation

6.3 Verfügbarkeit

- 99.9% SLA (Service-Level-Agreement)
- Disaster-Recovery-Plan dokumentiert (RTO 4h, RPO 1h)
- Backups in 2 geografisch getrennten Schweizer Lokationen

6.4 Belastbarkeit

- DDoS-Protection
- Rate-Limiting auf API-Ebene
- Penetrationstest 2026 Q1 (Sanitized-Report auf Anfrage)

6.5 Wiederherstellung

- Quartalsweise Disaster-Recovery-Drills
- Recovery Time Objective (RTO): 4 Stunden
- Recovery Point Objective (RPO): 1 Stunde

6.6 Regelmäßige Überprüfung

- Externe Audits jährlich (geplant Q4 2026)
- Internal Security-Reviews monatlich
- ISO 27001 Audit (target Q4 2026)
- SOC 2 Type II (target Q1 2027)

7. Datenresidenz

Hosting **ausschließlich in der Schweiz** (Zürich primär + Genf sekundär). Keine Daten-Replikation in US/Asien. Anthropic-API-Calls erfolgen via EU-Region wo verfügbar.

8. EU AI Act Compliance

Sofern der Verantwortliche Scrutare's AI-Funktionen (High-Risk Annex III) nutzt, gelten zusätzlich:

- AI-System-Register dokumentiert
- Audit-Trail aller LLM-Calls (6 Monate Retention)
- Human-Oversight-Mechanismen aktiv
- Model-Cards verfügbar unter scrutare.ch/de/legal/ai-governance

9. Vertragsbeendigung

- 30 Tage Datenexport-Window nach Vertragsende
- Vollständige Löschung innerhalb 60 Tagen
- Schriftliche Löschungs-Bestätigung

10. Haftung

Beschränkungen gemäß Hauptvertrag. Für Datenpannen aufgrund grober Fahrlässigkeit oder Vorsatz uneingeschränkte Haftung gemäß OR Art. 99.

11. Schlussbestimmungen

- **Anwendbares Recht:** Schweizerisches Recht
- **Gerichtsstand:** Zürich
- **Schriftform:** Änderungen bedürfen Schriftform
- **Salvatorische Klausel:** Bei Unwirksamkeit einzelner Klauseln bleibt der Restvertrag wirksam

Kontakt

Datenschutzbeauftragter: dpo@scrutare.ch
Compliance: compliance@scrutare.ch
Aufsichtsbehörde: Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB), edoeb.admin.ch

Unterzeichnung:

_____

Verantwortlicher (Kunde)

_____

Auftragsverarbeiter (MProfi AG)