AUFTRAGSVERARBEITUNG

Auftragsverarbeitungs-vertrag

Vereinbarung nach Art. 28 Datenschutz-Grundverordnung (DSGVO) für die Nutzung der Software-as-a-Service-Plattform ASEIO.

Version 1.1	Vertragsart	Rechtsgrundlage
Stand: 23. Juli 2026	Vereinbarung zur Auftragsverarbeitung	Art. 28 DSGVO

Vertragsparteien

Verantwortlicher

Kunde gemäß ASEIO-Nutzungsvertrag

Unternehmen / Organisation:

_____

Anschrift:

_____

Datenschutzkontakt:

_____

Auftragsverarbeiter

TradeX International AG

Chaltenbodenstrasse 16
CH-8834 Schindellegi, Schweiz
Datenschutzkontakt: info@tradexag.ch

Vertragsbestandteil
Dieser AVV ergänzt den ASEIO-Nutzungsvertrag. Er gilt für jede Verarbeitung personenbezogener Daten durch TradeX im Auftrag des Kunden. Die Anlagen sind Bestandteil dieser Vereinbarung.

Vereinbarung zur Auftragsverarbeitung

Die nachfolgenden Regelungen konkretisieren die Rechte und Pflichten der Vertragsparteien bei der Verarbeitung personenbezogener Daten im Auftrag.

1. Parteien und Geltungsbereich

Dieser Auftragsverarbeitungsvertrag (AVV) wird zwischen dem im ASEIO-Nutzungsvertrag bezeichneten Kunden (nachfolgend „Verantwortlicher“) und der TradeX International AG, Chaltenbodenstrasse 16, CH-8834 Schindellegi, Schweiz (nachfolgend „Auftragsverarbeiter“) geschlossen.

Der AVV ergänzt den Vertrag über die Nutzung der Software-as-a-Service-Plattform ASEIO (Hauptvertrag). Er gilt, soweit der Auftragsverarbeiter bei der Leistungserbringung personenbezogene Daten im Auftrag des Verantwortlichen im Sinne von Art. 28 DSGVO verarbeitet. Handelt der Kunde seinerseits als Auftragsverarbeiter, gelten seine Weisungen zugleich als Weisungen des jeweils Verantwortlichen und TradeX als weiterer Auftragsverarbeiter.

Bei Widersprüchen gehen die datenschutzrechtlichen Regelungen dieses AVV den Regelungen des Hauptvertrags vor. Im Übrigen bleibt der Hauptvertrag unberührt.

2. Gegenstand, Zweck und Dauer der Verarbeitung

Gegenstand der Verarbeitung ist die Bereitstellung, Absicherung, Wartung und Unterstützung von ASEIO. Die Plattform dient insbesondere dem Import, der Speicherung, Bearbeitung, Anreicherung, KI-gestützten Optimierung und dem Export von Produkt-, Listing-, Katalog- und zugehörigen Geschäftsdaten sowie der Anbindung der vom Verantwortlichen ausgewählten Drittsysteme.

Die Verarbeitung beginnt mit der Bereitstellung des Kundenkontos und dauert für die Laufzeit des Hauptvertrags sowie darüber hinaus nur so lange an, wie Daten nach dessen Beendigung vertragsgemäß zurückzugeben, zu löschen oder aufgrund zwingender gesetzlicher Pflichten aufzubewahren sind.

3. Art der Verarbeitung

Je nach Nutzung umfasst die Verarbeitung insbesondere das Erheben bzw. Empfangen, Erfassen, Ordnen, Speichern, Auslesen, Abgleichen, Strukturieren, Verändern, Übermitteln, Bereitstellen, Einschränken und Löschen von Daten. Eine Offenlegung an verbundene Systeme erfolgt nur durch die Konfiguration oder Einzelaktion des Verantwortlichen oder soweit sie für den vereinbarten Plattformbetrieb erforderlich ist.

4. Datenarten und betroffene Personen

ASEIO ist auf Unternehmens- und Produktdaten ausgerichtet. Personenbezogene Daten können dennoch enthalten oder mit solchen Daten verknüpft sein.

