

Technische und organisatorische Maßnahmen (TOM)

nach Art. 32 DSGVO, Anlage zum Auftragsverarbeitungsvertrag

Stand: 11. Oktober 2026. Alle Angaben wurden an diesem Tag gegen den Quellcode und das laufende System geprüft.

Dieses Dokument beschreibt, was tatsächlich umgesetzt ist. Was es derzeit nicht gibt, steht ausdrücklich in Abschnitt 7. Sie sollen eine Lücke nicht erst im Betrieb entdecken.

1. Vertraulichkeit

1.1 Zutrittskontrolle

- Betrieb auf einem Cloud-Server der Hetzner Online GmbH im Rechenzentrum **Nürnberg**.
- Physische Sicherung durch Hetzner nach dessen Angaben (Zutrittskontrolle, Videoüberwachung, Personal rund um die Uhr); Hetzner ist nach ISO/IEC 27001 zertifiziert.
- Der Auftragsverarbeiter hat keinen physischen Zugang zur Hardware.

1.2 Zugangskontrolle

- Persönliche Konten mit Passwort für alle Nutzergruppen, Mindestlänge 8 Zeichen.
- Anmeldung über Supabase Auth, selbst betrieben auf demselben Server. Sitzungen beruhen auf signierten Tokens mit einer Laufzeit von einer Stunde, die automatisch erneuert werden.
- Fachkräfte und Eltern erhalten einen persönlichen Einladungscode, der nach 7 Tagen verfällt. Einladungen für Träger-Zugänge gelten 14 Tage.
- Serverzugang für den Betreiber ausschließlich per SSH-Schlüssel; die Anmeldung per Passwort ist abgeschaltet.
- Von außen erreichbar sind nur die Ports 22 (SSH), 80 und 443 (Web). Die Datenbank ist aus dem Internet nicht direkt erreichbar.

- Das Verwaltungswerkzeug der Datenbank ist zusätzlich durch einen eigenen Passwortschutz gesichert.

1.3 Zugriffskontrolle

Jede Prüfung erfolgt auf dem Server, nicht im Browser.

Rolle	Darf
Schulverwaltung (Einrichtung)	alle Alben, Gruppen, Kinder, Eltern und Einwilligungen der eigenen Einrichtung; Kollegium einladen; Tarif verwalten
Fachkraft (Einrichtung)	Alben der eigenen Gruppen; Kinder, Eltern und Einwilligungen der ganzen Einrichtung
Träger	Übersicht der eigenen Einrichtungen, Nutzungszahlen, Namen und E-Mail-Adressen der Mitarbeitenden, Verträge und Rechnungen. Kein Zugriff auf Kinder, Fotos, Alben oder Einwilligungen
Elternteil	Fotos nur unter den vier Bedingungen unten
Inhaber einer Galerie	eigene Galerien, Fotos und Links
Empfänger eines Galerie-Links	die Galerie, für die Link und PIN gelten (Abschnitt 1.4)
Betreiber	ein einziges Betreiberkonto (siehe Abschnitt 5)

Eltern sehen ein Foto nur, wenn alle Bedingungen erfüllt sind:

1. das Album ist veröffentlicht,
2. das Album ist der Gruppe des eigenen Kindes zugeordnet,
3. für das **eigene Kind** liegt eine gültige Einwilligung vor,
4. das Foto ist nicht ausgeblendet.

Weitere Maßnahmen:

- Fotodateien liegen in einem **nicht öffentlichen** Speicher. Ausgeliefert werden sie nur über signierte, zeitlich begrenzte Links: Ansicht 1 Stunde, Einzeldownload 5 Minuten, ZIP-Datei 1 Stunde.

- Row Level Security ist auf **allen 42 Tabellen** der Anwendung aktiv, zusätzlich zur Prüfung in der Anwendung.
- Jede Serveraktion ist an die angemeldete Sitzung gebunden. Ein automatischer Test verhindert, dass eine neue Aktion ohne diese Prüfung ausgeliefert wird.

