Auftragsbearbeitungsvertrag (AVV / DPA) JuristerAI

Version: 1.0
Gültig ab: 1. Juni 2026
Anbieterin: Smart Process AG
Marke: JuristerAI
Webseite: jurister.ai

1. Vertragspartnerin

Vertragspartnerin des Kunden ist:

Smart Process AG
Lattenhofweg 4
8640 Rapperswil
Schweiz

JuristerAI ist eine Marke der Smart Process AG.

Dieser Auftragsbearbeitungsvertrag («AVV» / «DPA») regelt die Bearbeitung von Personendaten durch Smart Process AG im Rahmen der Nutzung von JuristerAI. Der Kunde ist Verantwortlicher für die von ihm in JuristerAI eingebrachten Personendaten. Smart Process AG handelt als Auftragsbearbeiterin und bearbeitet diese Daten im Auftrag des Kunden.

2. Gegenstand und Dauer der Bearbeitung

Gegenstand der Bearbeitung ist die Bereitstellung, der Betrieb, die Wartung, die Sicherung und der Support der JuristerAI-Plattform.

Die Dauer der Bearbeitung richtet sich nach der Dauer des Vertrags über die Nutzung von JuristerAI sowie nach allfälligen gesetzlichen oder vertraglichen Aufbewahrungs-, Rückgabe- und Löschfristen.

3. Art und Zweck der Bearbeitung

Die Bearbeitung dient der Bereitstellung der JuristerAI-Plattform und der Erbringung der gebuchten Produktmodule, insbesondere Transkription, Dokumentenaufbereitung, Fallanalyse, Suche, Chat, Quellenangaben, Benutzerverwaltung, Sicherheit, Support, Abrechnung, Produkt-Analytics und Datenexport.

Details finden sich in Anhang 1.

4. Weisungsbindung

Smart Process AG bearbeitet Personendaten nur gemäss Vertrag, dokumentierten Weisungen des Kunden und anwendbarem Recht.

Dies gilt auch für allfällige Übermittlungen in ein Drittland oder an eine internationale Organisation. Solche Übermittlungen erfolgen nur nach dokumentierter Weisung des Kunden oder soweit sie nach anwendbarem Recht zulässig sind.

Die im Vertrag, in den AGB, in diesem AVV und in der Plattformnutzung angelegten Bearbeitungen gelten als dokumentierte Weisungen des Kunden.

Ist Smart Process AG der Ansicht, dass eine Weisung gegen anwendbares Datenschutzrecht oder sonstiges Recht verstösst, informiert Smart Process AG den Kunden, soweit dies rechtlich zulässig ist.

5. Verantwortung des Kunden

Der Kunde bleibt verantwortlich für die Rechtmässigkeit der Bearbeitung der von ihm in JuristerAI eingebrachten Daten. Dies umfasst insbesondere die Berechtigung zur Bearbeitung und Übermittlung von Mandats-, Fall-, Audio-, Dokumenten-, Behörden- und Personendaten an JuristerAI.

Der Kunde bleibt zudem verantwortlich für die Einhaltung der für ihn geltenden Berufs-, Amts-, Datenschutz- und Geheimhaltungspflichten sowie für allfällige interne Freigaben, Weisungen oder Einwilligungen.

6. Vertraulichkeit

Smart Process AG stellt sicher, dass Personen mit Zugriff auf Kundendaten zur Vertraulichkeit verpflichtet sind oder einer angemessenen gesetzlichen Vertraulichkeitspflicht unterstehen.

Die Vertraulichkeitspflichten erfassen insbesondere Mandats-, Fall- und Behördendaten sowie Informationen, die einem Berufs-, Amts- oder sonstigen Geheimhaltungsschutz unterliegen können.

Zugriffe auf Kundendaten erfolgen nur, soweit dies für Betrieb, Sicherheit, Support, Fehlerbehebung oder vertraglich vereinbarte Leistungen erforderlich ist.

7. Technische und organisatorische Massnahmen

Smart Process AG trifft angemessene technische und organisatorische Massnahmen zum Schutz der Kundendaten. Die Massnahmen sind in Anhang 2: Technische und organisatorische Massnahmen beschrieben.

