

Vertrag zur Auftragsverarbeitung (AVV)

gemäß Art. 28 DSGVO – cheezee als Auftragsverarbeiter

1. Parteien

Verantwortlicher: [Fotograf/Fotostudio, Anschrift].

Auftragsverarbeiter: SmartLab 35, Inhaber Santiago Ramirez Sonntag, Eichsfeld 24, 36037 Fulda, Deutschland; E-Mail: info@smartlab35.com; USt-IdNr.: DE368278017. Die Plattform wird unter der Produktbezeichnung „cheezee“ angeboten.

2. Gegenstand und Dauer

Gegenstand ist die Verarbeitung personenbezogener Daten im Rahmen der Bereitstellung der cheezee-Plattform. Die Verarbeitung dauert grundsätzlich für die Laufzeit des SaaS-Vertrags zuzüglich technisch und gesetzlich erforderlicher Lösch-/Abwicklungsfristen.

3. Art und Zweck der Verarbeitung

Hosting, Speicherung, Strukturierung, Abruf, Übermittlung innerhalb der vom Verantwortlichen freigegebenen Workflows, Galerie-/Bestellbereitstellung, E-Mail-Workflows, Termin-/Shootingverwaltung, technische Bildverarbeitung, ggf. automatisierte Gesichtszuordnung, Support, Datensicherung, Sicherheitsprotokollierung und Löschung.

4. Datenarten

Stammdaten und Kontaktdaten von Eltern/Erziehungsberechtigten; Kinderprofile (z. B. Name, Gruppe/Klasse, Zuordnung zum Elternkonto); Foto- und Bilddaten; Referenzbilder; ggf. Gesichtsausschnitte und numerische Gesichtsmerkmale/Embeddings; Buchungs-, Bestell- und Downloaddaten; Kommunikationsdaten; Einwilligungs-/Nachweisdaten; technische Protokoll- und Geräte-/Verbindungsdaten.

5. Betroffene Personen

Kunden/Benutzer des Fotografen; Eltern und sonstige Sorgeberechtigte; Kinder/Minderjährige; abgebildete Familienangehörige; Beschäftigte/Benutzer des Studios; ggf. Ansprechpartner von Einrichtungen.

6. Weisungsbindung

cheezee verarbeitet Auftragsdaten ausschließlich auf dokumentierte Weisung des Verantwortlichen, soweit keine unionsrechtliche oder nationale gesetzliche Verpflichtung eine Verarbeitung verlangt. Offensichtlich rechtswidrige Weisungen werden beanstandet und bis zur Klärung nicht umgesetzt, soweit erforderlich.

7. Vertraulichkeit

cheezee stellt sicher, dass zur Verarbeitung befugte Personen auf Vertraulichkeit verpflichtet sind und nur im erforderlichen Umfang Zugriff erhalten.

8. Sicherheit der Verarbeitung

cheezee trifft angemessene technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO. Die aktuelle TOM-Anlage ist Bestandteil dieses Vertrags. Maßnahmen werden risikoorientiert weiterentwickelt, ohne das vereinbarte Schutzniveau zu unterschreiten.

9. Unterauftragsverarbeiter

Der Verantwortliche erteilt eine allgemeine Genehmigung zum Einsatz der in Anlage 2 genannten Unterauftragsverarbeiter. Neue oder ersetzte Unterauftragsverarbeiter werden mindestens 14 Tage vorher elektronisch angekündigt. Der Verantwortliche kann aus begründeten datenschutzrechtlichen Gründen widersprechen. Die Parteien bemühen sich um eine zumutbare Lösung; ist diese nicht möglich, kann der betroffene Dienst nach Maßgabe des Hauptvertrags beendet werden.

10. Unterstützung des Verantwortlichen

cheezee unterstützt den Verantwortlichen unter Berücksichtigung der Art der Verarbeitung bei Betroffenenanfragen, Datenschutz-Folgenabschätzungen, Konsultationen von Aufsichtsbehörden und bei der Erfüllung der Pflichten nach Art. 32 bis 36 DSGVO, soweit die betreffenden Informationen bei cheezee verfügbar sind.

