

Auftragsverarbeitungsvertrag (AVV) gemäß Art. 28 DSGVO

zwischen dem Kunden (nachfolgend „Verantwortlicher“ oder „Auftraggeber“) und der Pakera AI Packaging Optimization GmbH, Brunnenweg 35, 83666 Waakirchen, Deutschland (nachfolgend „Pakera“, „Auftragnehmer“ oder „Auftragsverarbeiter“)

Stand: August 2026

Präambel

Dieser Auftragsverarbeitungsvertrag (AVV) konkretisiert die datenschutzrechtlichen Pflichten der Parteien im Rahmen der Nutzung der SaaS-Plattform Pakera gemäß den AGB von Pakera. Er gilt für alle Tätigkeiten, bei denen Pakera personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet (Art. 4 Nr. 8, Art. 28 DSGVO).

Der Verantwortliche ist für die Rechtmäßigkeit der Verarbeitung und die Wahrung der Betroffenenrechte allein verantwortlich (Art. 24 DSGVO). Pakera verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen, sofern keine gesetzliche Verpflichtung zur Verarbeitung besteht.

1. Gegenstand, Art und Zweck der Verarbeitung

Gegenstand und Dauer der Verarbeitung ergeben sich aus dem Hauptvertrag (AGB), dem Bestellformular, soweit vorhanden, und entsprechen der Vertragslaufzeit. Art, Zweck der Verarbeitung, Art der personenbezogenen Daten und Kategorien betroffener Personen sind in **Anhang 1** beschrieben.

2. Weisungsrecht des Verantwortlichen

2.1 Pakera verarbeitet personenbezogene Daten nur im Rahmen der getroffenen Vereinbarungen und nach dokumentierten Weisungen des Verantwortlichen, es sei denn, Pakera ist gesetzlich zur Verarbeitung verpflichtet (in diesem Fall teilt Pakera dem Verantwortlichen diese Anforderungen vor der Verarbeitung mit, sofern das Recht dies nicht wegen eines wichtigen öffentlichen Interesses verbietet).

2.2 Weisungen werden grundsätzlich in Textform erteilt; mündliche Weisungen sind unverzüglich in Textform zu bestätigen. Die im Hauptvertrag und in diesem AVV getroffenen Regelungen gelten als Erstweisung.

2.3 Pakera informiert den Verantwortlichen unverzüglich, wenn sie der Auffassung ist, dass eine Weisung gegen die DSGVO oder andere Datenschutzvorschriften verstößt. Pakera ist berechtigt, die Durchführung der betreffenden Weisung bis zu deren Bestätigung oder Änderung auszusetzen.

3. Pflichten von Pakera (Auftragsverarbeiter)

Pakera verpflichtet sich insbesondere,

- personenbezogene Daten ausschließlich gemäß Ziffer 2 zu verarbeiten;

- sicherzustellen, dass die zur Verarbeitung befugten Personen zur Vertraulichkeit verpflichtet sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 lit. b, Art. 29, Art. 32 Abs. 4 DSGVO);
- die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen (TOM) gemäß Anhang 2 zu treffen und einzuhalten;
- die Bedingungen für die Inanspruchnahme weiterer Auftragsverarbeiter (Subprozessoren) gemäß Ziffer 5 einzuhalten;
- den Verantwortlichen mit geeigneten technischen und organisatorischen Maßnahmen nach Möglichkeit dabei zu unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der Betroffenenrechte (Kapitel III DSGVO) nachzukommen (Art. 28 Abs. 3 lit. e DSGVO);
- den Verantwortlichen bei der Einhaltung der Pflichten gemäß Art. 32 bis 36 DSGVO (Datensicherheit, Meldung von Datenschutzverletzungen, Datenschutz-Folgenabschätzung, vorherige Konsultation) unter Berücksichtigung der Art der Verarbeitung und der ihr zur Verfügung stehenden Informationen zu unterstützen (Art. 28 Abs. 3 lit. f DSGVO);
- nach Wahl des Verantwortlichen alle personenbezogenen Daten nach Abschluss der Erbringung der Verarbeitungsleistungen zu löschen oder zurückzugeben und vorhandene Kopien zu vernichten, sofern keine gesetzliche Aufbewahrungspflicht besteht (Ziffer 8);
- dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der Pflichten aus Art. 28 DSGVO zur Verfügung zu stellen und Überprüfungen gemäß Ziffer 7 zu ermöglichen und dazu beizutragen;
- einen Datenschutzbeauftragten zu benennen, soweit gesetzlich erforderlich;
- ein Verzeichnis aller Kategorien von im Auftrag durchgeführten Verarbeitungstätigkeiten gemäß Art. 30 Abs. 2 DSGVO zu führen.