Die Massnahmen werden risikobasiert umgesetzt und weiterentwickelt. Dabei werden insbesondere Vertraulichkeit, Integrität, Verfügbarkeit, Nachvollziehbarkeit, Mandantentrennung, Zugriffskontrolle und Schweizer Datenhaltung berücksichtigt.

8. Unterauftragsbearbeiter

Smart Process AG darf Unterauftragsbearbeiter einsetzen, soweit diese in Anhang 3 aufgeführt sind oder der Kunde allgemein oder spezifisch zugestimmt hat.

Smart Process AG verpflichtet Unterauftragsbearbeiter vertraglich zu Datenschutz-, Sicherheits- und Vertraulichkeitspflichten, die den Pflichten aus diesem AVV im Wesentlichen entsprechen.

Smart Process AG informiert den Kunden über wesentliche Änderungen bei Unterauftragsbearbeitern. Der Kunde kann aus berechtigten Datenschutzgründen widersprechen. Erfolgt ein berechtigter Widerspruch und ist keine zumutbare Alternative möglich, können die Parteien die betroffene Leistung nach den vertraglichen Regelungen beenden.

9. Unterstützung des Kunden

Smart Process AG unterstützt den Kunden im angemessenen Umfang bei der Erfüllung datenschutzrechtlicher Pflichten, soweit dies die Bearbeitung durch JuristerAI betrifft und Smart Process AG über die dafür erforderlichen Informationen verfügt.

Dazu gehören insbesondere die Unterstützung bei Anfragen betroffener Personen, Datenexport, Löschung, Berichtigung, Einschränkung der Bearbeitung, Sicherheitsvorfällen sowie, soweit anwendbar, bei Datenschutz-Folgenabschätzungen oder Konsultationen mit Aufsichtsbehörden.

Die Unterstützung erfolgt nach den verfügbaren Funktionen der Plattform, den vereinbarten Supportprozessen und den Regelungen dieses Vertrags.

10. Sicherheitsvorfälle

Smart Process AG informiert den Kunden unverzüglich über Sicherheitsvorfälle, die Kundendaten betreffen, sobald Smart Process AG davon Kenntnis erlangt.

Die Mitteilung enthält, soweit verfügbar, Art des Vorfalls, betroffene Daten, mögliche Auswirkungen und ergriffene oder vorgeschlagene Massnahmen.

Smart Process AG unterstützt den Kunden im angemessenen Umfang bei der Erfüllung gesetzlicher Melde- oder Informationspflichten, soweit diese den Sicherheitsvorfall und die Bearbeitung durch JuristerAI betreffen.

11. Rückgabe und Löschung

Nach Vertragsende werden Kundendaten nach Wahl des Kunden zurückgegeben oder gelöscht, sofern keine gesetzlichen Pflichten oder berechtigten Gründe einer Löschung entgegenstehen.

Die Rückgabe erfolgt nach den verfügbaren Exportfunktionen oder nach einer individuell vereinbarten Methode. Äussert der Kunde innerhalb einer angemessenen Frist keine Wahl, können Kundendaten nach den vorgesehenen Löschprozessen gelöscht werden. Nach erfolgter Rückgabe oder Ablauf der vereinbarten Frist werden Kundendaten gelöscht, soweit keine Aufbewahrungspflichten oder berechtigten Gründe entgegenstehen.

12. Nachweise, Audits und Entschädigung

Smart Process AG stellt dem Kunden auf Anfrage angemessene Standardinformationen zum Nachweis der Einhaltung dieses Vertrags zur Verfügung. Dieser Abschnitt betrifft den Nachweis der Vertragseinhaltung, Sicherheitsmassnahmen und Auditierung, nicht die operative Unterstützung bei einzelnen Datenschutzanfragen nach Ziffer 9.

Zu den Standardinformationen können insbesondere dieser AVV, die technischen und organisatorischen Massnahmen, die Unterauftragsbearbeiterliste sowie vorhandene Sicherheits- oder Compliance-Nachweise gehören.

