Vertrag zur Auftragsverarbeitung (AVV) für Kitaeule

gemäß Art. 28 Datenschutz-Grundverordnung (DSGVO)

Vertragsparteien

Verantwortlicher (Auftraggeber):

Kita: _____

Träger: _____

Anschrift: _____

Vertreten durch: _____

E-Mail: _____

Auftragsverarbeiter (Auftragnehmer):

IT-Service Clemens, Maximilian Clemens
Über der Delle 18, 57482 Wenden
E-Mail: maximilian.clemens@it-clemens.de

§ 1 Gegenstand und Dauer

(1) Der Auftragnehmer stellt dem Auftraggeber die Web-App Kitaeule (app.kitaeule.de) für die Kommunikation und Verwaltung zwischen Kita und Eltern bereit und verarbeitet dabei personenbezogene Daten im Auftrag des Auftraggebers.

(2) Der Vertrag gilt, solange der Auftraggeber Kitaeule nutzt. Er endet mit der Kündigung der Nutzung.

§ 2 Art und Zweck der Verarbeitung

(1) Art: Erheben (Eingaben der Kita und der Eltern), Speichern, Abfragen und Anzeigen für berechtigte Nutzer, Übermitteln zwischen Nutzern derselben Kita, Sichern und Löschen.

(2) Zweck:

- Verwaltung der Kita-Stammdaten (Gruppen, Kinder, Team)
- Verknüpfung der Eltern mit ihren Kindern über Einladungscodes
- Kommunikation zwischen Kita und Eltern (Pinnwand, Nachrichten), sobald verfügbar
- Abwesenheiten und Termine, sobald verfügbar

§ 3 Art der Daten

(1) Kinder: Vorname, Nachname, Geburtsdatum (freiwillig), Gruppe, Verknüpfung mit Eltern; Abwesenheiten mit Grund, sobald verfügbar.

(2) Eltern und Mitarbeitende: E-Mail-Adresse, Rolle in der Kita (Leitung, Erzieher:in, Eltern), Zuordnung zu Kindern, Inhalte der Kommunikation, sobald verfügbar.

(3) Technische Daten: Sitzungsdaten, Protokolle der Server (IP-Adresse, Zeit, Adresse), Passkeys.

(4) Nicht verarbeitet werden Gesundheitsdaten (Art. 9 DSGVO), Fotos der Kinder und Zahlungsdaten.

§ 4 Betroffene Personen

Kinder der Einrichtung, ihre Eltern und Erziehungsberechtigten, Mitarbeitende der Einrichtung.

§ 5 Pflichten des Auftragnehmers

(1) Der Auftragnehmer
a) verarbeitet die Daten nur auf dokumentierte Weisung des Auftraggebers; die Nutzung der App durch den Auftraggeber gilt als Weisung,
b) verpflichtet alle Personen, die Zugang zu den Daten haben, zur Vertraulichkeit,
c) trifft die technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO (Anlage 1),
d) hält die Bedingungen für Unterauftragsverarbeiter ein (§ 7),
e) unterstützt den Auftraggeber bei Anfragen Betroffener (Auskunft, Berichtigung, Löschung, Datenübertragbarkeit),
f) unterstützt den Auftraggeber bei den Pflichten nach Art. 32 bis 36 DSGVO,
g) löscht oder übergibt nach Vertragsende alle Daten (§ 10),
h) stellt alle nötigen Informationen bereit und ermöglicht Überprüfungen.

(2) Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn eine Weisung nach seiner Auffassung gegen Datenschutzrecht verstößt.

§ 6 Pflichten des Auftraggebers

Der Auftraggeber
a) stellt die Rechtmäßigkeit der Verarbeitung sicher, insbesondere informiert er Eltern und Mitarbeitende nach Art. 13 DSGVO und holt nötige Einwilligungen ein,
b) gibt Einladungscodes nur an die berechtigten Personen weiter,
c) entfernt Kinder, Eltern und Mitarbeitende, die die Einrichtung verlassen, zeitnah aus der App.

