

Vertrag zur Auftragsverarbeitung

nach Art. 28 der Verordnung (EU) 2016/679 (DSGVO)

Fassung vom 27. Oktober 2026

zwischen

[Auftraggeber: Firma, Rechtsform, Anschrift, vertreten durch]

— nachfolgend „Verantwortlicher“ —

und

Tayfun Gülcan, Franz-Liszt-Straße 38, 38106 Braunschweig, Deutschland

— nachfolgend „Auftragsverarbeiter“ —

1. Gegenstand und Dauer

Der Auftragsverarbeiter erbringt für den Verantwortlichen den Dienst **Vryne** (Wissensbasis mit belegten Antworten, nachfolgend „Dienst“). Im Rahmen dieses Dienstes verarbeitet er personenbezogene Daten im Auftrag des Verantwortlichen. Dieser Vertrag gilt für die Dauer des Hauptvertrags über die Nutzung des Dienstes.

2. Art und Zweck der Verarbeitung

Verarbeitet werden die Inhalte, die der Verantwortliche in den Dienst einbringt, sowie die zu deren Betrieb erforderlichen Metadaten. Zweck ist ausschließlich die Bereitstellung des Dienstes: Speichern, Aufbereiten, Durchsuchen und Beantworten von Fragen auf Grundlage der eingebrachten Dokumente, Verwaltung von Konten, Rollen und Organisationen sowie die Abrechnung von Guthaben.

3. Kategorien personenbezogener Daten

- Bestands- und Kontaktdaten von Mitgliedern (Name, E-Mail-Adresse, Anzeigenname, optional Profilbild)
- Anmeldedaten (Sitzungskennung, Zeitstempel, IP-Adresse, Browserkennung)
- Inhaltsdaten aus hochgeladenen Dokumenten, Fragen, Antworten und Zitaten
- Nutzungsdaten (verbrauchte Credits, Aktivitätseinträge)
- Abrechnungsdaten (Bestellnummer, Produkt, Betrag — keine Zahlungsmittel)

Der Verantwortliche entscheidet, welche Inhalte er einbringt. Besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO sind nicht Gegenstand des Dienstes; ihre Verarbeitung ist nicht vorgesehen.

4. Kategorien betroffener Personen

Mitarbeitende und sonstige Nutzer des Verantwortlichen sowie Personen, deren Daten in eingebrachten Dokumenten enthalten sind.

5. Weisungsbindung

Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen, einschließlich der Übermittlung in ein Drittland, sofern nicht unions- oder mitgliedstaatliches Recht ihn zu einer anderen Verarbeitung verpflichtet. Ist eine solche Pflicht gegeben, teilt er dem Verantwortlichen die rechtlichen Anforderungen vor der Verarbeitung mit, sofern dies rechtlich zulässig ist.

Weisungen erteilt der Verantwortliche über die Administrationsoberfläche des Dienstes oder in Textform an support@vryne.com.

6. Vertraulichkeit

Der Auftragsverarbeiter verpflichtet alle Personen, die Zugang zu den Daten haben, zur Vertraulichkeit. Der Zugang ist auf Personen beschränkt, die ihn für die Erbringung des Dienstes benötigen.

7. Sicherheit der Verarbeitung (Art. 32 DSGVO)

Der Auftragsverarbeiter trifft die in **Anlage 1** beschriebenen technischen und organisatorischen Maßnahmen. Sie entsprechen dem Stand der Technik und werden fortlaufend überprüft. Änderungen dürfen das Schutzniveau nicht unterschreiten; wesentliche Änderungen dokumentiert der Auftragsverarbeiter.

8. Unterauftragsverhältnisse

Der Verantwortliche stimmt der Einbeziehung der in **Anlage 2** genannten Unterauftragsverarbeiter zu. Neue Unterauftragsverarbeiter kündigt der Auftragsverarbeiter mindestens 30 Tage vorher an; der Verantwortliche kann aus wichtigem Grund widersprechen. Ein Wechsel ist erst nach Ablauf der Frist oder nach Einigung zulässig. Der Auftragsverarbeiter verpflichtet Unterauftragsverarbeiter schriftlich auf dieselben Pflichten.

9. Unterstützung des Verantwortlichen

Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Erfüllung der Rechte betroffener Personen (Art. 15–21 DSGVO) sowie bei der Meldung von Verletzungen des Schutzes personenbezogener Daten (Art. 33, 34 DSGVO) und bei der Erstellung einer Datenschutz-Folgenabschätzung (Art. 35 DSGVO), soweit ihm die dafür nötigen Informationen vorliegen.

Der Verantwortliche kann Auskunft, Datenexport und die Löschung eines Kontos über support@vryne.com verlangen. Der Auftragsverarbeiter antwortet innerhalb eines Monats.

10. Löschung und Rückgabe

Nach Beendigung des Hauptvertrags stellt der Auftragsverarbeiter die Daten 30 Tage lang auf Anfrage zum Export bereit und löscht sie anschließend, sofern keine gesetzlichen Aufbewahrungspflichten entgegenstehen. Gelöschte Dokumente entfernen auch die zugehörigen Textabschnitte und Vektoren.

