

Auftragsverarbeitungsvertrag — Template

Rhyzon Hive · Modus Managed-Ops · Vertragspartner: innostett gmbh oder Winey GmbH

Stand: Juli 2026 (v3)

Bezug: Master-Vertrag §3

Quelle: rhyzon.ch/trust.html

Hinweis: Dieses Dokument ist ein **Template** für Vertragsverhandlungen. Es ist **nicht** unterschriftsreif. Vor erstem echten Vertragsschluss erfolgt anwaltliche Validierung. Eckige Klammern [...] markieren kundenspezifisch auszufüllende Felder. Bei Konflikten zwischen diesem Template und der finalen Fassung gilt die finale Fassung.

1. Vertragsparteien

Verantwortlicher (Controller):

[Kunde — Name, Adresse, vertretungsberechtigte Person, UID-Nr.]

Auftragsverarbeiter (Processor):

[innostett gmbh, Basel, CHE-470.237.325 | bzw. Winey GmbH, Liestal, CHE-211.342.368], Schweiz
Kontakt: info@rhyzon.ch

Dieser AVV ist Bestandteil des Master-Vertrags §3 und ergänzt diesen für den Modus Managed-Ops um die spezifischen Auftragsverarbeitungs-Klauseln.

2. Gegenstand und Dauer

Der Auftragsverarbeiter verarbeitet personenbezogene Daten im Auftrag des Verantwortlichen im Rahmen der Nutzung von **Rhyzon Hive** — einer KI-Wissensplattform mit Self-Hosted-Architektur (Single-Tenant by Design).

Dauer: entspricht der Vertragslaufzeit des Managed-Ops-Vertrags (Master-Vertrag §1 Option Ops).

3. Art und Zweck der Verarbeitung

Verarbeitungszweck	Beschreibung
Dokumenten-Indexierung	Extraktion, Embedding und Speicherung von Textinhalten aus Kundendokumenten
RAG-Suche	Vektorbasierte Suche in indexierten Dokumenten zur Beantwortung von Fragen

LLM-Verarbeitung	Weiterleitung von Prompts an LLM-Anbieter zur Generierung von Antworten
Chat-Routing	Entscheidung welche Aktion auf eine Chat-Nachricht folgt
Audit-Logging	Protokollierung aller KI-Operationen (append-only, ISAE-vorbereitet)

4. Kategorien betroffener Personen und Daten

Betroffene Personen: Mitarbeitende des Verantwortlichen (Hive-Nutzer); ggf. Endkunden des Verantwortlichen (wenn deren Daten in den verarbeiteten Dokumenten enthalten).

Datenkategorien: Name, E-Mail-Adresse, Rolle (Mitarbeitende); Inhalte von Dokumenten (können personenbezogene Daten Dritter enthalten); Chat-Nachrichten und Suchanfragen; Nutzungsprotokolle (Audit-Log).

5. Technische und organisatorische Massnahmen (TOM)

Verbindliche TOM gemäss Anhang *tom.md*: TLS 1.3 in Transit; Disk-Encryption auf Infomaniak-VM-Ebene; Fernet-Verschlüsselung der LLM-Credentials; physische Mandantentrennung pro Kunden-VM und -Datenbank (Single-Tenant), rollenbasierte Rechtentrennung innerhalb des Hives über PostgreSQL Row-Level-Security (RLS); append-only Audit-Trail; restic-Backups auf Infomaniak Swiss Backup mit Retention 7d/4w/3m; SSH-Zugang nur durch innostett/Winey-Operativ.

6. Sub-Auftragsverarbeiter

6.1 Echte Sub-Auftragsverarbeiter

Anbieter	Zweck	Standort
Infomaniak Network SA	VM-Hosting, Backup, LLM (Standard, ch_only-fähig)	Schweiz
Anthropic, PBC	LLM des MCP-Clients (Claude.ai / Claude Code) — Opt-in, nur bei ch_only=false	US / EU (Standardvertragsklauseln)

6.2 Connector-Drittdienste — keine Sub-AVV

Slack, Google Workspace (Gmail, Drive), Infomaniak kSuite (kMail, kDrive, kChat), Microsoft 365, Bexio/Glide u.a. ERP-/CRM-Systeme sind **keine** Sub-Auftragsverarbeiter, sondern Datenflussziele auf Anweisung des Verantwortlichen. Vertragsbeziehungen bestehen direkt zwischen Verantwortlichem und Drittdienst.