Darüber hinausgehende kundenspezifische Nachweise, umfangreiche Fragebögen, zusätzliche Sicherheitsabklärungen, Vor-Ort-Audits, technische Prüfungen, Abstimmungen mit Prüfstellen oder sonstige ausserordentliche Unterstützungsleistungen werden nach Aufwand entschädigt. Der Stundensatz beträgt CHF 220 exkl. MWST, sofern nicht schriftlich ein anderer Stundensatz vereinbart wurde.

Audits sind vorgängig anzukündigen, während üblicher Geschäftszeiten durchzuführen und so auszugestalten, dass Betrieb, Sicherheit, Vertraulichkeit, Geschäftsgeheimnisse und Rechte anderer Kunden nicht beeinträchtigt werden.

Audits berechtigen nicht zum Zugriff auf Daten anderer Kunden, Quellcode, interne Systeme, sicherheitskritische Informationen oder Geschäftsgeheimnisse, soweit dies für den Nachweis der Einhaltung dieses Vertrags nicht zwingend erforderlich ist.

13. Verhältnis zu anderen Dokumenten

Dieser AVV ergänzt die Allgemeinen Geschäftsbedingungen JuristerAI, das jeweils anwendbare Angebot, Bestellformular, Abonnement oder eine individuelle Vereinbarung zwischen den Parteien.

Bei Widersprüchen hinsichtlich der Bearbeitung von Kundendaten geht dieser AVV vor. Für kommerzielle, produktbezogene oder sonstige nicht datenschutzrechtliche Regelungen bleiben die AGB JuristerAI bzw. die jeweilige individuelle Vereinbarung massgeblich.

Die Datenschutzerklärung informiert ergänzend über die Bearbeitung von Personendaten im Zusammenhang mit Website, Warteliste, Kontaktanfragen und Plattformnutzung. Sie ersetzt diesen AVV nicht.

14. Änderungen dieses AVV

Smart Process AG kann diesen AVV anpassen, wenn sich die Leistungen, die technische Umsetzung, die eingesetzten Unterauftragsbearbeiter oder die rechtlichen Anforderungen ändern.

Wesentliche Änderungen werden dem Kunden in geeigneter Weise mitgeteilt. Der Kunde kann wesentlichen Änderungen aus berechtigten Datenschutzgründen widersprechen. Erfolgt ein berechtigter Widerspruch und ist keine zumutbare Fortführung der betroffenen Leistung möglich, können die Parteien die betroffene Leistung nach den vertraglichen Regelungen beenden. Nutzt

der Kunde JuristerAI nach Inkrafttreten der Änderung ohne Widerspruch weiter, gilt dies als Zustimmung, soweit keine zwingenden Rechte entgegenstehen.

15. Anwendbares Recht und Gerichtsstand

Es gilt schweizerisches Recht. Gerichtsstand ist Rapperswil-Jona SG.

Anhang 1: Beschreibung der Datenbearbeitung

Dieser Anhang beschreibt die Auftragsbearbeitung im Rahmen der JuristerAI-Plattform. Weitere allgemeine Informationen zur Bearbeitung von Personendaten finden sich in der Datenschutzerklärung.

1. Gegenstand und Zweck

Smart Process AG bearbeitet Kundendaten im Auftrag des Kunden, um die JuristerAI-Plattform bereitzustellen und die gebuchten Produktmodule zu erbringen. Dazu gehören insbesondere Transkription, Dokumentenaufbereitung, Fallanalyse, Suche, Chat, Quellenangaben, Benutzerverwaltung, Sicherheit, Support, Abrechnung, Produkt-Analytics und Datenexport.

2. Art der Bearbeitung

Die Bearbeitung umfasst insbesondere das Speichern, Hochladen, Strukturieren, Auslesen, Transkribieren, Analysieren, Zusammenfassen, Kategorisieren, Suchen, Verknüpfen, Bereitstellen, Exportieren, Protokollieren und Löschen von Daten.

3. Kategorien von Personendaten

Bearbeitet werden insbesondere Benutzer-, Kontakt-, Rollen-, Berechtigungs-, Mandats-, Fall-, Dokument-, Audio-, Transkript-, Eingabe-, Prompt-, Such-, Chat-, Metadaten-, Log- und Audit-Daten.