1.4 Galerien mit Link und PIN

- Eine Galerie ist nur mit Link **und** PIN (4 Ziffern, automatisch erzeugt) oder einem selbst gewählten Passwort erreichbar.
- Nach 5 falschen Eingaben innerhalb von 15 Minuten wird ein Gerät gesperrt, nach 30 falschen Eingaben pro Stunde der ganze Link.
- Die PIN wird als SHA-256-Hashwert gespeichert. Automatisch erzeugte vierstellige PINs werden zusätzlich im Klartext gespeichert, damit der Inhaber sie erneut anzeigen und weitergeben kann; wer Zugriff auf die Datenbank hat, kann sie also lesen.
- Ein persönlicher Link für ein Kind zeigt nur die Fotos dieses Kindes und die bestätigten Gruppenfotos. Ein allgemeiner Galerie-Link zeigt die ganze Galerie, einschließlich der Originaldateien zum Herunterladen.

1.5 Trennungskontrolle

- Jede Einrichtung und jedes Galerie-Konto hat eine eigene Kennung. Alle Abfragen sind auf die Einrichtung bzw. das Konto des angemeldeten Nutzers und seine Rolle beschränkt (Abschnitt 1.3); Daten anderer Einrichtungen oder Konten sind nicht erreichbar.

2. Integrität

2.1 Weitergabekontrolle

- Sämtlicher Datenverkehr ist per **TLS 1.2 oder 1.3** verschlüsselt (Zertifikate von Let's Encrypt, Reverse Proxy Caddy).
- HSTS (`max-age=31536000; includeSubDomains; preload`) und weitere Sicherheits-Header, darunter eine Content Security Policy.
- Kein CDN und kein vorgeschalteter Dienst eines Dritten. Die Domains zeigen direkt auf den Server in Nürnberg.

2.2 Eingabekontrolle

- **Audit-Protokoll** für Upload, Löschen und Ausblenden von Fotos, Albumaktionen, Ansichten und Downloads durch Eltern, Änderungen von Einwilligungen, Registrierungen sowie Aktionen des Betreibers. Gespeichert werden handelnde Person, Aktion, betroffener Datensatz, Zeitpunkt, IP-Adresse und Browserkennung.
- **Einwilligungen werden nicht überschrieben.** Jede Änderung beendet den bisherigen Eintrag und legt einen neuen an, mit Zeitpunkt, erfassender Person und bei Widerruf einer Begründung.

3. Verfügbarkeit und Belastbarkeit

Was	Wie	Wo	Aufbewahrung
Datenbank	tägliche Sicherung, verschlüsselt mit AES-256	Hetzner Object Storage, Nürnberg, zusätzlich auf dem Server	35 Tage im Speicher, 7 Tage auf dem Server
Fotodateien	tägliche Kopie in einen getrennten Speicherbereich	Hetzner Object Storage, Nürnberg	gelöschte Dateien fallen nach höchstens 7 Tagen heraus

- Nach jedem Lauf wird geprüft, dass die Datenbanksicherung vollständig hochgeladen ist. Am 11. Oktober 2026 wurde zusätzlich eine Sicherung entschlüsselt und ihr Inhaltsverzeichnis geprüft. Eine vollständige Probe-Wiederherstellung steht noch aus (Abschnitt 7).
- Automatische Sicherheitsupdates des Betriebssystems (Ubuntu 24.04 LTS, täglich über unattended-upgrades).
- Fehler in den Protokollen werden alle 15 Minuten ausgewertet und an den Betreiber gemeldet.
- Brandschutz, Notstrom und redundante Anbindung durch das Rechenzentrum nach Angaben von Hetzner.

4. Datenschutz durch Technikgestaltung (Art. 25 DSGVO)

- Fotos sind nach dem Hochladen für Eltern **nicht sichtbar**, bis das Album veröffentlicht ist.
- Ohne gültige Einwilligung für das eigene Kind sehen Eltern kein Album.

- **Bildmetadaten:** Vorschaubilder werden ohne EXIF- und GPS-Daten ausgeliefert. Beim Herunterladen eines einzelnen Fotos erhält man die Originaldatei mit ihren Metadaten. Wir empfehlen, in der Kamera-App die Speicherung des Aufnahmeorts abzuschalten.
- **Gesichter:** Zur automatischen Drehung von Fotos erkennt der Server, wo im Bild Gesichter sind. Personen werden dabei nicht identifiziert, es werden keine biometrischen Merkmale gespeichert, und es ist kein Dritter beteiligt.
- Keine Werbung, keine Tracking-Dienste Dritter, keine Schriftarten oder Skripte von fremden Servern. Die Reichweitenmessung Umami läuft auf dem eigenen Server, setzt keine Cookies und wird auf der Website erst nach Zustimmung geladen.
- Keine KI-Dienste Dritter. Fotos verlassen den Server nicht zur Analyse.

