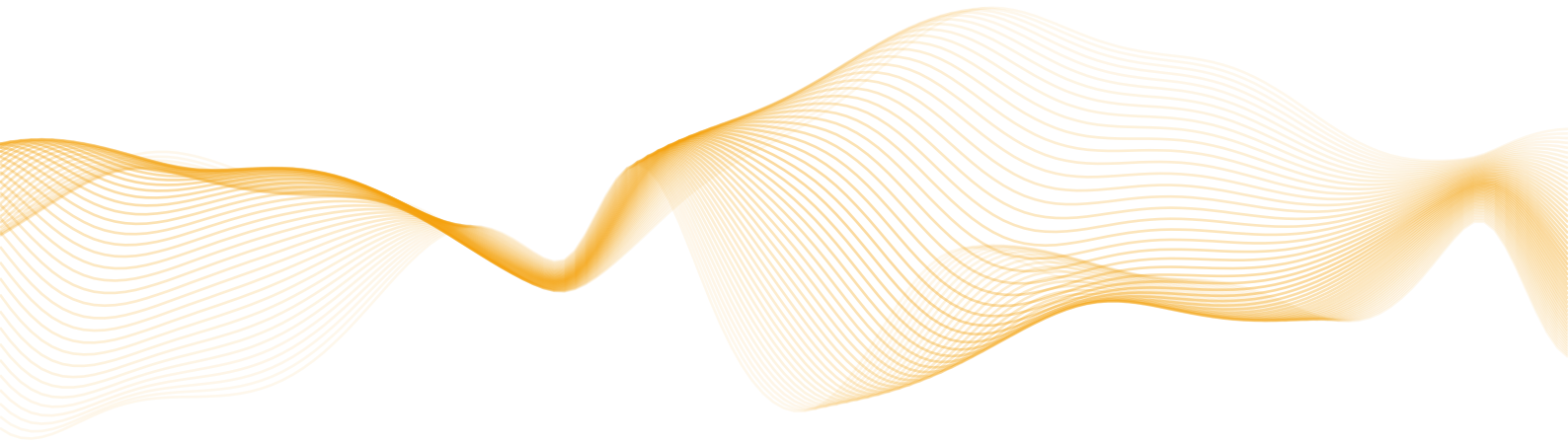
techtropy

# Auftragsverarbeitungsvertrag



Kunde (Verantwortlicher)

Organisation

Adresse

Auftragsverarbeiter

techtropy GmbH
Am Anger 1
87672 Roßhaupten
Amtsgericht Kempten (Allgäu)
HRB 19212

Fassung vom

21. November 2026

Dies ist der Vertrag über die Auftragsverarbeitung nach Art. 28 DSGVO („Vertrag“) zwischen dem Kunden im Sinne der Nutzungsbedingungen als Verantwortlichem („Kunde“) und der techtropy GmbH, Am Anger 1, 87672 Roßhaupten als Auftragsverarbeiter („wir“). „Dienst“ und „Organisation“ haben die Bedeutung, die ihnen die Nutzungsbedingungen geben. „Nutzer“ im Sinne dieses Vertrags sind die Mitglieder der Organisation des Kunden und die Personen, die er einlädt. Handelt ein Agent mit dem Agentenschlüssel eines Nutzers, gilt das als Handeln dieses Nutzers (3.6). Der Kunde ist Verantwortlicher für die personenbezogenen Daten, die seine Nutzer in den Dienst einstellen und die dort über sie entstehen, soweit nicht nach 2.1 wir Verantwortlicher sind.

# 1 Geltung

1.1 Dieser Vertrag ist Bestandteil der Nutzungsbedingungen (https://techtropy.com/de/nutzungsbedingungen). Er gilt für jeden Kunden, für den wir personenbezogene Daten im Auftrag verarbeiten.

1.2 Dieser Vertrag kommt in einem elektronischen Format zustande (Art. 28 Abs. 9 DSGVO), wenn eine vertretungsberechtigte Person die Nutzungsbedingungen für den Kunden annimmt.