Je nach Inhalt der vom Kunden eingebrachten Daten können auch besonders schützenswerte Personendaten sowie Informationen verarbeitet werden, die einem Berufs-, Amts- oder sonstigen Geheimhaltungsschutz unterliegen.

4. Kategorien betroffener Personen

Betroffene Personen können insbesondere Benutzer des Kunden, Klienten und Mandanten, Parteien, Gegenparteien, Vertreter, Zeugen, Mitarbeitende, Behördenpersonen sowie sonstige in Dokumenten, Audiodateien oder Fallunterlagen erwähnte Personen sein.

5. Produkt-Analytics

Technische Nutzungs- und Betriebsdaten können für Sicherheit, Support, Kapazitätsplanung, Abrechnung und Produktverbesserung ausgewertet werden.

Inhalte von Kundendokumenten, Audiodateien, Transkripten, Prompts oder Fallunterlagen werden nicht für Produkt-Analytics ausgewertet, ausser dies ist für Support, Fehlerbehebung oder eine vom Kunden gewünschte Analyse erforderlich.

Kundendaten werden nicht für KI-Training verwendet.

Anhang 2: Technische und organisatorische Massnahmen

Dieser Anhang beschreibt die technischen und organisatorischen Massnahmen zum Schutz von Kundendaten. Die Massnahmen orientieren sich risikobasiert an etablierten Sicherheitskontrollen, insbesondere aus dem ISO-27001-Umfeld, an den Anforderungen des Schweizer Datenschutzrechts, der DSGVO sowie, soweit anwendbar, an KI-spezifischen Anforderungen des EU AI Act.

Die Massnahmen werden dem Risiko, dem Stand der Technik, der Art der bearbeiteten Daten und dem gewählten Betriebsmodell angemessen umgesetzt und weiterentwickelt.

1. Informationssicherheits-Management

- Entwicklung und Betrieb über einen ISO-27001-zertifizierten Technologiepartner
- definierte Rollen und Verantwortlichkeiten für Informationssicherheit, Betrieb, Entwicklung und Support
- risikobasierter Ansatz für Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit
- dokumentierte Sicherheitsprozesse für Betrieb, Zugriff, Änderungen, Vorfälle und Unterauftragsbearbeiter
- regelmässige Überprüfung und Weiterentwicklung der Sicherheitsmassnahmen

2. Schweizer Datenhaltung und Datensouveränität

- Verarbeitung produktiver Kundendaten in Schweizer Infrastruktur
- Speicherung produktiver Daten in Schweizer Rechenzentren
- keine US-Cloud, auch nicht mit Schweizer Rechenzentrum
- keine Übermittlung vertraulicher Kundendaten an öffentliche Chatbots oder proprietäre externe KI-Dienste
- Einsatz von Schweizer Cloud- und KI-Inference-Anbietern, soweit externe Infrastrukturdienste eingesetzt werden
- Trennung produktiver Kundendaten von Entwicklungs-, Test- und Demo-Umgebungen, soweit technisch und organisatorisch erforderlich

3. Mandantentrennung und Zugriffskontrolle

- logische Trennung von Daten nach Kunde, Organisation, Benutzer und Fall
- rollenbasierte Zugriffskontrolle für Benutzer und Administratoren
- Berechtigungsvergabe nach dem Need-to-know- und Least-Privilege-Prinzip
- getrennte Benutzerkonten; keine gemeinsame Nutzung administrativer Konten im Regelbetrieb
- regelmässige Überprüfung privilegierter Zugriffe
- beschränkte Support- und Betriebszugriffe auf Kundendaten, nur soweit für Betrieb, Sicherheit, Support, Fehlerbehebung oder vertraglich vereinbarte Leistungen erforderlich

4. Authentifizierung und Benutzerverwaltung

- persönliche Benutzerkonten für Plattformnutzer
- sichere Authentifizierungsverfahren
- administrative Zugriffe mit erhöhten Schutzmassnahmen
- Möglichkeit zur kundenbezogenen Benutzer- und Rollenverwaltung, soweit produktseitig vorgesehen
- Deaktivierung oder Entzug von Zugriffsrechten bei Wegfall der Berechtigung
- SSO oder kundenspezifische Identitätsintegration als individuelle oder paketabhängige Option

