eduBITES GmbH

Löschkonzept
(Data Deletion Concept)

Version 2.0 | 13.05.2026 | Kundendokument

Rahmenwerk	Abdeckung
DSGVO	Artikel 5 Abs. 1 lit. e — Speicherbegrenzung Artikel 17 — Recht auf Löschung („Recht auf Vergessenwerden")
ISO 27001:2022	A.8.10 — Löschung von Informationen A.5.34 — Schutz personenbezogener Daten (PII)
DIN 66398	Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen

1. Zweck

Dieses Löschkonzept legt den Rahmen für die systematische und datenschutzkonforme Löschung personenbezogener Daten bei der eduBITES GmbH fest. Es stellt die Einhaltung des Grundsatzes der Speicherbegrenzung gemäß Artikel 5 Abs. 1 lit. e DSGVO sicher, wonach personenbezogene Daten nur so lange in einer Form gespeichert werden dürfen, die die Identifizierung der betroffenen Personen ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist.

Dieses Dokument definiert:

- Die von der eduBITES GmbH verarbeiteten Datenkategorien und deren geltende Aufbewahrungsfristen.
- Die Auslöser für die Löschung personenbezogener Daten.
- Die Verfahren für die technische Löschung und Anonymisierung.
- Das Sperrkonzept für Daten, die aufgrund gesetzlicher Aufbewahrungspflichten nicht gelöscht werden können.
- Die Verantwortlichkeiten und Dokumentationsanforderungen für Löschaktivitäten.

2. Geltungsbereich

Dieses Konzept gilt für:

- Alle personenbezogenen Daten, die von der eduBITES GmbH verarbeitet werden, unabhängig vom Format (digital oder physisch).
- Alle Informationssysteme, Anwendungen und Speichermedien, die zur Verarbeitung personenbezogener Daten verwendet werden, einschließlich der eduBITES-Plattform, der AWS-Infrastruktur (eu-central-1, Frankfurt), Supabase (PostgreSQL, EU), Google Workspace und aller Unterauftragsverarbeiter.
- Alle Sicherungs- und Archivierungssysteme.
- Alle Mitarbeiter, Auftragnehmer und Dritte, die personenbezogene Daten im Auftrag der eduBITES GmbH verarbeiten.

3. Referenzstandard: DIN 66398

Dieses Löschkonzept basiert auf den Grundsätzen und der Methodik der DIN 66398:2016 — Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten.

Das DIN-66398-Rahmenwerk bietet einen strukturierten Ansatz für:

- Die Identifizierung von Datenkategorien und deren zugehörigen Verarbeitungszwecken.
- Die Ableitung von Löschfristen aus Verarbeitungszwecken und gesetzlichen Aufbewahrungspflichten.
- Die Definition von Löschregeln für jede Datenkategorie.
- Die Festlegung von Löschklassen zur Gruppierung von Daten mit ähnlichen Aufbewahrungsanforderungen.
- Die Durchführung regelmäßiger Löschläufe.

Das Löschkonzept folgt dem Grundsatz der DIN 66398, dass personenbezogene Daten zu löschen sind, wenn der Zweck der Verarbeitung entfallen ist und keine entgegenstehende gesetzliche Aufbewahrungspflicht besteht.

4. Grundsätze der Datenlöschung

4.1 Speicherbegrenzung (Art. 5 Abs. 1 lit. e DSGVO)

Personenbezogene Daten dürfen nur so lange in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist. Sobald der Zweck erfüllt ist oder die Rechtsgrundlage für die Verarbeitung entfallen ist, sind die Daten zu löschen, sofern keine gesetzliche Aufbewahrungspflicht besteht.

4.2 Zweckgebundene Aufbewahrung

Die Aufbewahrungsfristen leiten sich aus dem Verarbeitungszweck ab, wie er im Verzeichnis der Verarbeitungstätigkeiten dokumentiert ist. Gelten mehrere Zwecke für dieselben Daten, bestimmt die längste geltende Aufbewahrungsfrist den Löschzeitpunkt.

