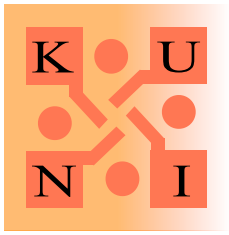

Löschkonzept gemäß DSGVO

Organisation: KUNI
Version: 1.0
Stand: November 2025

1. Einleitung

Dieses Löschkonzept beschreibt die Verfahren und Grundsätze zum sicheren und DSGVO-konformen Löschen personenbezogener Daten in der KUNI-App. Die App wird von unterschiedlichen Nutzergruppen mit verschiedenen Zugriffsrechten verwendet: Personalwesen, Eltern, Erzieher, Kitaleitungen sowie Mitarbeitende des Trägers. Dabei werden sensible und vielfältige personenbezogene Daten verarbeitet, die besonderen Schutz erfordern. Ziel dieses Konzepts ist es, die Aufbewahrung, Löschung und Dokumentation der Daten systematisch, transparent und rechtssicher zu gestalten, um den Schutz der Betroffenen und die Einhaltung gesetzlicher Vorgaben zu gewährleisten.

2. Authentifizierungsrelevante Daten

2.1 Temporäre Authentifizierungsdaten

Datenobjekt	Speicherort	Verarbeitungszweck	Löschfrist	Löschmethode	Rechtsgrundlage
JWT-Token (inkl. Username, Rollen, Scopes, Displaynamen und Claims)	Cookie im Browser	Authentifizierung, Sitzungserhaltung	Endet mit Ablauf des Tokens, manuelles Löschen des Cookies oder nach Abmeldung	Automatisches Entfernen beim Ablauf oder beim Ausloggen; manuelles Löschen möglich	Art. 6 Abs. 1 lit. b DSGVO (Vertragserfüllung)
Passwort	Browser RAM	Authentifizierung, Ableitung privater Schlüssel	Sofort nach Authentifizierung	Automatisches Entfernen nach erfolgreicher oder fehlgeschlagener Authentifizierung	Art. 6 Abs. 1 lit. b DSGVO (Vertragserfüllung)
Challenge	Backend RAM	Authentifizierung, Schutz vor Replay-Angriffen	Sofort nach Authentifizierung	Automatisches Entfernen nach erfolgreicher oder fehlgeschlagener Authentifizierung	Art. 6 Abs. 1 lit. b DSGVO (Vertragserfüllung)

2.2 Allgemein personenbezogene Daten (persistent)

Datenobjekt	Speicherort	Verarbeitungszweck	Löschfrist	Löschmethode	Rechtsgrundlage
Username	Datenbank	Benutzerverwaltung, Zugriffssteuerung, Authentifizierung	3 Jahre nach Accountlöschung	DELETE mit VACUUM FULL in PostgreSQL	Art. 6 Abs. 1 lit. b DSGVO (Vertragserfüllung)
Salt	Datenbank	Absicherung der Passwortverarbeitung, Schutz vor Rainbow-Table-Angriffen	3 Jahre nach Accountlöschung	DELETE mit VACUUM FULL in PostgreSQL	Art. 6 Abs. 1 lit. b DSGVO (Vertragserfüllung)

Datenobjekt	Speicherort	Verarbeitungszweck	Löschfrist	Löschmethode	Rechtsgrundlage
Verifier (Public Key aus dem Passwort)	Datenbank	Authentifizierung, Zero-Knowledge-Verifikation	3 Jahre nach Accountlöschung	DELETE mit VACUUM FULL in PostgreSQL	Art. 6 Abs. 1 lit. b DSGVO (Vertragserfüllung)
E-Mail	Datenbank	Kommunikation mit dem Nutzer (z. B. Passwort-Reset, Benachrichtigungen)	3 Jahre nach Accountlöschung	DELETE mit VACUUM FULL in PostgreSQL	Art. 6 Abs. 1 lit. b DSGVO (Vertragserfüllung)
LastLogin	Datenbank	Erkennung unautorisierter Zugriffe, Benutzerinformation, Support, Verwaltung inaktiver Konten	3 Jahre nach Accountlöschung oder bei manueller Löschung durch Nutzer	DELETE mit VACUUM FULL in PostgreSQL	Art. 6 Abs. 1 lit. b DSGVO, Art. 6 Abs. 1 lit. f DSGVO (berechtigtes Interesse)

3. Interessenabwägung

Die Verarbeitung bestimmter personenbezogener Daten erfolgt auf Grundlage von Art. 6 Abs. 1 lit. f DSGVO (berechtigtes Interesse). Gemäß den Anforderungen der DSGVO wurde eine Interessenabwägung durchgeführt, um sicherzustellen, dass die Rechte und Freiheiten der betroffenen Personen nicht überwiegen. Die folgende Tabelle dokumentiert die Bewertung im Rahmen dieser Abwägung.

Datenobjekt	Berechtigtes Interesse des Verantwortlichen	Erforderlichkeit der Verarbeitung	Schutzmaßnahmen & Betroffenenrechte	Abwägungsergebnis
LastLogin	Erhöhung der Sicherheit durch Erkennung unautorisierter Zugriffe; Verbesserung der Nutzertransparenz durch Anzeige des letzten Logins; Unterstützung bei Supportanfragen und Fehleranalyse; Grundlage für die Verwaltung inaktiver Konten	Die Speicherung des Zeitstempels ist erforderlich, um die genannten Zwecke zu erfüllen. Eine gleichwertige Alternative zur Erreichung dieser Ziele ohne personenbezogene Daten ist nicht gegeben.	Keine Weitergabe an Dritte; keine automatisierte Entscheidungsfindung oder Profilbildung; transparente Information in der Datenschutzerklärung; Möglichkeit zur Einsicht und Löschung durch den Nutzer	Die Verarbeitung ist unter Berücksichtigung der Schutzmaßnahmen und des geringen Eingriffsgrads zulässig. Die Interessen des Verantwortlichen überwiegen nicht die Rechte der betroffenen Person.