1.3 Widersprechen sich dieser Vertrag und die Nutzungsbedingungen beim Datenschutz, gilt dieser Vertrag. Im Übrigen gelten die Nutzungsbedingungen, auch für anwendbares Recht, Gerichtsstand und Änderungen dieses Vertrags.

1.4 Die Anlagen 1 bis 6 sind Bestandteil dieses Vertrags.

# 2 Rollen

2.1 Für die Konten der Nutzer, Server-Logdateien, Seitenstatistik, E-Mail-Protokoll und Supportanfragen sind wir selbst Verantwortlicher, wie die Datenschutzerklärung (https://techtropy.com/de/datenschutzerklaerung) beschreibt. Die Mitgliedschaft eines Nutzers in der Organisation des Kunden sowie die Rollen und die Inhalte dieses Nutzers verarbeiten wir im Auftrag.

2.2 Eine gemeinsame Verantwortlichkeit nach Art. 26 DSGVO besteht nicht.

# 3 Weisungen

3.1 Wir verarbeiten die Daten, für die der Kunde verantwortlich ist, nur, um den Dienst zu betreiben, und nur auf dokumentierte Weisung des Kunden.

3.2 Weisungen erteilt der Kunde (a) über die Einstellungen des Dienstes, (b) durch die Nutzung der Funktionen des Dienstes und (c) in Textform durch seine Administratoren an die in Abschnitt 14 genannte Adresse.

3.3 Als angewiesen gilt auch die Verarbeitung, die erforderlich ist, um die bestellten Produkte einzurichten, die Nutzer des Kunden zu unterstützen und die Sicherheit des Dienstes zu gewährleisten.

3.4 Mehraufwand durch Weisungen, Überprüfungen oder Unterstützung, der über den Betrieb des Dienstes hinausgeht, vergütet uns der Kunde angemessen, sofern wir den Mehraufwand nicht zu vertreten haben.

3.5 Ruft ein Nutzer des Kunden eine KI-Funktion auf, weist uns der Kunde damit an, den Text an den Unterauftragsverarbeiter zu übermitteln, den Anlage 3 für KI-Funktionen nennt und der in einem Drittland sitzt.

3.6 Was ein Nutzer des Kunden über einen Agentenschlüssel oder eine verbundene App liest oder ändert, ist eine Verarbeitung auf Weisung des Kunden, wie die Nutzung des Dienstes durch den Nutzer selbst. Die App ist nicht unser Unterauftragsverarbeiter.

3.7 Für die Rechtmäßigkeit der Verarbeitung und die Wahrung der Rechte der betroffenen Personen ist der Kunde verantwortlich, und er informiert sie nach Art. 13 und 14 DSGVO.

3.8 Die Anlagen 4 und 5 ergänzen Weisungen je Art des Kunden.

3.9 Verpflichtet uns das Recht der Union oder eines Mitgliedstaats, dem wir unterliegen, zu einer anderen Verarbeitung, teilen wir dem Kunden diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

3.10 Sind wir der Auffassung, dass eine Weisung gegen die DSGVO oder andere Datenschutzvorschriften der Union oder der Mitgliedstaaten verstößt, informieren wir den Kunden unverzüglich. Wir dürfen die Ausführung der Weisung aussetzen, bis der Kunde sie bestätigt oder ändert.

## 4 Anonyme Statistiken

Der Kunde weist uns an, aus den Daten des Planspiels anonymisierte, zusammengefasste Auswertungen zu bilden, die weder eine Person noch den Kunden erkennen lassen.

## 5 Vertraulichkeit und Zugriff

5.1 Alle, die wir zur Verarbeitung ermächtigen, sind zur Vertraulichkeit verpflichtet.

5.2 Nur benannte Mitglieder unseres Teams können eine Organisation öffnen. Jeden solchen Zugriff protokollieren wir mit Person, Zeitpunkt und Vorgang, bewahren das Protokoll 365 Tage auf und zeigen es den Administratoren der Organisation.

## 6 Unterauftragsverarbeiter

6.1 Der Kunde erlaubt uns allgemein, die in Anlage 3 genannten Unterauftragsverarbeiter einzusetzen. Jeder von ihnen ist durch einen Vertrag an Datenschutzpflichten gebunden, die den unseren aus diesem Vertrag inhaltlich entsprechen (Art. 28 Abs. 4 DSGVO). Für ihre Pflichterfüllung haften wir gegenüber dem Kunden.