4.3 Gesetzliche Aufbewahrungspflichten

Soweit deutsches oder EU-Recht die Aufbewahrung von Daten über die Erfüllung des ursprünglichen Verarbeitungszwecks hinaus vorschreibt, werden die Daten gesperrt (eingeschränkt) statt gelöscht und dürfen nur noch zum Zweck der Erfüllung der gesetzlichen Aufbewahrungspflicht verarbeitet werden (siehe Abschnitt 8).

4.4 Regelmäßige Löschläufe

Die Löschung erfolgt durch regelmäßige, systematische Löschläufe und nicht durch Ad-hoc-Löschungen. Dies gewährleistet Konsistenz, Vollständigkeit und Nachvollziehbarkeit.

4.5 Unumkehrbarkeit

Die Löschung ist so durchzuführen, dass die personenbezogenen Daten mit herkömmlichen technischen Mitteln unwiederbringlich nicht wiederherstellbar sind. Die Methode muss dem Speichermedium und der Sensibilität der Daten angemessen sein.

5. Datenkategorien und Aufbewahrungsfristen

Die folgende Tabelle definiert die von der eduBITES GmbH verarbeiteten Datenkategorien, deren Aufbewahrungsfristen und die jeweilige Rechtsgrundlage.

Nr.	Datenkategorie	Aufbewahrungsfrist	Rechtsgrundlage	Löschfrist
1	Kundenplattformdaten (Benutzerkonten, Lernfortschritt, Nutzungsdaten)	Vertragsdauer + 60 Tage	Art. 6 Abs. 1 lit. b DSGVO Vertragserfüllung	60 Tage nach Vertragsende
2	Mitarbeiter-HR-Daten (Beschäftigungsdaten, Gehaltsabrechnung, Steuer)	Beschäftigungsdauer + gesetzl. Fristen (6 J. § 257 HGB / 10 J. § 147 AO)	Art. 6 Abs. 1 lit. b, c DSGVO § 26 BDSG § 257 HGB / § 147 AO	Ende des Kalenderjahres nach Ablauf der längsten gesetzl. Frist
3	Finanz-/Buchhaltungsdaten (Rechnungen, Belege, Kontoauszüge)	10 Jahre	§ 147 AO § 257 HGB	Ende des Kalenderjahres nach Ablauf der 10-Jahres-Frist

4	Vertragsdokumente (Kunden-/Lieferantenverträge, AVVs)	6 Jahre	§ 257 HGB	Ende des Kalenderjahres nach Ablauf der 6-Jahres-Frist
5	Bewerbungsdaten (abgelehnte Bewerber)	6 Monate	Art. 6 Abs. 1 lit. f DSGVO § 15 Abs. 4 AGG	6 Monate nach Ablehnungsmitteilung
6	Protokolldaten (System-, Zugriffs-, Sicherheitsprotokolle)	12 Monate	Art. 6 Abs. 1 lit. f DSGVO Berechtigtes Interesse (IT-Sicherheit)	12 Monate nach Erstellung
7	ISMS-Dokumentation (Richtlinien, Audits, Risikobewertungen)	4 Jahre	Art. 5 Abs. 2 DSGVO Rechenschaftspflicht ISO 27001	4 Jahre nach Ablösung des Dokuments
8	Marketing-Einwilligungen (Einwilligungsstatus, Zeitstempel)	Bis zum Widerruf + 3 Jahre	Art. 6 Abs. 1 lit. a, Art. 7 DSGVO § 195 BGB	3 Jahre nach Widerruf der Einwilligung
9	Sicherungsdaten (Backups)	30 Tage	Art. 32 DSGVO Sicherheit / Notfall-wiederherstellung	30 Tage nach Erstellung (rollierender Zyklus)