11. Datenschutzvorfälle

cheezee informiert den Verantwortlichen unverzüglich nach Bekanntwerden einer Verletzung des Schutzes personenbezogener Auftragsdaten und stellt die verfügbaren Informationen bereit, die der Verantwortliche für seine Bewertung und etwaige Meldungen benötigt. Das Verfahren umfasst mindestens Zeitpunkt, Art des Vorfalls, betroffene Systeme/Daten, mögliche Folgen, ergriffene bzw. geplante Gegenmaßnahmen und Ansprechpartner.

12. Nachweise und Audits

cheezee stellt erforderliche Informationen zum Nachweis der Einhaltung von Art. 28 DSGVO bereit. Audits sollen vorrangig durch geeignete Dokumentation, Zertifikate oder standardisierte Prüfberichte erfolgen. Vor-Ort-Prüfungen sind bei berechtigtem Anlass und nach angemessener Vorankündigung möglich, unter Wahrung von Betriebs- und Geschäftsgeheimnissen sowie Rechten anderer Kunden.

13. Drittlandübermittlungen

Eine Verarbeitung außerhalb EU/EWR erfolgt nur bei Vorliegen der Voraussetzungen der Art. 44 ff. DSGVO und wird in der Unterauftragsverarbeiterliste transparent gemacht. Geeignete Garantien, insbesondere Angemessenheitsbeschlüsse oder Standardvertragsklauseln, werden soweit erforderlich eingesetzt.

14. Vertragsende und Löschung

Nach Ende der Verarbeitung löscht oder gibt cheezee die Auftragsdaten nach dokumentierter Weisung des Verantwortlichen zurück, soweit keine gesetzliche Pflicht zur weiteren Speicherung besteht. Der Fotograf bzw. das Fotostudio bestimmt als Verantwortlicher insbesondere, wie lange gekaufte Bilddateien seinen Kunden zum Download bereitgestellt und wann diese anschließend gelöscht werden. cheezee setzt die vom Verantwortlichen festgelegten Fristen und Löschweisungen technisch um. Backupkopien laufen innerhalb der dokumentierten Rotation aus; bei Restore werden Löschmarker bzw. Löschaufträge erneut angewandt.

Anlage 1 – Technische und organisatorische Maßnahmen

- Zutritts-/physische Sicherheit: Nutzung professioneller Rechenzentren; physischer Zugang nur durch autorisierte Betreiber.
- Zugangskontrolle: individuelle Benutzerkonten; sichere Passwortspeicherung; Admin-/Superadmin-Berechtigungen nach Rollenprinzip; MFA für privilegierte Zugänge vor Produktivstart vorsehen.
- Zugriffskontrolle: Mandantentrennung, rollenbasierte Berechtigungen, Least-Privilege-Prinzip, Trennung von Eltern-, Studio- und Superadmin-Funktionen.
- Übertragung: TLS für Webzugriffe und API-Kommunikation; verschlüsselte administrative Zugänge.
- Speicherung: Datenbank und Object Storage in EU-Standort; Secrets nicht im Quellcode; Zugangsdaten verschlüsselt/geschützt.
- Protokollierung: sicherheitsrelevante Admin-, Login-, Zahlungs- und Verarbeitungsvorgänge angemessen protokollieren; Protokolle zeitlich begrenzen.
- Verfügbarkeit: Backup-/Restore-Verfahren, Monitoring, Patchmanagement, dokumentierte Wiederherstellungsprozesse.
- Mandantenfähigkeit: logische Trennung sämtlicher Kundendaten und Storage-Keys; automatisierte Tests gegen Cross-Tenant-Zugriffe.
- KI-Verarbeitung: Verarbeitung nur für den konkreten Kundenauftrag; keine allgemeine Modellschulung mit Kundenbildern; frühzeitige Löschung temporärer Artefakte.
- Löschung: zentral dokumentierte Löschjobs für Shootings, Accounts, Embeddings, Previews, Logs und Backups; Löschstatus nachvollziehbar protokollieren.

Anlage 2 – Unterauftragsverarbeiter (auszufüllen)

Anbieter	Leistung	Daten/Verarbeitung	Ort	Transfergrundlage
Hetzner Online GmbH / [genaue Einheit]	Hosting/Object Storage	Plattform-, DB-, Bild-/Backupdaten	[DE/FI/EU]	EU/EWR
Stripe Payments Europe, Ltd. / relevante Stripe-Einheit	Zahlungsabwicklung/Connect	Zahlungs-, Transaktions-, Kontodaten	EU	EU