6.2 Außer in den Fällen der Anlage 3 verarbeiten wir die Daten nur in der Europäischen Union oder im Europäischen Wirtschaftsraum. Eine weitere Übermittlung in ein Drittland erlaubt der Kunde über das Verfahren für neue Unterauftragsverarbeiter, und sie erfolgt nur nach Kapitel V DSGVO.

6.3 Nebenleistungen ohne konkreten Bezug zum Dienst, etwa Telekommunikation, Post und Transport oder Wartung, sind keine Unterauftragsverarbeitung. Auch dort wahren wir die Vertraulichkeit.

6.4 Wollen wir einen Unterauftragsverarbeiter hinzufügen oder ersetzen, teilen wir das den Administratoren des Kunden mindestens 30 Tage vorher per E-Mail mit.

6.5 Der Kunde kann bis zum Wirksamwerden aus einem sachlichen datenschutzrechtlichen Grund widersprechen und nennt ihn dabei. Finden wir dann keine zumutbare Lösung, kann jede Seite die betroffenen Produkte zum Wirksamwerden kündigen. Vorausbezahlte Entgelte erstatten wir in diesem Fall anteilig.

## 7 Sicherheit

7.1 Wir treffen die technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO, die Anlage 2 beschreibt.

7.2 Wir dürfen die Maßnahmen ändern, solange ihr Schutzniveau nicht sinkt. Auf Anfrage erläutern wir sie dem Kunden vertraulich näher.

7.3 Sicherungen nennt Anlage 6.

## 8 Sicherheitsvorfälle

8.1 Erfahren wir von einer Verletzung des Schutzes der Daten, für die der Kunde verantwortlich ist, informieren wir seine Administratoren unverzüglich, spätestens innerhalb von 48 Stunden, per E-Mail. Die Mitteilung enthält, soweit bekannt, die Angaben nach Art. 33 Abs. 3 DSGVO, und wir ergänzen sie, sobald wir mehr wissen.

8.2 Behörden und betroffene Personen informieren wir nur auf Weisung des Kunden.

8.3 Wir unterstützen den Kunden bei seinen Pflichten nach Art. 32 bis 36 DSGVO, soweit uns die Angaben vorliegen.

## 9 Rechte der betroffenen Personen

9.1 Wir unterstützen den Kunden mit geeigneten Maßnahmen dabei, die Anfragen betroffener Personen nach Art. 15 bis 22 DSGVO zu beantworten.

9.2 Eine Anfrage, die uns direkt erreicht, leiten wir unverzüglich an den Kunden weiter und beantworten sie nicht selbst. Dasselbe gilt für Anfragen von Behörden und Dritten zu den Daten, für die der Kunde verantwortlich ist, soweit das Recht es erlaubt.

# 10 Überprüfung und Nachweis

10.1 Wir geben dem Kunden die Angaben, die er braucht, um die Einhaltung der Pflichten aus Art. 28 DSGVO und diesem Vertrag nachzuweisen.

10.2 Wir ermöglichen Überprüfungen durch den Kunden oder einen von ihm beauftragten Prüfer, der zur Vertraulichkeit verpflichtet ist, und wirken daran mit.

10.3 Eine Überprüfung wird mindestens 14 Tage vorher angekündigt und findet zu unseren Geschäftszeiten und ohne konkreten Anlass maximal einmal im Jahr statt. Sie darf den Dienst nicht stören und keine Daten anderer Kunden erreichen.

10.4 Soweit ein aktueller Prüfbericht oder eine Zertifizierung, auch unseres Hosting-Anbieters, die Frage beantwortet, genügt dieser Nachweis.

# 11 Haftung

11.1 Im Verhältnis zum Kunden haften wir nicht für Schäden, die darauf beruhen, dass wir eine Weisung des Kunden befolgt haben, sofern wir unserer Hinweispflicht nach 3.10 nachgekommen sind. Unsere unbeschränkte Haftung nach den Nutzungsbedingungen, insbesondere bei Vorsatz, grober Fahrlässigkeit und der Verletzung von Leben, Körper oder Gesundheit, bleibt unberührt. Im Übrigen gilt die Haftungsbeschränkung der Nutzungsbedingungen.