5.1 Hinweise zu Aufbewahrungsfristen

- **Kalenderjahresregel:** Bei gesetzlichen Aufbewahrungsfristen (HGB, AO) beginnt die Frist am Ende des Kalenderjahres, in dem das maßgebliche Ereignis eingetreten ist.
- **Längste Frist gilt:** Gelten mehrere Aufbewahrungsfristen für dieselben Daten, ist die längste Frist maßgeblich.
- **Unterauftragsverarbeiter:** Von Unterauftragsverarbeitern verarbeitete Daten werden gemäß dem Auftragsverarbeitungsvertrag gelöscht. Unterauftragsverarbeiter sind vertraglich verpflichtet, Daten auf Weisung oder bei Beendigung des AVV zu löschen.
- **Weisungsgebundenheit:** Soweit die eduBITES GmbH Daten als Auftragsverarbeiter im Auftrag eines Kunden (Verantwortlicher) verarbeitet, erfolgt die Löschung nach den Weisungen des Kunden gemäß AVV.

6. Löschverfahren

6.1 Technische Löschung

Die technische Löschung macht personenbezogene Daten dauerhaft unzugänglich und unwiederbringlich. Je nach System und Speichermedium werden folgende Methoden eingesetzt:

System / Medium	Löschmethode
eduBITES-Plattform / Supabase (Datenbank)	Logische Löschung (DELETE-Operationen) mit Verifizierung; automatische Bereinigung von Soft-Delete-Datensätzen nach Ablauf der Aufbewahrungsfrist
AWS S3 (Dateispeicher)	Objektlöschung mit Lifecycle-Policies zur automatisierten Bereinigung
Google Workspace (E-Mail, Dokumente)	Löschung aus Benutzerkonto und Papierkorb; Admin-Löschung bei ausgeschiedenen Mitarbeitern
Sicherungssysteme (AWS)	Rollierender Sicherungszyklus mit 30 Tagen Aufbewahrung; abgelaufene Sicherungen werden automatisch überschrieben/gelöscht

Physische Medien (Papierdokumente)	Kreuzschnitt-Aktenvernichtung (DIN 66399, Sicherheitsstufe P-4 oder höher)
Lokale Geräte (Laptops, Mobilgeräte)	Sichere Löschtools; Vollverschlüsselung stellt sicher, dass Daten bei Außerbetriebnahme nicht wiederherstellbar sind
Unterauftragsverarbeiter-Systeme	Löschanweisung gemäß AVV; schriftliche Löschbestätigung des Unterauftragsverarbeiters

6.2 Anonymisierung

Soweit eine vollständige Löschung nicht möglich oder nicht erforderlich ist, kann die Anonymisierung als Alternative eingesetzt werden. Die Anonymisierung muss die Daten so verändern, dass die betroffene Person weder direkt noch indirekt identifizierbar ist.

Anonymisierte Daten sind keine personenbezogenen Daten im Sinne der DSGVO und dürfen zu statistischen oder analytischen Zwecken aufbewahrt werden.

Anonymisierungsmethoden umfassen:

- Aggregation (Zusammenführung einzelner Datensätze zu statistischen Zusammenfassungen).
- Entfernung aller direkten und indirekten Identifikationsmerkmale.
- Randomisierung oder Generalisierung von Datenwerten.

6.3 Löschzyklen

Häufigkeit	Umfang
Täglich	Automatische Bereinigung abgelaufener Sitzungsdaten und temporärer Dateien
Monatlich	Überprüfung und Löschung von Daten, deren Aufbewahrungsfrist in Produktivsystemen abgelaufen ist
Vierteljährlich	Umfassende Überprüfung aller Datenkategorien gegen den Aufbewahrungsplan
Jährlich	Vollständiges Audit der Aufbewahrungsfristen und Lösch-Compliance über alle Systeme

7. Löschauslöser

Folgende Ereignisse lösen die Pflicht zur Löschung personenbezogener Daten aus:

Nr.	Auslöser	Maßnahme	Frist
1	Vertragsbeendigung	Löschung aller Kundenplattformdaten (Benutzerkonten, Lerndaten, Analysen)	Innerhalb von 60 Tagen
2	Zweckerfüllung	Löschung personenbezogener Daten nach Erreichen des Verarbeitungszwecks	Nächster regulärer Löschlauf
3	Widerruf der Einwilligung	Einstellung der Verarbeitung und Löschung, wenn die Einwilligung die einzige Rechtsgrundlage war	Innerhalb von 30 Tagen
4	Betroffenenanfrage (Art. 17)	Löschung gemäß Verfahren für Betroffenenrechte	Innerhalb eines Monats
5	Ende des Arbeitsverhältnisses	Löschung der Mitarbeiter-HR-Daten nach	Gemäß Aufbewahrungsplan (Abschnitt 5)

		Ablauf der gesetzlichen Aufbewahrungsfrist	
6	Ablehnung einer Bewerbung	Löschung der Bewerberdaten	6 Monate nach Mitteilung
7	Ablauf der Aufbewahrungsfrist	Löschung der Daten bei Ablauf der definierten Aufbewahrungsfrist	Nächster regulärer Löschlauf
8	Wegfall der Rechtsgrundlage	Löschung personenbezogener Daten bei Wegfall der Rechtsgrundlage	Nächster regulärer Löschlauf
9	Wechsel des Unterauftragsverarbeiters / AVV-Beendigung	Sicherstellung der Datenlöschung durch den bisherigen Unterauftragsverarbeiter gemäß AVV	Gemäß AVV-Klausel (i.d.R. 30 Tage)

8. Sperrkonzept

8.1 Zweck der Sperrung

Die Sperrung (Einschränkung der Verarbeitung) findet Anwendung, wenn personenbezogene Daten aufgrund gesetzlicher Aufbewahrungspflichten aufbewahrt werden müssen, der ursprüngliche Verarbeitungszweck jedoch erfüllt ist. In diesen Fällen werden die Daten von der allgemeinen Verarbeitung ausgeschlossen und dürfen nur noch zum Zweck der Erfüllung der gesetzlichen Aufbewahrungspflicht verarbeitet werden.

8.2 Anwendungsfälle

Die Sperrung wird in folgenden Situationen angewendet:

- Der Verarbeitungszweck ist erfüllt, aber gesetzliche Aufbewahrungsfristen (HGB, AO) erfordern die weitere Speicherung.
- Eine betroffene Person hat die Einschränkung der Verarbeitung gemäß Art. 18 DSGVO verlangt.
- Die Richtigkeit personenbezogener Daten wird bestritten und die Überprüfung steht aus.
- Die Verarbeitung ist unrechtmäßig, aber die betroffene Person widerspricht der Löschung und verlangt stattdessen die Einschränkung.
- Die Daten werden vom Verantwortlichen nicht mehr benötigt, die betroffene Person benötigt sie jedoch zur Geltendmachung von Rechtsansprüchen.

8.3 Umsetzung der Sperrung

Gesperrte Daten werden:

- Im System eindeutig als „gesperrt" oder „eingeschränkt" gekennzeichnet.
- Soweit technisch möglich aus aktiven Verarbeitungsumgebungen entfernt.
- In einem Bereich mit eingeschränktem Zugriff gespeichert (z. B. separates Datenbankschema, Archivierung).
- Nur autorisierten Personen für den spezifischen Zweck der gesetzlichen Aufbewahrungspflicht zugänglich gemacht.
- Durch dieselben oder verstärkte technische und organisatorische Maßnahmen wie aktive Daten geschützt.

8.4 Entsperrung

Gesperrte Daten dürfen nur mit folgenden Voraussetzungen entsperrt (wieder aktiv verarbeitet) werden:

- Eine dokumentierte und genehmigte rechtliche Begründung liegt vor.
- Die Einwilligung der betroffenen Person (soweit anwendbar) wurde eingeholt.
- Die Genehmigung des Datenschutzbeauftragten wurde erteilt.