4. Technische und organisatorische Maßnahmen (TOM)

Pakera trifft die in Anhang 2 beschriebenen technischen und organisatorischen Maßnahmen nach dem Stand der Technik. Pakera ist berechtigt, die Maßnahmen weiterzuentwickeln und anzupassen, darf das vereinbarte Schutzniveau dabei jedoch nicht unterschreiten. Wesentliche Änderungen sind zu dokumentieren.

5. Inanspruchnahme weiterer Auftragsverarbeiter (Subprozessoren)

5.1 Der Verantwortliche erteilt seine allgemeine Genehmigung zum Einsatz weiterer Auftragsverarbeiter (Subprozessoren). Die zum Zeitpunkt des Vertragsschlusses eingesetzten Subprozessoren sind in Anhang 3 aufgeführt und gelten als genehmigt.

5.2 Pakera informiert den Verantwortlichen über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder Ersetzung von Subprozessoren mit einer Frist von mindestens vierzehn (14) Tagen vorab und gibt dem Verantwortlichen die Möglichkeit, der Änderung

zu widersprechen (Art. 28 Abs. 2 DSGVO).

Die Information kann auch über eine jeweils aktuelle Subprozessorenliste im Trust Center erfolgen.

5.3 Widerspricht der Verantwortliche der Änderung aus einem wichtigen datenschutzrechtlichen Grund, und kann keine einvernehmliche Lösung gefunden werden, steht dem Verantwortlichen ein Sonderkündigungsrecht hinsichtlich der betroffenen Leistung zu.

5.4 Pakera verpflichtet jeden Subprozessor vertraglich auf im Wesentlichen dieselben Datenschutzpflichten, wie sie in diesem AVV festgelegt sind (Art. 28 Abs. 4 DSGVO), insbesondere auf hinreichende Garantien für geeignete technische und organisatorische Maßnahmen. Bei Subprozessoren in Drittländern stellt Pakera ein angemessenes Schutzniveau sicher (z. B. Angemessenheitsbeschluss oder EU-Standardvertragsklauseln nebst ergänzenden Maßnahmen, Art. 46 DSGVO).

6. Meldung von Datenschutzverletzungen

6.1 Pakera meldet dem Verantwortlichen jede Verletzung des Schutzes personenbezogener Daten, die im Verantwortungsbereich von Pakera oder ihrer Subprozessoren eingetreten ist, unverzüglich nach Bekanntwerden, in der Regel innerhalb von 48 Stunden.

6.2 Die Meldung enthält mindestens die nach Art. 33 Abs. 3 DSGVO erforderlichen Angaben, soweit Pakera bekannt. Pakera unterstützt den Verantwortlichen bei dessen Melde- und Benachrichtigungspflichten gegenüber der Aufsichtsbehörde (Art. 33 DSGVO) und gegenüber betroffenen Personen (Art. 34 DSGVO).

7. Kontroll- und Auditrechte

7.1 Der Verantwortliche hat das Recht, sich von der Einhaltung der vereinbarten Maßnahmen zu überzeugen (Art. 28 Abs. 3 lit. h DSGVO). Pakera stellt hierfür die erforderlichen Informationen bereit und kann den Nachweis vorrangig durch geeignete Zertifizierungen, aktuelle Testate oder Berichte unabhängiger Stellen führen.

7.2 Soweit ein Nachweis durch Dokumentation nicht ausreicht, kann der Verantwortliche nach rechtzeitiger Ankündigung (in der Regel mindestens 30 Tage vorab), während der üblichen Geschäftszeiten, ohne Störung des Betriebsablaufs und nicht häufiger als einmal jährlich (sowie anlassbezogen) eine Vor-Ort-Prüfung durchführen oder durch einen zur Vertraulichkeit verpflichteten Dritten durchführen lassen. Etwaige Kosten eigener Aufwände trägt jede Partei selbst; unverhältnismäßige Aufwände kann Pakera dem Verantwortlichen angemessen in Rechnung stellen.

8. Löschung und Rückgabe nach Vertragsende

8.1 Nach Beendigung der Verarbeitungsleistungen löscht Pakera nach Wahl des Verantwortlichen alle personenbezogenen Daten oder gibt sie zurück und vernichtet vorhandene Kopien, sofern keine gesetzliche Pflicht zur Speicherung besteht.