- Datenarten: Namen, geschäftliche Kontakt- und Kontodaten, Organisations- und Rollenzuordnungen, Produkt-, Listing-, Katalog- und Geschäftsdaten mit möglichem Personenbezug, Inhalte und Dateien, technische Nutzungs-, Protokoll- und Supportdaten sowie verschlüsselt gespeicherte Integrations-Zugangsdaten.
- Betroffene Personen: Beschäftigte, Beauftragte und sonstige Nutzer des Verantwortlichen sowie Geschäftspartner, Lieferanten und Ansprechpartner, soweit deren Daten vom Verantwortlichen in ASEIO eingebracht werden.
- Nicht vorgesehene Daten: ASEIO ruft aus angebundenen Shops und Marktplätzen keine Endkunden- oder Bestelldaten ab. Besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO sowie Daten über strafrechtliche Verurteilungen nach Art. 10 DSGVO dürfen nur nach vorheriger ausdrücklicher Vereinbarung verarbeitet werden.

5. Weisungsgebundene Verarbeitung

Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen, soweit nicht Unionsrecht oder das Recht eines Mitgliedstaats bzw. anderes zwingend anwendbares Recht eine Verarbeitung verlangt. In diesem Fall informiert er den Verantwortlichen vor der Verarbeitung, sofern das betreffende Recht dies nicht aus wichtigen Gründen des öffentlichen Interesses untersagt.

Als dokumentierte Weisungen gelten insbesondere der Hauptvertrag und dieser AVV, die vom Verantwortlichen vorgenommenen Einstellungen, ausgelösten Aktionen und API-Aufrufe sowie Weisungen in Textform über die vereinbarten Supportkanäle. Hält der Auftragsverarbeiter eine Weisung für datenschutzrechtswidrig, informiert er den Verantwortlichen unverzüglich und darf ihre Ausführung bis zur Klärung aussetzen.

6. Pflichten des Verantwortlichen

Der Verantwortliche ist für die Rechtmäßigkeit der Verarbeitung, die Wahrung der Rechte betroffener Personen, die Richtigkeit seiner Weisungen und die Auswahl geeigneter Plattformfunktionen verantwortlich. Er stellt insbesondere sicher, dass für die eingebrachten Daten eine Rechtsgrundlage besteht, die erforderlichen Informationspflichten erfüllt sind und nur erforderliche Daten verarbeitet werden.

Der Verantwortliche verwaltet seine Nutzer, Rollen, Integrationen und Exporte nach dem Need-to-know-Prinzip und informiert den Auftragsverarbeiter unverzüglich über erkennbare Fehler, Sicherheitsvorfälle oder unrechtmäßige Weisungen.

7. Vertraulichkeit und Zugriffsberechtigung

Der Auftragsverarbeiter stellt sicher, dass zur Verarbeitung befugte Personen zur Vertraulichkeit verpflichtet sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Zugriff auf Auftragsdaten erhalten nur Personen, die ihn zur Leistungserbringung, Störungsbehebung, Sicherheit oder Erfüllung gesetzlicher Pflichten benötigen.

8. Sicherheit der Verarbeitung

Der Auftragsverarbeiter trifft unter Berücksichtigung des Stands der Technik, der Implementierungskosten sowie Art, Umfang, Umständen und Zwecken der Verarbeitung angemessene technische und organisatorische Maßnahmen nach Art. 32 DSGVO. Die in Anlage 1 beschriebenen Maßnahmen dürfen weiterentwickelt werden, sofern das vereinbarte Schutzniveau nicht unterschritten wird.

9. Unterstützung und Betroffenenrechte

Der Auftragsverarbeiter unterstützt den Verantwortlichen unter Berücksichtigung der Art der Verarbeitung und der verfügbaren Informationen angemessen bei der Erfüllung seiner Pflichten nach Art. 12 bis 22, 32 bis 36 DSGVO, insbesondere bei Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit, Sicherheitsbewertungen und Datenschutz-Folgenabschätzungen.

