

Technische und organisatorische Maßnahmen (TOM)

Öffentliche Fassung für Kitas und Träger

Version 1.0 · Stand August 2026

Diese öffentliche Fassung beschreibt die wesentlichen Schutzmaßnahmen auf einem für Kitas, Träger und Datenschutzbeauftragte geeigneten Niveau. Sicherheitskritische interne Betriebsdetails werden nicht veröffentlicht.

1. Zugang und Berechtigungen

- Individuelle Benutzerkonten und rollenbasierte Berechtigungen.
- Serverseitige Autorisierungsprüfungen für Einrichtung, Gruppe, Eltern-Kind-Zuordnung, Chatteilnahme und geschützte Ressourcen.
- Administrative Zugriffe werden auf erforderliche Personen und Aufgaben begrenzt; nicht mehr benötigte Rechte werden entzogen.

2. Trennung und Zugriffskontrolle

- Datenzugriffe werden serverseitig geprüft und nicht allein durch die Darstellung in der App gesteuert.
- Private Kommunikationsbereiche sind teilnehmerbezogen; Medien und Dateien werden ressourcenbezogen autorisiert.
- Supportzugriffe auf fachliche Inhalte erfolgen nur, soweit dies für einen konkreten Support- oder Sicherheitsfall erforderlich ist.

3. Übertragung und Speicherung

- Die Datenübertragung zwischen App/Web und Backend erfolgt über verschlüsselte Transportverbindungen.
- Das produktive Backend und die relationale Datenbank werden in Deutschland betrieben.
- Produktive Mediendateien werden in Frankfurt verarbeitet.
- Für besonders sensible Informationen werden zusätzliche Schutzmaßnahmen eingesetzt.

4. Authentifizierung und Push

- Die Nutzeranmeldung erfolgt über einen spezialisierten Authentifizierungsdienst.
- Push-Benachrichtigungen enthalten keine Kindernamen, Chat- oder Nachrichtentexte, Gesundheitsdetails oder E-Mail-Adressen.
- An Push-Dienste werden generische Hinweise sowie notwendige Routinginformationen und Ereigniskategorien übermittelt.

5. Datenminimierung und Schutz der Privatsphäre

- Es werden nur Daten verarbeitet, die für Konto, Berechtigung und die tatsächlich genutzten Funktionen erforderlich sind.
- Kinder- und Familiendaten werden nicht verkauft und nicht für individuelle Werbeprojekte genutzt.
- Es findet keine kontinuierliche GPS-Ortung von Kindern oder Nutzern statt.
- Bei vorgesehenen Bild-Upload-Prozessen werden Kamera- und GPS-Metadaten aus den Bilddateien entfernt.

6. Entwicklung und Änderungen

- Änderungen durchlaufen Codeprüfung, automatisierte Tests und technische Qualitätskontrollen.
- Sicherheitsrelevante Abhängigkeiten und Konfigurationen werden im Entwicklungs- und Freigabeprozess berücksichtigt.
- Schutzmaßnahmen werden bei wesentlichen technischen oder organisatorischen Änderungen weiterentwickelt.

7. Löschung und Datenlebenszyklus

- Technische Löschprozesse und automatisierte Löschläufe unterstützen die Entfernung von Daten nach Zweckfortfall oder Standardfrist.
- Standardfristen sind im separaten Aufbewahrungs- und Löschkonzept dokumentiert.
- Bei Beendigung der Nutzung werden Daten nach Weisung und unter Beachtung gesetzlicher Pflichten entfernt oder zurückgegeben.

8. Verfügbarkeit und Wiederherstellung

- Für Wiederherstellung und Betriebsfortführung bestehen technische und organisatorische Verfahren.
- Die Wiederherstellbarkeit wurde praktisch erprobt; Sicherungs- und Wiederherstellungsverfahren werden dem Betriebsumfang entsprechend fortgeführt und weiterentwickelt.

9. Sicherheitsvorfälle

- Es besteht ein Prozess zur Erkennung, Bewertung, Eindämmung, Dokumentation und Nachbereitung von Sicherheitsvorfällen.
- Betroffene Auftraggeber werden bei einem relevanten Vorfall unverzüglich mit den verfügbaren Informationen unterstützt.

10. Dienstleister

- Die für den Produktbetrieb eingesetzten technischen Kernanbieter und ihre Zwecke werden in einer separaten, öffentlich zugänglichen Dienstleisterübersicht transparent dargestellt.