11. Kontrollrechte

Der Verantwortliche ist berechtigt, die Einhaltung dieses Vertrags zu überprüfen. Der Auftragsverarbeiter beantwortet dazu Auskunftersuchen und stellt die in Anlage 1 beschriebenen Maßnahmen dar. Ein Vor-Ort-Termin ist nach Voranmeldung mit angemessener Frist möglich; er darf den laufenden Betrieb nicht beeinträchtigen.

12. Drittlandübermittlung

Dokumente, Fragen, Antworten und Vektoren verarbeitet der Auftragsverarbeiter ausschließlich in Rechenzentren in Deutschland. Der Mailversand erfolgt vorübergehend über **Resend** (Vereinigte Staaten) auf Grundlage der Standardvertragsklauseln nach Art. 46 Abs. 2 lit. c DSGVO; übermittelt werden nur Empfängeradresse und Nachrichtentext, nie Dokumentinhalte. Der Auftragsverarbeiter ersetzt diesen Baustein durch einen Anbieter in der Europäischen Union und kündigt dies 30 Tage vorher an.

13. Haftung

Es gilt die Haftungsregelung des Hauptvertrags. Die Haftung nach Art. 82 DSGVO bleibt unberührt.

14. Schlussbestimmungen

Es gilt deutsches Recht. Ausschließlicher Gerichtsstand ist Braunschweig, soweit der Verantwortliche Kaufmann, juristische Person des öffentlichen Rechts oder öffentlich-rechtliches Sondervermögen ist. Änderungen bedürfen der Textform. Sollte eine Bestimmung unwirksam sein, bleibt der übrige Vertrag wirksam.

Ort, Datum:

Verantwortlicher

Tayfun Gülcan — Auftragsverarbeiter

Anlage 1 — Technische und organisatorische Maßnahmen

Zugriffskontrolle. Jede Anfrage wird serverseitig geprüft. Aktionen laufen über Berechtigungen, die an die Organisation und die Rolle gebunden sind; jede Datenbankabfrage filtert auf die aktive Organisation. Die Rolle wird bei jedem Request gegen die Mitgliedertabelle geprüft, nicht aus dem Client übernommen.

Mandamententrennung. Dokumente, Textabschnitte, Chats und Vektoren gehören je genau einer Organisation. Die Trennung ist an jeder Lesestelle umgesetzt und wird durch automatisierte Tests gegen eine echte Datenbank überprüft.

Weitergabekontrolle. Transportverschlüsselung über TLS. Die Anwendung antwortet ausschließlich über HTTPS; HSTS ist mit einer Gültigkeit von einem Jahr gesetzt. Der Zugriff auf die

Dokumentenablage erfolgt über signierte, organisierte Schlüsselpfade (org/<id>/), die nicht aus Nutzereingaben gebaut werden.

Verfügbarkeitskontrolle. Überwachte Infrastruktur mit automatischer Neustartlogik, tägliche Sicherung der Datenbank durch den Hosting-Dienstleister, keine Replikation in Regionen außerhalb Deutschlands. Eine öffentliche Statusseite und ein Health-Endpunkt messen Datenbank, Warteschlange, Dokumentenablage und Suche live. Zugesagte Verfügbarkeit: 99,5 % pro Kalendermonat, geplante Wartung ausgenommen.

Trennungskontrolle. Zugänge sind personenbezogen; es gibt keine gemeinsamen Konten. Sitzungen laufen nach sieben Tagen ohne Nutzung ab, Anmeldelinks nach 90 Minuten. Einmal-Links sind an die hinterlegte Adresse gebunden.

Integrität. Änderungen an Dokumenten und Einstellungen werden im Aktivitätsprotokoll festgehalten. Sicherungskopien werden turnusmäßig überschrieben; Wiederherstellungen werden stichprobenartig geprüft.

Datensparsamkeit. Die Anwendung verarbeitet nur die für den Dienst nötigen Daten. Es gibt keine Werbe- oder Profiling-Cookies; die Reichweitenmessung arbeitet cookielos über einen EU-Endpunkt und ist abschaltbar.

Organisation. Sicherheitsrelevante Abhängigkeiten werden regelmäßig aktualisiert; Schwachstellenmeldungen werden innerhalb von drei Werktagen bestätigt. Ein Sicherheitsvorfall mit Auswirkung auf die Daten des Verantwortlichen wird diesem unverzüglich mitgeteilt.

Anlage 2 — Unterauftragsverarbeiter

Dienstleister	Sitz	Zweck	Ort der Verarbeitung
Sliplane	Berlin, Deutschland	Hosting von Anwendung, Datenbank, Ablage, Suchinstanz	Falkenstein, Deutschland
Melious	Europäische Union	Inferenz-Gateway für Sprachmodelle	Deutschland
CopeCart	Berlin, Deutschland	Zahlungsabwicklung und Rechnungstellung	Berlin, Deutschland
Fathom	Europäische Union	Cookielose Reichweitenmessung	EU (EU-Endpunkt)
Resend	USA	Versand von Anmeldelinks, Einladungen, Kaufbestätigungen	USA — vorübergehend

Alle Dienstleister sind vertraglich nach Art. 28 DSGVO gebunden. Für Resend gelten die Standardvertragsklauseln nach Art. 46 Abs. 2 lit. c DSGVO.