Geht ein Antrag einer betroffenen Person unmittelbar beim Auftragsverarbeiter ein und betrifft er Auftragsdaten, leitet dieser ihn an den Verantwortlichen weiter und beantwortet ihn ohne Weisung grundsätzlich nicht, soweit keine gesetzliche Pflicht zur unmittelbaren Antwort besteht.

10. Datenschutzverletzungen

Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, nachdem ihm eine Verletzung des Schutzes personenbezogener Auftragsdaten bekannt geworden ist. Die Mitteilung enthält, soweit verfügbar, die für Meldungen nach Art. 33 und 34 DSGVO erforderlichen Informationen. Noch nicht verfügbare Informationen werden ohne unangemessene Verzögerung nachgereicht. Der Auftragsverarbeiter unterstützt den Verantwortlichen angemessen bei Untersuchung, Eindämmung und Behebung.

11. Weitere Auftragsverarbeiter

Der Verantwortliche erteilt die allgemeine schriftliche Genehmigung, die in Anlage 2 aufgeführten weiteren Auftragsverarbeiter einzusetzen. Der Auftragsverarbeiter informiert über beabsichtigte Hinzuziehungen oder Ersetzungen mindestens 30 Tage vorab in Textform oder über die Plattform. Der Verantwortliche kann innerhalb von 14 Tagen aus begründeten datenschutzrechtlichen Gründen widersprechen.

Der Auftragsverarbeiter legt weiteren Auftragsverarbeitern im erforderlichen Umfang gleichwertige Datenschutzpflichten auf und bleibt gegenüber dem Verantwortlichen für deren Pflichterfüllung verantwortlich. Produktdaten-Lizenzgeber und vom Verantwortlichen selbst angebundene Zielsysteme sind keine weiteren Auftragsverarbeiter des Auftragsverarbeiters, soweit sie nicht von TradeX zur Verarbeitung personenbezogener Auftragsdaten in deren Auftrag eingesetzt werden.

12. Drittlandübermittlungen

Die Schweiz ist durch einen Angemessenheitsbeschluss der Europäischen Kommission als Drittland mit angemessenem Datenschutzniveau anerkannt. Eine weitere Verarbeitung außerhalb der EU bzw. des EWR oder der Schweiz erfolgt nur, wenn die Voraussetzungen der Art. 44 ff. DSGVO und des anwendbaren Schweizer Datenschutzrechts erfüllt sind. Dies kann insbesondere auf einem Angemessenheitsbeschluss, einer wirksamen Zertifizierung unter einem anerkannten Datenschutzrahmen oder EU-Standardvertragsklauseln einschließlich erforderlicher ergänzender Maßnahmen beruhen.

13. Nachweise und Kontrollen

Der Auftragsverarbeiter stellt dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung von Art. 28 DSGVO zur Verfügung und ermöglicht angemessene Überprüfungen einschließlich Inspektionen durch den Verantwortlichen oder einen von ihm beauftragten Prüfer. Vorrangig sind aktuelle Zertifikate, Prüfberichte, Sicherheitsdokumentationen und schriftliche Auskünfte zu nutzen.

Soweit diese Nachweise nicht ausreichen, kann der Verantwortliche selbst oder durch einen unabhängigen, zur Vertraulichkeit verpflichteten Prüfer nach angemessener Vorankündigung und während üblicher Geschäftszeiten eine erforderliche Prüfung durchführen. Geschäftsgeheimnisse und Daten anderer Kunden sind zu schützen. Zusätzlicher Aufwand kann nach dem Hauptvertrag berechnet werden, es sei denn, die Prüfung weist einen wesentlichen vom Auftragsverarbeiter zu vertretenden Verstoß nach.

14. Rückgabe und Löschung

Nach Ende der Auftragsverarbeitung löscht oder gibt der Auftragsverarbeiter nach Wahl des Verantwortlichen die personenbezogenen Auftragsdaten zurück und löscht vorhandene Kopien, soweit keine gesetzliche Aufbewahrungspflicht entgegensteht. Der Verantwortliche soll verfügbare Exportfunktionen vor Vertragsende nutzen.