5. Verschlüsselung und Kommunikationssicherheit

- verschlüsselte Übertragung von Daten zwischen Benutzer, Plattform und Systemkomponenten
- Verschlüsselung gespeicherter Daten, soweit technisch vorgesehen und angemessen
- sichere Verwaltung von Geheimnissen, Zugangsdaten und Schlüsseln
- Schutz administrativer Schnittstellen durch geeignete Zugriffsbeschränkungen

6. Protokollierung, Monitoring und Auditierbarkeit

- Protokollierung sicherheitsrelevanter System- und Zugriffsvorgänge
- Audit-Logs für relevante administrative und sicherheitsbezogene Aktionen
- Monitoring der produktiven Betriebsumgebung zur Erkennung von Störungen und Auffälligkeiten
- Schutz von Logdaten vor unbefugtem Zugriff und Manipulation
- Aufbewahrung von Logs nach risikobasierten und betrieblichen Anforderungen

7. Betriebssicherheit und Verfügbarkeit

- Betrieb in kontrollierter Schweizer Infrastruktur
- Überwachung zentraler Systemkomponenten
- definierte Prozesse für Betrieb, Wartung und Störungsbehebung
- geplante Wartungsfenster und sicherheitsrelevante Notfallwartungen nach den Regelungen der AGB und des Standard-SLA
- Kapazitätsplanung und Performance-Überwachung nach betrieblichem Bedarf
- Backup- und Wiederherstellungsprozesse für produktive Daten

8. Change-, Release-, Konfigurationsmanagement

- geregelte Prozesse für Änderungen an Software, Infrastruktur und Konfiguration
- Trennung von Entwicklungs-, Test- und Produktivumgebungen
- Prüfung und Freigabe wesentlicher Änderungen vor produktiver Nutzung
- Möglichkeit zum Rollback oder zur Fehlerbehebung bei fehlgeschlagenen Änderungen
- Dokumentation relevanter Änderungen

9. Sichere Entwicklung

- Entwicklung nach anerkannten Grundsätzen sicherer Softwareentwicklung
- Code Reviews oder vergleichbare Qualitätssicherungsprozesse
- Schutz von Entwicklungs- und Deployment-Prozessen
- Einsatz von Versionskontrolle und kontrollierten Release-Prozessen
- risikobasierte Prüfung sicherheitsrelevanter Änderungen
- keine Verwendung produktiver Kundendaten in Entwicklung oder Test, sofern nicht erforderlich, vereinbart oder angemessen geschützt

10. Schwachstellen- und Patch-Management

- Monitoring und Bewertung technischer Schwachstellen
- zeitnahe Behandlung kritischer Sicherheitsupdates nach Risiko und betrieblicher Dringlichkeit
- Schutz vor bekannten, relevanten Sicherheitsrisiken in Applikation, Infrastruktur und Abhängigkeiten
- sicherheitsrelevante Notfallmassnahmen bei erhöhtem Risiko

11. Incident Management

- Prozess zur Erkennung, Bewertung, Behandlung und Dokumentation von Sicherheitsvorfällen
- Eskalation relevanter Vorfälle an verantwortliche Stellen
- Information betroffener Kunden bei Sicherheitsvorfällen, die Kundendaten betreffen
- Massnahmen zur Eindämmung, Behebung und Nachbearbeitung von Vorfällen
- Unterstützung des Kunden bei datenschutzrechtlichen Melde- und Informationspflichten nach Massgabe dieses AVV

12. Datenlebenszyklus, Export und Löschung

- Verarbeitung von Kundendaten nur zu den vertraglich vereinbarten Zwecken
- Exportmöglichkeiten nach den verfügbaren Produktfunktionen
- Rückgabe oder Löschung von Kundendaten nach Vertragsende gemäss Vertrag
- Löschprozesse für Kundendaten, soweit keine gesetzlichen Pflichten oder berechtigten Gründe entgegenstehen
- keine Nutzung von Kundendaten für KI-Training