11.2 Die Haftung gegenüber betroffenen Personen nach Art. 82 DSGVO bleibt unberührt.

# 12 Rückgabe und Löschung

12.1 Wird eine Organisation gelöscht oder endet die Verarbeitung, kann der Kunde bis 30 Tage danach die Rückgabe seiner Daten in einem gängigen, maschinenlesbaren Format verlangen. Danach löschen wir die Daten mit allen Kopien, sofern uns das Gesetz nicht zur Aufbewahrung verpflichtet. Sicherungskopien folgen innerhalb von 7 Tagen.

12.2 Die Löschung bestätigen wir auf Anfrage.

12.3 Löscht ein Nutzer sein eigenes Konto, bleiben seine Beiträge beim Kunden.

# 13 Sprache

Dieser Vertrag liegt in deutscher und englischer Sprache vor. Bei Abweichungen oder Auslegungszweifeln ist allein die deutsche Fassung maßgeblich.

# 14 Kontakt

Adresse für diesen Vertrag und für Fragen zu dieser Seite: dpa@techtropy.com.

# A1 Anlage 1 zur Verarbeitung

A1.1 Gegenstand ist der Betrieb des Dienstes für den Kunden in den Produkten, die er bestellt hat.

A1.2 Wir speichern die Daten, rechnen mit ihnen, zeigen sie an und übermitteln sie an die Personen, die der Kunde berechtigt.

A1.3 Zweck ist die Zusammenarbeit der Nutzer des Kunden, die Durchführung seiner Seminare und Planspiele und die Unterstützung des Kunden durch unser Team.

A1.4 Die Verarbeitung dauert, bis die Daten nach diesem Vertrag zurückgegeben oder gelöscht sind.

A1.5 Betroffene Personen sind die Nutzer des Kunden und Personen, die in seinen Inhalten vorkommen.

A1.6 Die Daten sind Name, E-Mail-Adresse, die Berechtigungen je Produkt, die Teams und die erstellten Inhalte einschließlich hochgeladener Dokumente. Im Planspiel kommen die Züge, die aktuelle Seite jeder Person und die Dauer je Seite hinzu.

A1.7 Besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO sind nicht Gegenstand des Dienstes, und der Kunde bringt sie nicht ein.

# A2 Anlage 2 zu den technischen und organisatorischen Maßnahmen

A2.1 Verbindungen zum Dienst über öffentliche Netze sind mit TLS 1.3 verschlüsselt, für ältere Clients mit TLS 1.2 und Forward Secrecy, und nutzen einen hybriden Post-Quanten-Schlüsselaustausch, wo der Client ihn unterstützt. Auch die Datenbank erreicht der Dienst über TLS 1.3, und Server und Datenbanken sind aus dem Internet nicht direkt erreichbar.

A2.2 Die Datenträger mit der Datenbank, dem Dateispeicher und den Containern sind mit LUKS2 und AES-256 im XTS-Modus verschlüsselt, und die Schlüssel zum Entsperren liegen getrennt von diesen Datenträgern. Das schützt die Daten, wenn ein Datenträger oder eine Kopie davon den Server verlässt, aber nicht vor dem Hosting-Anbieter oder einem Zugriff auf den laufenden Server.

A2.3 Supportanfragen sind zusätzlich in der Anwendung mit AES-256-GCM unter einem eigenen Schlüssel der Organisation verschlüsselt, sodass eine Kopie der Datenbank allein sie nicht offenlegt.

A2.4 Die Anmeldung läuft über Einmalcodes per E-Mail, deren Versand und Prüfung wir begrenzen, und Rollen und Berechtigungen bestimmen, was eine Person sieht und ändern darf.

A2.5 Mitglieder unseres Teams melden sich zusätzlich mit einem zweiten Faktor an, und ihre Zugriffsrechte sind nach Aufgaben getrennt.