5. Organisatorische Maßnahmen

- Der Dienst wird von Vadim Shchepin als Einzelunternehmer betrieben. Es gibt keine weiteren Personen mit Zugang zu personenbezogenen Daten.
- Es gibt ein einziges Betreiberkonto. Meldet sich der Betreiber zur Unterstützung als ein Nutzer an, wird das vorher im Audit-Protokoll vermerkt; der Nutzer wird darüber nicht automatisch benachrichtigt. Ansichten von Kindern und Fotos einer Einrichtung durch den Betreiber werden protokolliert, Ansichten von Fotos in Galerien derzeit nicht.
- Verletzungen des Schutzes personenbezogener Daten werden dem Verantwortlichen unverzüglich, spätestens binnen **48 Stunden** nach Kenntnis gemeldet (AVV § 9). Der Ablauf von Erkennen, Eindämmen, Bewerten, Melden und Dokumentieren ist schriftlich festgelegt.
- Ein Verzeichnis der Verarbeitungstätigkeiten als Auftragsverarbeiter nach Art. 30 Abs. 2 DSGVO wird geführt.
- Unterauftragsverarbeiter nur mit Vertrag nach Art. 28 DSGVO (Dokument [Unterauftragsverarbeiter](#)).

6. Verfahren zur regelmäßigen Überprüfung

- Bei jeder Änderung am Code laufen automatische Tests, darunter eine Prüfung der Zugriffsrechte aller Serveraktionen. Ohne bestandene Tests wird nichts ausgeliefert.
- Die Angaben in diesem Dokument werden bei jeder wesentlichen Änderung neu gegen das laufende System geprüft. Das Datum steht oben.

7. Grenzen, offen benannt

Thema	Stand
Zwei-Faktor-Anmeldung	nicht vorhanden
Verschlüsselung der Serverfestplatte und der Datenbank	nicht vorhanden. Die Datenbanksicherungen sind verschlüsselt, die Kopie der Fotodateien nicht.
Unabhängige Sicherung	Die Kopie der Fotodateien liegt beim selben Anbieter im selben Rechenzentrum. Sie schützt vor versehentlichem Löschen, nicht vor einem Ausfall des Rechenzentrums.
Probe-Wiederherstellung	Eine vollständige Wiederherstellung aus der Sicherung wurde noch nicht durchgeführt und dokumentiert.
Metadaten in Originaldateien	Einzeldownloads sind Originaldateien mit EXIF- und gegebenenfalls GPS-Daten. In ZIP-Dateien wird ein Original verwendet, wenn kein Vorschaubild vorliegt.
Rechte von Fachkräften	Die Rolle Fachkraft beschränkt Alben auf die eigenen Gruppen, nicht aber Kinder, Eltern und Einwilligungen.
PIN im Klartext	Automatisch erzeugte PINs sind zusätzlich lesbar gespeichert (Abschnitt 1.4).
Galerien in Einrichtungen	Fachkräfte einer Einrichtung können zusätzlich Galerien mit Link und PIN anlegen. Diese laufen ohne Einwilligungsprüfung je Kind (Dokument Rollen, Rechtsgrundlage und Sichtbarkeit).
Protokollierung	Anmeldungen, das Löschen eines Kindes und Ansichten von Galerie-Fotos durch den Betreiber werden nicht im Audit-Protokoll vermerkt.
Dienstprotokolle	Die internen Protokolle der Anmelde- und Datenbankdienste werden derzeit länger als 90 Tage aufbewahrt (Dokument Speicher- und Löschkonzept , Abschnitt 3).
Vorschaubilder bei Galerien	Wird ein Foto, eine Galerie oder ein Galerie-Konto gelöscht, bleiben die Vorschaubilder derzeit im Speicher. Ohne Datenbankeintrag sind sie über die Plattform nicht mehr erreichbar.
Automatische Löschung	Ein Ablaufdatum sperrt eine Galerie, löscht sie aber nicht. Löschungen erfolgen durch den Verantwortlichen oder auf Weisung.
Vollständiger Datenexport	Fotos als ZIP-Datei je Album; ein Export aller Daten eines Kontos in einer Datei erfolgt auf Anfrage.

Diese Darstellung beschreibt die technische Umsetzung und stellt keine Rechtsberatung dar.