13. Vertraulichkeit und Geheimnisschutz

- Verpflichtung von Mitarbeitenden und eingesetzten Unterauftragsbearbeitern zur Vertraulichkeit
- besonderer Schutz von Mandats-, Fall- und Behördendaten
- Zugriff auf vertrauliche Kundendaten nur soweit erforderlich
- technische und organisatorische Unterstützung der Trennung von Organisationen, Benutzern und Fällen
- Schutz von Informationen, die einem Berufs-, Amts- oder sonstigen Geheimhaltungsschutz unterliegen können

14. Unterauftragsbearbeiter, Lieferantenkontrolle

- sorgfältige Auswahl von Unterauftragsbearbeitern
- vertragliche Verpflichtung von Unterauftragsbearbeitern zu Datenschutz-, Sicherheits- und Vertraulichkeitspflichten
- Einsatz von Unterauftragsbearbeitern gemäss Anhang 3
- Information über wesentliche Änderungen bei Unterauftragsbearbeitern nach Massgabe dieses AVV
- risikobasierte Überprüfung relevanter Lieferanten und Betriebsdienstleister

15. KI-Governance und EU-AI-Act-Readiness

- risikobasierte Steuerung des Einsatzes von KI-Funktionen
- Einsatz kontrolliert betriebener Open-Source- bzw. Open-Weight-KI-Modelle in Schweizer Infrastruktur oder über Schweizer KI-Inference-Anbieter
- keine Übermittlung vertraulicher Kundendaten an öffentliche Chatbots oder proprietäre externe KI-Dienste
- keine Nutzung von Kundendaten für KI-Training
- fachliche Prüfung und menschliche Kontrolle der KI-Ergebnisse durch den Kunden
- keine automatisierten Entscheidungen mit rechtlicher Wirkung gegenüber betroffenen Personen
- Quellenangaben, Referenzen oder Verweise auf zugrunde liegende Unterlagen, soweit produktseitig vorgesehen
- Protokollierung und Nachvollziehbarkeit relevanter Verarbeitungsvorgänge, soweit technisch vorgesehen
- risikobasierte Bewertung von KI-Funktionen, Datenflüssen, Modellnutzung und möglichen Fehlerrisiken
- Berücksichtigung anwendbarer Anforderungen des EU AI Act, insbesondere Transparenz, menschliche Aufsicht, Daten-Governance, technische Dokumentation und AI-Literacy, soweit einschlägig

16. Technikgestaltung und Voreinstellungen

- Berücksichtigung von Datenschutz, Vertraulichkeit und Datensicherheit bei Produktgestaltung und Weiterentwicklung
- zweckgebundene Verarbeitung von Kundendaten
- Begrenzung von Zugriffen, Datenflüssen und Speicherdauer nach vertraglichen und technischen Vorgaben
- Unterstützung von Export- und Löschprozessen nach den verfügbaren Produktfunktionen

17. Grenzen und kundenspezifische Massnahmen

Bestimmte Massnahmen hängen vom gewählten Paket, Betriebsmodell oder von individuellen Vereinbarungen ab. Dazu gehören insbesondere SSO, kundenspezifische Integrationen, dedizierte oder segregierte Betriebsmodelle, spezifische RTO/RPO-Vorgaben, erweiterte Audit- oder Reportingpflichten sowie individuelle SLA.

Anhang 3: Unterauftragsbearbeiter

Dieser Anhang nennt die Unterauftragsbearbeiter, die Smart Process AG im Zusammenhang mit JuristerAI einsetzen kann. Der Einsatz erfolgt nur, soweit dies für Entwicklung, Betrieb, Wartung, Sicherheit, Support, KI-Verarbeitung, Hosting oder Produkt-Analytics erforderlich ist.

Smart Process AG verpflichtet Unterauftragsbearbeiter vertraglich zu Datenschutz-, Sicherheits- und Vertraulichkeitspflichten, die den Pflichten aus diesem AVV im Wesentlichen entsprechen.

