

Hosting-Standorte und Datenflüsse

Technische Architektur von KinderAlbum

Stand: 11. Oktober 2026. Geprüft am laufenden System.

1. Komponenten

Komponente	Aufgabe	Betrieb	Standort
Caddy	TLS-Verschlüsselung, Weiterleitung an die Dienste	selbst	Hetzner Cloud, Nürnberg
Anwendung (Next.js)	Oberfläche, Rechteprüfung, Geschäftslogik	selbst	Hetzner Cloud, Nürnberg
Supabase (PostgreSQL, Anmeldung, API)	Konten, Kinder, Eltern, Einwilligungen, Protokolle	selbst	Hetzner Cloud, Nürnberg
Kong	interne Weiterleitung zu Datenbank- und Anmeldediensten	selbst	Hetzner Cloud, Nürnberg
imgproxy mit Zwischenspeicher	Erzeugung von Vorschaubildern	selbst	Hetzner Cloud, Nürnberg
Supabase Studio	Verwaltung der Datenbank durch den Betreiber, zusätzlich passwortgeschützt	selbst	Hetzner Cloud, Nürnberg
Umami	Reichweitenmessung der Website (nicht der Plattform), ohne Cookies; misst auch weitere Websites des Betreibers	selbst	Hetzner Cloud, Nürnberg
Protokolldienste (Vector, Logflare)	interne Protokolle der Anmelde- und Datenbankdienste	selbst	Hetzner Cloud, Nürnberg
Hetzner Object Storage	Fotodateien, Kopie der Fotodateien, verschlüsselte Datenbanksicherungen	Hetzner	Nürnberg

Komponente	Aufgabe	Betrieb	Standort
Amazon SES	Versand von E-Mails	AWS EMEA SARL	Frankfurt
Google Workspace	Postfächer des Betreibers (Support, Kontaktanfragen, technische Meldungen)	Google Cloud EMEA Ltd.	EU, Übermittlung in die USA möglich

Alle selbst betriebenen Dienste laufen in Docker-Containern auf einem Server mit Ubuntu 24.04 LTS. Von außen offen sind nur die Ports 22, 80 und 443.

2. Übersicht

```

`` Einrichtung / Galerie-Inhaber Eltern / Empfänger eines Links | | +-----
----- HTTPS -----+ | Caddy (TLS), Server in Nürnberg | +-----
-----+-----+ | | Anwendung Datenbank Object Storage
(Prüfung der (Konten, Kinder, (Fotodateien, Rechte) Einwilligungen) nicht öf-
fentlich) | | | verschlüsselte Sicherung tägliche Kopie | (Nürnberg) (Nürn-
berg) | Amazon SES (Frankfurt) ----> Einladungs- und Benachrichtigungsmails ``

```

3. Datenflüsse mit Elternkonten (Einrichtungen)

3.1 Einrichtung vorbereiten

1. Die Einrichtung legt Gruppen an und importiert Kinder (Vorname, Nachname, Geburtsdatum, Gruppe), einzeln oder als CSV-Datei.
2. Eltern werden eingeladen: per QR-Einladungskarte, per E-Mail oder per CSV-Datei (Name, E-Mail-Adresse, Kind, Beziehung).
3. E-Mail-Einladungen werden über Amazon SES versendet und gelten 7 Tage.

3.2 Fotos hochladen

1. Eine Fachkraft lädt Fotos in ein Album (JPEG, PNG, HEIC und weitere, bis 30 MB pro Foto).
2. Die Datei wird per HTTPS übertragen und im nicht öffentlichen Objektspeicher in Nürnberg abgelegt.
3. Auf dem Server entstehen Vorschaubilder ohne EXIF- und GPS-Daten.

4. Das Album bleibt für Eltern unsichtbar, bis es veröffentlicht und einer oder mehreren Gruppen zugeordnet ist.

3.3 Eltern sehen und laden Fotos

1. Das Elternteil meldet sich mit eigenem Konto an.
2. Die Anwendung prüft: Album veröffentlicht, der Gruppe des eigenen Kindes zugeordnet, gültige Einwilligung für das eigene Kind, Foto nicht ausgeblendet.
3. Ausgeliefert wird über signierte Links mit kurzer Laufzeit.
4. Herunterladen einzeln (Originaldatei) oder als ZIP-Datei je Album mit bis zu 200 Fotos (Vorschaubilder in voller Breite ohne Metadaten; fehlt ein Vorschaubild, das Original).
5. Ansichten und Downloads werden im Audit-Protokoll vermerkt.

3.4 Widerruf einer Einwilligung

1. Die Einrichtung erfasst den Widerruf beim Kind. Hat die Einrichtung es freigeschaltet, widerrufen Eltern selbst in ihrem Konto, ohne Begründung.
2. Ab sofort sehen die Eltern dieses Kindes keine Alben mehr. Ein bereits erzeugter ZIP-Link bleibt höchstens noch eine Stunde gültig. Heruntergeladene Dateien bleiben naturgemäß bei den Eltern.
3. **Fotos, auf denen dieses Kind zu sehen ist, bleiben für die übrigen berechtigten Eltern der Gruppe sichtbar**, bis die Einrichtung sie ausblendet oder löscht. Die Plattform erkennt nicht, welche Kinder auf einem Foto abgebildet sind.

4. Datenflüsse bei Galerien mit Link und PIN

1. Der Inhaber lädt Fotos in eine Galerie. Ablage und Vorschaubilder wie in 3.2.
2. Er teilt einen Link mit PIN oder Passwort, für die ganze Galerie oder als persönlichen Link je Kind. Fotografierte QR-Karten ordnen die folgenden Fotos automatisch einem Kind zu.
3. Der Empfänger öffnet den Link, gibt die PIN ein und sieht die Galerie bzw. die Fotos seines Kindes mit den bestätigten Gruppenfotos. Eine Einwilligungsprüfung je Kind findet nicht statt; der Inhaber hat die Rechtsgrundlage bei der Registrierung erklärt.
4. Herunterladen einzeln oder als ZIP-Datei (Originaldateien bis 200 Fotos, darüber Vorschaubilder).

5. Zugriffe werden mit gekürztem Hashwert der IP-Adresse und Browserkennung protokolliert und nach 90 Tagen gelöscht.

5. Drittlandübermittlung

- Fotos, Kinder- und Elterndaten liegen ausschließlich in **Deutschland** (Nürnberg). Sie verlassen den Server nur in Richtung der Berechtigten und in die Kopie im selben Rechenzentrum. Die Protokolle der selbst betriebenen Dienste und die Daten der Reichweitenmessung liegen ebenfalls auf dem Server in Nürnberg.
- E-Mails werden über Amazon SES in **Frankfurt** versendet. AWS EMEA SARL gehört zu einem US-Konzern.
- Die Postfächer des Betreibers liegen bei Google Workspace (EU, Übermittlung in die USA möglich). Einzelheiten im Dokument [Unterauftragsverarbeiter](#).

Diese Darstellung stellt keine Rechtsberatung dar.