A2.6 Jeden Zugriff unseres Teams auf eine Organisation protokollieren wir nach 5.2.

A2.7 Der Dienst greift auf die Datenbank mit einer Rolle zu, die Daten lesen und schreiben, aber die Struktur der Datenbank nicht ändern darf.

A2.8 Die Anwendungen laufen in gehärteten Containern ohne Administratorrechte und mit schreibgeschütztem Dateisystem.

A2.9 Agentenschlüssel, OAuth-Token und Einladungstoken speichern wir nur als Hashwert.

A2.10 Daten sind je Organisation getrennt, und jede Abfrage ist auf die Organisationen der anfragenden Person begrenzt.

A2.11 Der Server prüft Eingaben gegen festgelegte Schemas, bevor er sie verarbeitet.

A2.12 Jede Änderung der Datenbankstruktur proben wir vor der Auslieferung an einer Kopie der Datenbank, und vor einer solchen Auslieferung sichern wir die Datenbank zusätzlich.

A2.13 Die täglichen Sicherungen nach Anlage 6 bewahrt dataforest in Frankfurt auf.

A2.14 Wie wir Datenbank und Dateispeicher wiederherstellen, ist schriftlich festgelegt.

A2.15 Wir prüfen die Erreichbarkeit des Dienstes jede Minute und werden bei einem Ausfall per E-Mail benachrichtigt.

A2.16 Besuche im Planspiel und Zugriffsprotokolle löscht der Dienst automatisch nach den Fristen in der Datenschutzerklärung.

A2.17 Aus Logs entfernen wir Geheimnisse, Token und Cookies, und E-Mail-Adressen erscheinen nur maskiert. Warnungen und Fehler des Dienstes, die wir 30 Tage aufbewahren, enthalten keine IP-Adressen.

A2.18 Unser Hosting-Anbieter dataforest GmbH betreibt ein nach ISO/IEC 27001 zertifiziertes Informationssicherheits-Managementsystem (TÜV Saarland) und Rechenzentren in Frankfurt am Main.

A2.19 Bei jeder Änderung prüfen wir die Abhängigkeiten und bei jeder Auslieferung die Container-Images automatisch auf bekannte Schwachstellen. Vor einer Veröffentlichung, die Anmeldung oder Zugriffsrechte berührt, prüfen wir die Änderungen gesondert auf ihre Sicherheit.

## A3 Anlage 3 zu den Unterauftragsverarbeitern

A3.1 dataforest GmbH, Kriftel, Deutschland. Hosting unserer Server in Rechenzentren in Frankfurt, Deutschland.

A3.2 AhaSend B.V., Amsterdam, Niederlande. Versand von E-Mails, verarbeitet in der Europäischen Union.

A3.3 OpenRouter Inc., New York, USA. Leitet Text an den Anbieter des genutzten KI-Modells weiter, wenn ein Nutzer eine KI-Funktion aufruft. Die Modellanbieter sind weitere Unterauftragsverarbeiter von OpenRouter. OpenRouter wählt und wechselt sie und bindet sie durch Vertrag an Datenschutzpflichten, die den eigenen entsprechen (Art. 28 Abs. 4 DSGVO). Die Modellanbieter können in den USA oder einem anderen Drittland sitzen. Wir lassen jeden Aufruf nur an Anbieter leiten, die den Text nach der Verarbeitung nicht aufbewahren, außer soweit gesetzlich vorgeschrieben oder zur Abwehr von Missbrauch, und nicht zum Training nutzen. Welche Anbieter das derzeit sind, zeigt OpenRouter unter Provider Logging (https://openrouter.ai/docs/guides/privacy/provider-logging). Der Kunde ist damit einverstanden, dass ein Wechsel unter diesen Modellanbietern durch die dort veröffentlichte Liste mitgeteilt wird. Er kann einem Modellanbieter jederzeit aus einem sachlichen datenschutzrechtlichen Grund widersprechen. 6.5 Satz 2 und 3 gelten dann entsprechend, und die Kündigung wirkt mit ihrem Zugang. Für OpenRouter selbst gelten 6.4 und 6.5. Die Übermittlung beruht auf den Standardvertragsklauseln der Europäischen Kommission (Art. 46 Abs. 2 lit. c DSGVO).