Produktdaten im Papierkorb werden grundsätzlich nach 30 Tagen endgültig gelöscht. Sicherungskopien werden im regulären Zyklus innerhalb von rund 30 Tagen überschrieben bzw. gelöscht und bis dahin nur zur Wiederherstellung und Betriebssicherung verwendet. Gesetzlich aufzubewahrende Daten werden gesperrt und ausschließlich für den gesetzlichen Zweck verarbeitet.

15. Schlussbestimmungen

Änderungen und Ergänzungen dieses AVV bedürfen der Textform, soweit nicht eine strengere Form gesetzlich vorgeschrieben ist. Die elektronische Annahme des Hauptvertrags oder die vereinbarte Nutzung von ASEIO kann die Einbeziehung dieses AVV dokumentieren; auf Verlangen stellen die Parteien eine gesonderte Unterzeichnungsmöglichkeit bereit.

Haftung, Laufzeit, Kündigung, Rechtswahl und Gerichtsstand richten sich nach dem Hauptvertrag, soweit zwingendes Datenschutzrecht nichts anderes bestimmt. Stand: 23. Juli 2026.

Anlage 1

Technische und organisatorische Maßnahmen

Die nachfolgenden Maßnahmen konkretisieren das für die ASEIO-Plattform vereinbarte Schutzniveau. Sie werden risikoorientiert weiterentwickelt, ohne das Schutzniveau zu unterschreiten.

Maßnahmenbereich	Umsetzung bei ASEIO
Physischer Schutz und Rechenzentrum	Der Produktivbetrieb erfolgt in vertraglich gebundener Rechenzentrumsinfrastruktur in Deutschland. Der physische Zutritt zu Server-, Netzwerk- und Speichersystemen wird durch den Infrastrukturbetreiber kontrolliert; ASEIO-Administrationszugriffe erfolgen ausschließlich remote über geschützte Zugänge.
Identitäts- und Zugriffskontrolle	Individuelle Benutzerkonten, serverseitige Sitzungsprüfung, sichere Session-Cookies, rollen- und mandantenbezogene Berechtigungen sowie beschränkte Administrator- und Supportzugriffe nach dem Need-to-know-Prinzip. Zugriffsrechte werden bei Aufgabenwechsel oder Ausscheiden entzogen.
Mandantentrennung	Kundendaten werden logisch anhand der Organisation bzw. des Tenants getrennt. Serverseitige Autorisierungsprüfungen binden Datenzugriffe, Integrationen, Hintergrundaufgaben und Exporte an den angemeldeten Nutzer und dessen Tenant; tenantübergreifende Zugriffe werden nicht zugelassen.
Übertragungs- und Speicherschutz	TLS-verschlüsselte Übertragung mit HSTS und zusätzlichen Sicherheitsheadern. Integrations-Zugangsdaten werden serverseitig mit AES-256-GCM verschlüsselt gespeichert; Passwörter werden ausschließlich als kryptografische Hashes gespeichert. Schlüssel und Secrets werden getrennt vom Anwendungscode verwaltet.
Protokollierung und Geheimnisschutz	Sicherheits- und betriebsrelevante Vorgänge werden zur Fehleranalyse und Missbrauchserkennung protokolliert. Zugangs-, Signatur- und OAuth-Geheimnisse werden aus Proxy-Logs entfernt bzw. geschwärzt; Protokolle sind nur für befugte Betriebs- und Sicherheitsfunktionen zugänglich.
Verfügbarkeit, Sicherung und Wiederherstellung	Regelmäßige automatisierte Datenbanksicherungen mit begrenzter Aufbewahrung, getrennte Wiederherstellungsprüfungen sowie Healthchecks für Anwendung, Datenbank, Worker und Wartungsjobs. Queue-, Speicher- und Ressourcenstatus werden überwacht; Störungen werden erfasst und priorisiert bearbeitet.
Änderungs- und Schwachstellenmanagement	Änderungen werden versioniert, vor der Übernahme geprüft und durch automatisierte Build-, Typ- und Funktionstests abgesichert. Abhängigkeiten und Basissysteme werden gepflegt; sicherheitsrelevante Fehler werden nach Risiko priorisiert und nachvollziehbar behoben.
Datenminimierung, Aufbewahrung und Löschung	Plattformfunktionen sind auf Produkt-, Listing- und Geschäftsdaten ausgerichtet. Aus angebundenen Shops und Marktplätzen werden standardmäßig keine Endkunden- oder Bestelldaten abgerufen. Lösch- und Exportfunktionen, ein 30-tägiger Papierkorb sowie begrenzte Backup-Aufbewahrung unterstützen die festgelegten Löschfristen.
Sicherheitsvorfälle und Wirksamkeitskontrolle	Definierte Verfahren für Erkennung, Eindämmung, Untersuchung, Dokumentation und Meldung von Sicherheitsvorfällen. Berechtigungen, Wiederherstellbarkeit und technische Schutzmaßnahmen werden wiederkehrend sowie nach wesentlichen Änderungen überprüft.