8.5 Löschung nach Sperrung

Nach Ablauf der gesetzlichen Aufbewahrungspflicht werden gesperrte Daten unverzüglich im nächsten regulären Löschlauf gelöscht.

9. Verantwortlichkeiten

Rolle	Verantwortlichkeit
Informationssicherheits-management	Gesamtverantwortung für die Umsetzung und Pflege des Löschkonzepts; Sicherstellung der technischen Löschfähigkeiten; Genehmigung der Löschverfahren
Datenschutzbeauftragter (DSB)	Beratung zu Aufbewahrungsfristen und Rechtsgrundlagen; Überprüfung des Löschkonzepts; Bewertung der Anonymisierung; Genehmigung von Sperr- und Entsperrentscheidungen
Datenschutzkoordinator	Koordinierung der Löschläufe; Führung des Löschprotokolls; Überwachung der Aufbewahrungsfristen; Koordinierung mit Unterauftragsverarbeitern
Entwicklungsteam	Implementierung technischer Löschmechanismen (automatisierte Löschung, Lifecycle-Policies, Bereinigungsprozesse); Ausführung von Löschanweisungen
Abteilungsleiter / Prozessverantwortliche	Sicherstellung der Einhaltung der Aufbewahrungsfristen in ihrem Bereich; Meldung von Änderungen an Verarbeitungstätigkeiten
Alle Mitarbeiter	Einhaltung der Aufbewahrungsfristen; keine Aufbewahrung personenbezogener Daten über die definierten Fristen hinaus; Meldung löschpflichtiger Daten

10. Dokumentation der Löschung

10.1 Löschprotokoll

Alle Löschaktivitäten werden in einem Löschprotokoll dokumentiert. Das Protokoll erfasst:

Feld	Beschreibung
Lösch-ID	Eindeutige Kennung (Format: DEL-[JJJJ]-[###])
Löschdatum	Datum der Durchführung der Löschung
Datenkategorie	Kategorie der gelöschten Daten (gemäß Abschnitt 5)
Beschreibung	Kurzbeschreibung der gelöschten Daten
System(e)	System(e), aus dem/denen die Daten gelöscht wurden
Löschmethode	Angewandte Methode (technische Löschung, Anonymisierung, Vernichtung)
Auslöser	Auslöser der Löschung (Vertragsende, Fristablauf, Betroffenenanfrage etc.)
Durchgeführt von	Person oder automatisierter Prozess, der die Löschung durchgeführt hat

Verifiziert von	Person, die die Löschung verifiziert hat
Bestätigung Unterauftrags-verarbeiter	Soweit zutreffend, Löschbestätigung des Unterauftragsverarbeiters

10.2 Aufbewahrung der Löschprotokolle

Löschprotokolle werden 4 Jahre aufbewahrt, um die Einhaltung der Rechenschaftspflicht gemäß Art. 5 Abs. 2 DSGVO nachzuweisen. Die Löschprotokolle selbst enthalten keine personenbezogenen Daten — nur Metadaten über die Löschaktivität.

11. Überprüfungszyklus

Dieses Löschkonzept wird überprüft:

- **Jährlich:** Umfassende Überprüfung aller Datenkategorien, Aufbewahrungsfristen und Löschverfahren.
- **Bei Rechtsänderungen:** Bei Änderungen des anwendbaren Datenschutzrechts, Steuerrechts (AO), Handelsrechts (HGB) oder anderer relevanter Vorschriften, die Aufbewahrungsfristen betreffen.
- **Bei organisatorischen Änderungen:** Bei Einführung neuer Verarbeitungstätigkeiten, Änderung bestehender Tätigkeiten oder Beauftragung neuer Unterauftragsverarbeiter.
- **Nach Vorfällen:** Wenn Datenschutzvorfälle Mängel im Löschkonzept aufdecken.
- **Nach Audits:** Wenn interne oder externe Audits Verbesserungsbedarf aufzeigen.