A3.4 Proton AG, Plan-les-Ouates, Schweiz. Postfächer unserer E-Mail-Adressen, etwa der Adresse in Abschnitt 14. Daten, für die der Kunde verantwortlich ist, verarbeitet Proton nur, soweit eine Nachricht an eine oder von einer dieser Adressen solche Daten enthält, etwa die Weisung eines Administrators oder die Anfrage einer betroffenen Person, die wir an den Kunden weiterleiten. Das betrifft Namen und E-Mail-Adressen der schreibenden und der genannten Personen sowie den Inhalt der Nachricht. Proton speichert die Nachrichten auf eigenen Servern in der Schweiz, in Deutschland oder in Norwegen. Für die Schweiz beruht die Übermittlung auf der Entscheidung 2000/518/EG der Kommission vom 26. Juli 2000, die dort ein angemessenes Schutzniveau feststellt und nach Art. 45 Abs. 9 DSGVO in Kraft bleibt.

## A4 Anlage 4 für Geschäftskunden

A4.1 Diese Anlage gilt für Kunden, die den Dienst als Geschäftskunden nutzen, wie für ihre Organisation festgehalten.

A4.2 Die Personen derselben Simulation sehen, auf welcher Seite die anderen gerade sind und ob sie untätig geworden sind, und die Simulation zeichnet Seitenaufrufe und Züge je Person auf.

A4.3 Die Zeit je Seite sieht nur eine Moderation, die der Kunde einsetzt, je Person oder nur je Unternehmen, wie der Kunde es in den Einstellungen seiner Organisation festlegt.

A4.4 Besteht ein Betriebsrat, holt der Kunde dessen Zustimmung ein, bevor er die Zeit je Seite personenbezogen auswertet (§ 87 Abs. 1 Nr. 6 BetrVG).

A4.5 Der Kunde nutzt den Dienst nicht, (a) um Beschäftigte oder Bewerbende einzustellen, auszuwählen, zu beurteilen oder zu überwachen oder (b) um über ihr Arbeitsverhältnis, ihre Aufgaben, ihre Beförderung oder ihre Kündigung zu entscheiden.

# A5 Anlage 5 für Bildungseinrichtungen

A5.1 Diese Anlage gilt für Hochschulen, Business Schools und andere Kunden, die den Dienst in der Lehre nutzen, wie für ihre Organisation festgehalten.

A5.2 Im Planspiel legt der Kunde in den Einstellungen seiner Organisation fest, ob die Spielleitung die Zeit je Seite für jede Person sieht oder nur die Summe je Unternehmen.

A5.3 Soweit erforderlich, holt der Kunde die Zustimmung des Betriebsrats oder Personalrats ein, bevor er die Zeit je Seite personenbezogen auswertet (§ 87 Abs. 1 Nr. 6 BetrVG oder die entsprechende Vorschrift des Personalvertretungsrechts).

# A6 Anlage 6 zu den Instanzen

A6.1 Die Daten einer Organisation liegen auf der gemeinsamen Instanz des Dienstes oder, wenn vereinbart, auf einer dedizierten Instanz mit eigener Datenbank und eigenem Dateispeicher. Kopien davon halten nur die Sicherungen.

A6.2 dataforest sichert jede Instanz täglich und bewahrt die letzten 7 Sicherungen auf.

A6.3 Eine Sicherung dient allein der Wiederherstellung der Instanz.

A6.4 Eine Instanz meldet uns nur Betriebssummen, die keine Person nennen und keinen Inhalt einer Organisation enthalten.

# Annahme

Dieser Vertrag kommt in einem elektronischen Format im Dienst zustande. Diese Felder dienen Ihren eigenen Unterlagen und ersetzen das nicht.

| Kunde (Verantwortlicher) | Auftragsverarbeiter |
| --- | --- |
| | techtropy GmbH |
| Organisation | Organisation |
| | |
| Ort, Datum | Ort, Datum |
| | |
| Unterschrift | Unterschrift |
| | |
| Name und Funktion in Druckschrift | Name und Funktion in Druckschrift |