Anlage 2

Weitere Auftragsverarbeiter

Die folgende Liste nennt die für den ASEIO-Betrieb eingesetzten Anbieter. Sie erfasst weitere Auftragsverarbeiter und kennzeichnet Leistungen, bei denen der Anbieter teilweise in eigener datenschutzrechtlicher Verantwortung handelt.

Anbieter	Ort / Transfer	Zweck	Daten / Schutz
Hetzner Online GmbH	Deutschland / EU Verarbeitung in der EU; AV-Vertrag mit dem Anbieter	Hosting, Server-, Netzwerk- und Speicherinfrastruktur einschließlich Backups	Sämtliche in ASEIO gespeicherten Auftragsdaten
OpenAI Ireland Limited und verbundene Unterauftragsverarbeiter	Irland; mögliche weitere Verarbeitung in Drittländern Anbieter-DPA; für Drittlandtransfers insbesondere Angemessenheitsmechanismen bzw. EU-Standardvertragsklauseln	KI-gestützte Textgenerierung, Extraktion und Optimierung auf aktive Veranlassung des Nutzers	Nur die für die jeweilige KI-Anfrage erforderlichen Produktinhalte und technischen Metadaten; keine Zahlungs- oder Zugangsdaten
Plus Five Five, Inc. (Resend)	USA Anbieter-DPA einschließlich EU-Standardvertragsklauseln	SMTP-Versand transaktionaler E-Mails und technischer Störungsmeldungen	E-Mail-Adresse, Absender, Betreff, Nachrichteninhalt sowie Zustell- und Ereignisdaten
Stripe Payments Europe, Limited, Stripe Technology Europe, Limited und eingesetzte Stripe-Unternehmen	Irland / international Stripe-DPA und geeignete Transfermechanismen; Stripe handelt je nach Leistung teilweise als eigener Verantwortlicher, sodass dieser AVV insoweit nicht gilt	Zahlungsabwicklung, Abonnement- und Abrechnungsverwaltung	Abrechnungskontakt, E-Mail-Adresse, Organisations-, Plan- und Transaktionsreferenzen; Zahlungsdaten werden direkt durch Stripe erhoben

Hinweis: Das Infrastruktur-Monitoring wird im ASEIO-Hosting selbst betrieben und begründet derzeit keinen zusätzlichen externen Auftragsverarbeiter. Die Aktivierung eines externen Monitoring-Dienstes richtet sich nach Ziffer 11.

Anlage 3

Vertragsdaten und Unterzeichnung

Die Vertragsdaten des Verantwortlichen ergeben sich aus dem ASEIO-Vertragskonto und können für eine gesonderte Unterzeichnung nachfolgend ergänzt werden.

Elektronische Annahme: Nach Ziffer 15 kann die Einbeziehung dieses AVV auch elektronisch dokumentiert werden. Die Unterschriftsfelder dienen der gesonderten Unterzeichnung, falls eine Partei diese verlangt.

Verantwortlicher

Kunde gemäß ASEIO-Nutzungsvertrag

Unternehmen und Anschrift gemäß Vertragskonto

Ort, Datum

_____

Name und Funktion

_____

Unterschrift

_____

Auftragsverarbeiter

TradeX International AG

Chaltenbodenstrasse 16, CH-8834 Schindellegi, Schweiz

Ort, Datum

_____

Name und Funktion

_____

Unterschrift

_____