§ 7 Unterauftragsverarbeiter

(1) Genehmigt sind:

Unterauftragnehmer	Tätigkeit	Standort
Hetzner Online GmbH, Gunzenhausen	Server (Rechenzentrum), Versand von E-Mails	Deutschland
IONOS SE, Montabaur	Speicher für die Sicherungen der Datenbank	Deutschland (Frankfurt am Main)

(2) Über neue Unterauftragnehmer informiert der Auftragnehmer vorher per E-Mail. Der Auftraggeber kann binnen 14 Tagen widersprechen und bei berechtigtem Widerspruch außerordentlich kündigen.

§ 8 Kontrollrechte

Der Auftraggeber kann sich nach Absprache von den Maßnahmen in Anlage 1 überzeugen. Der Auftragnehmer erteilt dazu Auskunft.

§ 9 Meldung von Datenschutzverletzungen

Der Auftragnehmer meldet dem Auftraggeber eine Verletzung des Schutzes personenbezogener Daten unverzüglich, spätestens innerhalb von 24 Stunden nach Kenntnis,

mit Art der Verletzung, betroffenen Daten und Personen, wahrscheinlichen Folgen und ergriffenen Maßnahmen.

§ 10 Löschung und Rückgabe

Nach Vertragsende exportiert der Auftragnehmer die Daten auf Wunsch und löscht sie spätestens nach 30 Tagen. Gelöschte Daten sind in den Sicherungen noch bis zu 30 Tage enthalten und werden dann überschrieben. Die Löschung bestätigt der Auftragnehmer per E-Mail.

§ 11 Haftung und Schluss

(1) Die Haftung richtet sich nach Art. 82 DSGVO.
(2) Änderungen bedürfen der Textform. Es gilt deutsches Recht.
(3) Ist eine Bestimmung unwirksam, bleibt der Rest wirksam.

Zustimmung

Kita / Träger, Ort, Datum, Name: _____

IT-Service Clemens, Ort, Datum, Name: _____

Anlage 1: Technische und organisatorische Maßnahmen (Stand November 2026)

Vertraulichkeit

- **Zutritt:** Server in Rechenzentren der Hetzner Online GmbH in Deutschland (ISO 27001), kein eigener Serverraum.
- **Zugang:** Anmeldung über Keycloak mit Passkey oder Einmal-Code per E-Mail, Passwort nur als Rückfall und nur gehasht. Administrativer Zugang zu den Servern nur für den Betreiber, mit Schlüssel bzw. Passkey.
- **Zugriff:** Rollen je Kita (Leitung, Erzieher:in, Eltern). Eltern sehen nur ihre eigenen Kinder. Jede Abfrage ist auf die Kita des angemeldeten Kontos beschränkt; automatische Tests prüfen für jede Funktion, dass eine andere Kita nichts sieht.
- **Trennung:** Jede Kita ist ein eigener Mandant (facility_id). Produktion, Testsystem und andere Dienste laufen in getrennten Namespaces mit Netzwerkregeln; die Datenbank ist nur für die App erreichbar.
- **Einladungscodes:** gelten 14 Tage, nur einmal, und werden nur als Prüfsumme gespeichert.

Integrität

- **Weitergabe:** nur verschlüsselt (HTTPS mit TLS, HSTS). Zugriffstokens bleiben auf dem Server, der Browser bekommt nur ein Sitzungs-Cookie (httpOnly, SameSite). Keine Inhalte oder Skripte von Dritten.

Verfügbarkeit

- Tägliche Sicherung der Datenbank mit fortlaufender Archivierung, Aufbewahrung 30 Tage.

Überprüfung

- Updates der Komponenten zeitnah; Änderungen nur über geprüfte Pull Requests mit automatischen Tests.