Unterauftrags-bearbeiter	Rolle	Leistungen	Daten-standort	Zugriff / Verarbeitung	Zertifizierungen und Nachweise
skyquest AG Sumpfstrasse 26 6312 Steinhausen Schweiz	Schweizer Technologie-, Entwicklungs- und Betriebspartner	Software- und KI-Entwicklung; CloudOps; Managed Cloud Services; Plattformbetrieb; Wartung; Monitoring; Sicherheit; technische Weiterentwicklung; Unterstützung bei Compliance, Incident Management, Fehlerbehebung und technischem Support	Schweiz	Zugriff auf Kundendaten nur soweit für Entwicklung, Betrieb, Wartung, Sicherheit, Support, Fehlerbehebung oder vertraglich vereinbarte Leistungen erforderlich.	ISO 27001 zertifiziert. Prozesse und Betrieb sind auf revDSG-/DSGVO-konforme Verarbeitung ausgerichtet. Weitergehende Trust-, Sicherheits- und Compliance-Informationen werden über das Trust Center unter trust.skyquest.ch bereitgestellt.
Akenes SA / Exoscale Boulevard de Grancy 19A 1006 Lausanne Schweiz	Schweizer Cloud-Infrastruktur-Anbieter	Cloud-Infrastruktur für produktive Systeme; Rechen-, Speicher-, Netzwerk- und Plattformdienste; Betrieb von Infrastrukturkomponenten in Schweizer Rechenzentren;	Schweiz	Infrastrukturbezogener Zugriff im Rahmen des Betriebs der Cloud-Infrastruktur. Ein inhaltlicher Zugriff auf Kundendaten ist nicht Zweck der Leistung.	Nach ISO/IEC 27001, ISO/IEC 27017 und ISO/IEC 27018 zertifiziert; SOC 2, BSI C5 und CSA STAR Nachweise. Unterstützt den Betrieb in Schweizer Infrastruktur

		Grundlage für skalierbaren und souveränen Plattformbetrieb			und eine revDSG-/DSGVO-konforme Ausgestaltung.
Infomaniak Network SA Rue Eugène-Marziano 25 1227 Les Acacias Schweiz	Schweizer KI-Inference-Anbieter	Ausführung von Open-Source- bzw. Open-Weight-KI-Modellen für Transkription, Dokumentenaufbereitung, Suche, Chat, Zusammenfassung oder Fallanalyse, soweit eingesetzt	Schweiz	Kundendaten werden nur punktuell und vorübergehend für die jeweilige KI-Inference verarbeitet. Keine dauerhafte Speicherung und inhaltlicher Zugriff auf Kundendaten ist nicht Zweck der Leistung. Keine Nutzung für KI-Training.	Nach ISO 27001:2022, ISO 9001:2015, ISO 14001:2015 und ISO 50001:2018 zertifiziert; Labels Swiss Hosting, Swiss Made Software und Swiss Made. Unterstützt eine revDSG-/DSGVO-konforme Ausgestaltung.
Safe Swiss Cloud AG Zurlindenstrasse 52a 8003 Zürich Schweiz	Schweizer KI-Inference-Anbieter	Ausführung von Open-Source- bzw. Open-Weight-KI-Modellen für Transkription, Dokumentenaufbereitung, Suche, Chat, Zusammenfassung oder Fallanalyse, soweit eingesetzt	Schweiz	Kundendaten werden nur punktuell und vorübergehend für die jeweilige KI-Inference verarbeitet. Keine dauerhafte Speicherung und inhaltlicher Zugriff auf Kundendaten ist nicht Zweck der Leistung. Keine Nutzung für KI-Training.	Nach ISO 27001, ISO 27017 und ISO 27018 zertifiziert. Unterstützt eine revDSG-/DSGVO-konforme Ausgestaltung.
Phoenix Systems AG Technopark 1 8005 Zürich Schweiz	Schweizer KI-Inference-Anbieter	Ausführung von Open-Source- bzw. Open-Weight-KI-Modellen für Transkription, Dokumentenaufbereitung, Suche, Chat, Zusammenfassung oder Fallanalyse, soweit eingesetzt	Schweiz	Kundendaten werden nur punktuell und vorübergehend für die jeweilige KI-Inference verarbeitet. Keine dauerhafte Speicherung und inhaltlicher Zugriff auf Kundendaten ist nicht Zweck der Leistung. Keine Nutzung für KI-Training.	Nach ISO 27001 zertifiziert; ISAE 3402 Type I und Type II Nachweise. Unterstützt eine revDSG-/DSGVO-konforme Ausgestaltung.