

SCRUTARE

Data Processing Agreement

DPA · revDSG + EU-GDPR Compliant

© 2026 MProfi AG · Version 1.0 · 2026-05-03

1. Subject Matter

This Data Processing Agreement (DPA) governs the processing of personal data by **MProfi AG** (hereinafter "Processor") under the Scrutare SaaS Agreement with the Customer (hereinafter "Controller") pursuant to Art. 9 revFADP (Switzerland) and Art. 28 GDPR.

2. Nature and Purpose of Processing

Area	Description
Purpose	Provision of Scrutare DD platform (document storage, AI analysis, IC memo generation, workstream workflow)
Data Categories	Target employee master data, LP contact data, deal documents, Q&A conversations
Data Subjects	Employees and stakeholders of the Target, LP representatives, GP team
Duration	SaaS contract term + 30 days data export window + 60 days deletion period

3. Sub-Processors

Sub-Processor	Purpose	Hosting	DPA
Hetzner Switzerland	Server hosting (primary)	CH (Zurich)	✓
Infomaniak	Backup hosting	CH (Geneva)	✓
Anthropic	AI document analysis	EU/US (with DPA)	✓
Mailjet	Transactional emails	EU (FR)	✓
Adyen	Payment processing	NL (EU)	✓

Sub-Processor changes will be communicated to the Controller 30 days in advance. Objection possible within 14 days.

4. Processor Obligations

- Process data only on documented Controller instructions
- Confidentiality obligation for all employees (NDA mandatory)
- Implement TOM per Section 6
- Support data subject access requests (revFADP Art. 25)
- Notify Controller of data breaches within **24 hours**

- Controller reports to FDPIC / DPA within 72 hours
- Audit right once per year with 30 days notice

5. Controller Rights

- Right to access and correction (revFADP Art. 25)
- Audit right (see Section 4)
- Sub-processor approval/objection right
- Data export in standardized format (CSV + JSON)
- Complete deletion after contract end

6. Technical and Organizational Measures (TOM)

6.1 Confidentiality

- AES-256 encryption at rest
- TLS 1.3 minimum for all connections
- Granular access control (role-based)
- 2-Factor authentication (2FA) mandatory
- Need-to-know principle for all employees

6.2 Integrity

- WORM audit trail (7-year retention)
- Hash-chain for tamper-proof
- Daily backup verification

6.3 Availability

- 99.9% SLA
- Documented disaster recovery plan (RTO 4h, RPO 1h)
- Backups in 2 geographically separated Swiss locations

6.4 Resilience

- DDoS protection
- API-level rate limiting
- Penetration test Q1 2026 (sanitized report on request)

6.5 Recovery

- Quarterly disaster recovery drills
- Recovery Time Objective (RTO): 4 hours
- Recovery Point Objective (RPO): 1 hour

6.6 Regular Review

- External audits annually (planned Q4 2026)
- Internal security reviews monthly
- ISO 27001 audit (target Q4 2026)
- SOC 2 Type II (target Q1 2027)

7. Data Residency

Hosting **exclusively in Switzerland** (Zurich primary + Geneva secondary). No data replication in US/Asia. Anthropic API calls via EU region where available.

8. EU AI Act Compliance

If the Controller uses Scrutare's AI features (High-Risk Annex III), additionally apply:

- AI System Register documented
- Audit trail of all LLM calls (6 months retention)
- Human oversight mechanisms active
- Model cards available at scrutare.ch/en/legal/ai-governance

9. Contract Termination

- 30 days data export window after contract end
- Complete deletion within 60 days
- Written deletion confirmation

10. Liability

Limitations per main contract. Unlimited liability for data breaches due to gross negligence or intent per Swiss Code of Obligations Art. 99.

11. Final Provisions

- **Governing Law:** Swiss law
- **Jurisdiction:** Zurich
- **Written form:** Amendments require written form
- **Severability:** Invalidity of individual clauses does not affect remaining contract

Contact

Data Protection Officer: dpo@scrutare.ch

Compliance: compliance@scrutare.ch

Supervisory Authority: Federal Data Protection and Information Commissioner (FDPIC), edob.admin.ch

Signature:

Controller (Customer)

Processor (MProfi AG)