Änderungen bei echten Sub-AVV (6.1): Vorab-Information mit 30 Tagen Widerspruchsrecht.

7. Pflichten des Auftragsverarbeiters

1. Verarbeitung nur auf dokumentierte Weisung des Verantwortlichen
2. Vertraulichkeitsverpflichtung aller Mitarbeitenden
3. Umsetzung der TOM gemäss §5 und Anhang *tom.md*
4. Unterstützung bei Betroffenenrechten innerhalb von 72 Stunden nach Anfrage
5. Löschung aller Daten nach Vertragsende gemäss §11
6. Bereitstellung aller Informationen für Audits gemäss §10
7. Unverzügliche Meldung von Datenschutzverletzungen an den Verantwortlichen — spätestens binnen **48 Stunden** nach Kenntnisnahme

8. Pflichten des Verantwortlichen

1. Sicherstellung der Rechtsgrundlage für die Datenverarbeitung
2. Information der betroffenen Personen über die Verarbeitung durch den Auftragsverarbeiter
3. Rechtzeitige Mitteilung von Betroffenen-Anfragen
4. Meldung an die Aufsichtsbehörde (EDÖB / EU-Aufsicht), falls erforderlich, binnen 72 Stunden

9. Datentransfer in Drittländer

Standard(ch_only=true): Alle Daten verbleiben in der Schweiz. Kein Transfer in Drittländer.

Bei ch_only=false: Transfer an Anthropic (US / EU) auf Basis der EU-Standardvertragsklauseln (SCCs). Erfordert explizite Zustimmung des Verantwortlichen, konfiguriert pro KI-Mitarbeiter.

10. Audits

Der Verantwortliche hat das Recht, die Einhaltung dieses Vertrags zu überprüfen. Die Audit-Frist richtet sich nach dem Anlass:

10.1 Routine-Audit (planmässig)

- Einsicht in den Audit-Trail (Hive-Portal oder pg_dump): jederzeit selbständig durch den Verantwortlichen
- Vor-Ort-Audit: 10 Arbeitstage Voranmeldung
- Schriftliche Auskunft auf Anfrage: 10 Arbeitstage

10.2 Anlassbezogenes Audit (Datenschutzverletzung, Behörden-Anfrage, ISAE-Audit-Anfrage Drittauditor)

- Vor-Ort-Audit: 48 Stunden Voranmeldung; bei Sicherstellungspflicht (forensische Sofortmassnahmen) auch sofortig
- Schriftliche Auskunft: nach Incident-Response-Frist-Logik

Bei Konflikten zwischen Audit-Frist und laufender Incident-Response geht die Incident-Response vor.

11. Vertragsende und Datenlöschung

1. **Datenexport:** Vollständiger Export aller Kundendaten (pg_dump pro Schema) innerhalb 30 Tagen
2. **Löschung:** Alle Kundendaten werden gelöscht (Schema-DROP, VPS-Dekommissionierung)
3. **Backups:** Automatische Löschung nach Ablauf der Retention (max. 3 Monate)
4. **Audit-Log:** Der Audit-Trail liegt auf der VM des Kunden (Verantwortlicher). Der Auftragsverarbeiter garantiert Unveränderlichkeit während der Vertragsdauer und einen vollständigen, integren Export bei Vertragsende; die gesetzliche Aufbewahrung (OR Art. 958f, soweit auf diese Unterlagen anwendbar) obliegt durchgehend dem Verantwortlichen als Buchführungspflichtigem
5. **Löschbestätigung:** Schriftliche Bestätigung an den Verantwortlichen

12. Anwendbares Recht und Gerichtsstand

Schweizer Recht. Gerichtsstand: Basel-Stadt (für innostett gmbh) bzw. Liestal BL (für Winey GmbH). Lugano-Konvention für EU-Cross-Border-Sachverhalte. Art. 100 OR (zwingende Haftung für Vorsatz und grobe Fahrlässigkeit) bleibt unberührt.

13. Anlagen

- Anhang 1 — Technische und organisatorische Massnahmen (*tom.md*)
- Anhang 2 — Liste der Sub-Auftragsverarbeiter (Stand wie §6)
- Anhang 3 — Datenschutz-Folgenabschätzung (DPIA, falls erforderlich)
- Master-Vertrag §1–§6 (*lizenzvertrag.md*)

Verantwortlicher (Kunde)

Auftragsverarbeiter

Name, Funktion, Datum, Ort

[innostett gmbh / Winey GmbH] — Name, Funktion,
Datum, Ort