8.2 Im Einklang mit dem Hauptvertrag werden Kundendaten nach Ablauf eines Abruf-/

Rückgabefensters von 30 Tagen nach Vertragsende unwiderruflich gelöscht; innerhalb dieses Fensters kann der Verantwortliche die Löschung oder Rückgabe gemäß Ziffer 8.1 wählen. Ausgenommen sind Support-Tickets sowie Daten, die aus rechtlichen Gründen (z. B. handels- und steuerrechtliche Aufbewahrungsfristen) aufbewahrt werden müssen, sowie Sicherungskopien (Backups), die im Zuge des regulären Sicherungszyklus turnusmäßig überschrieben werden. Für alle noch nicht gelöschten Daten gelten bis zur Löschung eine eingeschränkte Verarbeitung und die Maßnahmen dieses AVV fort.

8.3 Pakera weist die Löschung bzw. Rückgabe auf Anforderung in geeigneter Form nach.

9. Schlussbestimmungen

9.1 Bei Widersprüchen zwischen diesem AVV und den AGB gehen hinsichtlich datenschutzrechtlicher Regelungen die Bestimmungen dieses AVV vor.

9.2 Es gilt deutsches Recht. Gerichtsstand ist, soweit zulässig, München.

9.3 Sollten einzelne Bestimmungen unwirksam sein, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt.

Anhang 1 – Beschreibung der Verarbeitung

Art der Verarbeitung: Erheben, Erfassen, Speichern, Organisieren, Ordnen, Anpassen, Auslesen, Abfragen, Verwenden, Übermitteln (im Rahmen von Freigabeprozessen), Löschen und Vernichten personenbezogener Daten im Rahmen des Betriebs der SaaS-Plattform Pakera.

Zweck der Verarbeitung: Bereitstellung und Betrieb der vertraglich vereinbarten SaaS-Leistungen (Verpackungs- und Logistikoptimierung), einschließlich Nutzer- und Rechteverwaltung, Authentifizierung, Erstellung und Freigabe von Verpackungsergebnissen/Packanweisungen sowie zugehöriger Kommentar-/Freigabefunktionen, Support.

Art der personenbezogenen Daten:

- Stammdaten der Nutzer: Name, geschäftliche E-Mail-Adresse, Telefonnummer, Adresse, Job-Titel, Arbeitgeber/Firmenname
- Zugangs- und Authentifizierungsdaten: Login, verschlüsseltes Passwort, OTP-/Token-Informationen, Rollen-/Rechtezuordnung;
- Nutzungs- und Protokolldaten: IP-Adresse, Geräte-/Browserinformationen, Log- und Zugriffsdaten, Sitzungsdaten;
- Inhaltsbezogene Daten, die personenbezogene Informationen enthalten können (z. B. in hochgeladenen CAD-/Office-Dateien, Kommentaren und Freigabeseiten unbeabsichtigt enthaltene personenbezogene Daten);
- Daten externer Teilnehmer von Freigabeprozessen (z. B. Name, E-Mail-Adresse zur Zustellung des Freigabelinks, Kommentare).

Kategorien betroffener Personen: Mitarbeitende und Berechtigte des Verantwortlichen (Owner, Admins, Classified User, User), externe Teilnehmer von Freigabe-/Kommentierungsprozessen sowie sonstige Personen, deren personenbezogene Daten in den hochgeladenen Inhalten enthalten sein können.

Hinweis zu besonderen Datenkategorien: Eine Verarbeitung besonderer Kategorien personenbezogener Daten (Art. 9 DSGVO) ist nicht vorgesehen. Der Verantwortliche stellt sicher, dass keine besonderen Datenkategorien ohne gesonderte Vereinbarung in die Plattform eingebracht werden.

Dauer der Verarbeitung: Für die Laufzeit des Hauptvertrags. Für den Projektverlauf gelten folgende Aufbewahrungsfristen: Nicht registrierte Nutzung: keine Speicherung; Free: Speicherung für 30 Tage, anschließend automatische Löschung; Pro: Speicherung für 180 Tage, anschließend automatische Löschung; Business und Enterprise: dauerhafte Archivierung des Projektverlaufs oder bis zum Ende des Abonnements.

Anhang 2 – Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

Vertraulichkeit

- Zutrittskontrolle: Hosting der Kerndaten in zertifizierten Rechenzentren in Deutschland (Subprozessor, siehe Anhang 3) mit Zutrittssicherung, Bewachung und Zugangsprotokollierung des Rechenzentrumsbetreibers.
- Zugangskontrolle: Passwortgeschützter Zugang; Passwortspeicherung nach Bcrypt; Einmalpasswörter (OTP) und Passwörter für Registrierung, Login und Freigabeseite; Mehr-Faktor-Authentifizierung (MFA) und Single Sign-On (SSO).
- Zugriffskontrolle: Rollen- und Rechtekonzept (RBAC) mit Rollen Owner, Admin, Classified User, User; projektbezogene Zugriffsbeschränkung für besonders sensible/klassifizierte Daten (Enterprise); Need-to-know-Prinzip für Mitarbeitende von Pakera.
- Verschlüsselung: Transportverschlüsselung nach TLS 1.3; Verschlüsselung ruhender Daten nach AES-256-GCM; optionale Verschlüsselung von CAD-Daten mit Kundenpasswort (Bring Your Own Key)

Integrität

- Eingabekontrolle: Protokollierung von Zugriffen und sicherheitsrelevanten Ereignissen (Zugriffs-Logs ab Tarif Business); Nachvollziehbarkeit von Freigaben und deren Dokumentation/Archivierung.
- Weitergabekontrolle: Verschlüsselte Übertragung; gesicherte Freigabelinks mit Zugangssicherung (OTP) und zeitlicher Befristung.

Verfügbarkeit und Belastbarkeit

- Mehrfach redundante Infrastruktur mit unterbrechungsfreier Stromversorgung beim Hosting-Subprozessor; angestrebte Verfügbarkeit 99,6 % im Jahresmittel.
- Regelmäßige Datensicherungen (Backups); Schutzmaßnahmen gegen DDoS-Angriffe über OVHcloud und/oder Cloudflare.

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

- Datenschutz-Management und Überprüfung der Maßnahmen; Ausrichtung an ISO/IEC 27001.
- Auftragskontrolle durch vertragliche Verpflichtung der Subprozessoren (siehe Anhang 3) und Weisungsbindung.
- Incident-Response- und Meldeprozess gemäß Ziffer 6.

Anhang 3 – Liste der Subprozessoren

Diese Liste umfasst Auftragsverarbeiter, die im Rahmen des Betriebs von Pakera personenbezogene Daten im Auftrag des Verantwortlichen verarbeiten können. Andere Dienste, wie Marketing-/Website-Dienste, bei denen Pakera selbst Verantwortliche ist, sind in der Datenschutzerklärung aufgeführt.

Subprozessor	Zweck / Leistung	Sitz / Verarbeitungsort	Transfermechanismus (bei Drittland)
OVH GmbH	Hosting, Rechenzentrum, Infrastruktur, DDoS-Schutz	Deutschland, Verarbeitung auf Servern in Deutschland	N.A.
HubSpot Germany GmbH	CRM, Marketing	Deutschland, Verarbeitung auf Servern in Deutschland	EU-Standardvertragsklauseln + ggf. EU-US Data Privacy Framework
Hanko GmbH	Authentifizierung, Login, MFA/SSO	Deutschland, Verarbeitung auf Servern in Deutschland	N.A.
Cloudflare, Inc.	Bot-/Missbrauchsschutz, DDoS-Schutz	USA, Verarbeitung auf globalen Servern	EU-Standardvertragsklauseln + ggf. EU-US Data Privacy Framework
Microsoft Ireland Operations Ltd.	Email, Nutzeranalyse Webseite	USA, Verarbeitung auf Servern in EU	EU-Standardvertragsklauseln + ggf. EU-US Data Privacy Framework
Google Ireland Ltd.	Nutzeranalyse Webseite	USA, Verarbeitung auf globalen Servern	EU-Standardvertragsklauseln + ggf. EU-US Data Privacy Framework
PostHog, Inc.	Nutzeranalyse Webseite	USA, Verarbeitung auf Servern in Deutschland	EU-Standardvertragsklauseln + ggf. EU-US Data Privacy Framework

Subprozessor	Zweck / Leistung	Sitz / Verarbeitungsort	Transfermechanismus (bei Drittland)
Brevo GmbH	Versand von Transaktions-/System-E-Mails	Deutschland, Verarbeitung auf Servern in Deutschland	N.A.
FooMonk LLC (Instantly)	Email Outreach	USA, Verarbeitung auf Servern in USA	EU-Standardvertragsklauseln
Livestorm SAS	Webinare	Frankreich, Verarbeitung auf Servern in Irland	N.A.
Tella HQ, Inc.	Videostreaming	USA, Verarbeitung auf Servern in USA	EU-Standardvertragsklauseln
Framer B.V.	Marketingwebsite Hosting, Analyse	Niederlande, Verarbeitung auf Servern in USA	EU-US-DPF, sofern zutreffend; andernfalls EU-SCCs

Pakera AI Packaging Optimization GmbH · Brunnenweg 35, 83666 Waakirchen ·
 info@pakera.com