

B E T R I E B

Datenschutz und Löschfristen

Löschfristen, der Löschlauf, das Protokoll und die Stellen, an denen ein Personenbezug entstehen kann

ALPHA · Fassung 0.9.0

Handbuch-Fassung 1.0 · Stand 29.08.2026

Grams IT · Produktreihe Ordavis · .NET 10 · PostgreSQL · Exchange

ID-54 Datenschutz

Datenschutz und Löschfristen

Achtung: Alpha-Fassung. Ordervis Belegung steht in der Fassung 0.9.0 und ist eine Alpha-Fassung. Die Anwendung wird laufend weitergebaut: Masken, Menüwege, Bezeichnungen, Konfigurationsschlüssel und Abläufe können sich jederzeit und ohne Vorankündigung ändern — und mit ihnen die Angaben in diesem Handbuch. Dieses Kapitel beschreibt den Stand vom 29.08.2026. Weicht die Anwendung von einer Beschreibung ab, gilt die Anwendung und nicht dieses Blatt; melden Sie die Abweichung. Für den Echtbetrieb ist diese Fassung **nicht freigegeben**.

Für den Datenschutzbeauftragten und die Systemadministration.

Verantwortlich ist die betreibende Kommune, nicht der Hersteller. Dieses Dokument beschreibt, was das System tut und was einzustellen ist — es ersetzt weder das Verarbeitungsverzeichnis nach Art. 30 DSGVO noch die Abstimmung mit Ihrem DSB.

INHALT

- 1 · Die beiden Löschfristen
- 2 · Was der Löschlauf tut
 - Wann die Frist zu laufen beginnt
 - Was nie anonym wird
 - Anonymisiert, nicht gelöscht
- 3 · Das Löschprotokoll
- 4 · Welche Daten wo liegen
- 5 · Die Stellen, an denen ein Personenbezug entstehen kann
- 6 · Was das System zum Schutz tut
- 7 · Betroffenenrechte
- 8 · Was noch aussteht
- 9 · Die Pflichtseiten
- Verwandte Themen

1 · Die beiden Löschfristen

⚙️ **Am Server:** `Recht:LoeschfristVorgaengeJahre` , `Recht:LoeschfristKontenMonate` · 🔑
Schreibzugriff auf die Konfiguration

Schlüssel	Einheit	Was er steuert
<code>Recht:LoeschfristVorgaengeJahre</code>	Jahre	Aufbewahrung eines abgeschlossenen Vorgangs
<code>Recht:LoeschfristKontenMonate</code>	Monate	Löschung eines ungenutzten Kontos

Achtung: Sie sind leer ausgeliefert, und das ist Absicht. Eine erfundene Frist wäre schlimmer als eine fehlende — sie sähe geprüft aus, und niemand käme darauf, sie zu erfragen.

Solange sie fehlen, sagt die Datenschutzerklärung ausdrücklich „noch nicht festgelegt“ und **nennt die beiden Schlüssel**. Sind **beide** gesetzt, stehen dort die Zahlen.

Achtung: Eine `0` gilt nicht als Frist. „0 Jahre“ hieße „sofort löschen“ und stünde als Zusage auf einer öffentlichen Seite; eine nicht gesetzte Zahl in einer `appsettings.json` ist aber genau das. Die Anwendung behandelt `0` deshalb wie **nicht gesetzt**.

Eine fehlende Frist heißt nicht „sofort löschen“. Ist keine eingetragen, **passiert nichts** — und die Datenschutzerklärung sagt das auch so.

Die Frist ist eine fachliche Entscheidung Ihrer Kommune, nicht des Herstellers. Sie hängt an den Aufbewahrungsvorschriften für die Unterlagen, aus denen die Vorgänge entstehen.

2 · Was der Löschlauf tut

Sind die Fristen gesetzt, läuft **einmal am Tag** ein Durchgang (`Fristen:LoeschTaktStunden` , Vorgabe 24). Er

- **anonymisiert** Vorgänge, deren Frist abgelaufen ist: Name, E-Mail, Telefonnummer, Verein und Anlass werden geleert, die Verbindung zum Konto fällt. **Nummer, Stand, Zeiten und der Verlauf bleiben** — ein Bescheid muss auch Jahre später begründbar sein;
- **schreibt den Exchange-Termin neu**, ohne den Anlass — er ist der einzige Personenbezug im Kalender;
- **löscht** Konten, die zu lange nicht benutzt wurden, mitsamt dem gespeicherten Antragsentwurf und den Anmeldemarken;
- **protokolliert** jeden Lauf in `Loeschprotokoll` .

Wann die Frist zu laufen beginnt

Die Frist zählt ab dem späteren von beidem: dem Ende der Nutzung oder dem letzten Eintrag im Verlauf.

Warum beides zusammen: Eine Genehmigung wird Monate vor der Feier erteilt — ab dem Verlaufseintrag zu zählen wäre zu früh. Ein abgelehnter Antrag hat gar keinen Termin mehr — ab dem Nutzungsende zu zählen ginge nicht.

Was nie anonym wird

Achtung: Unentschiedene Vorgänge werden **nie anonym**. Sie wären danach nicht mehr bearbeitbar, und die Sachbearbeitung stünde vor einem Antrag ohne Absender.

Ein vergessener Antrag **verfällt** (ID-12 §4) — anonym wird er dadurch nicht.

Anonymisiert, nicht gelöscht

Achtung: Das ist eine Entscheidung, die vom Datenschutz mitgetragen sein sollte.

Der Vorgangsverlauf ist absichtlich **unveränderlich**. Die Alternative wäre eine benannte Ausnahme davon gewesen — und die hätte einen Weg geschaffen, auf dem sich Verlaufseinträge **löschen lassen**. Diesen Weg gibt es bewusst nicht.

3 · Das Löschprotokoll

Jeder Lauf schreibt eine Zeile in `loeschprotokoll`: Zahlen, Zeitpunkte und die Fristen, die dabei galten.

Keine Personendaten. Ein Protokoll, das aufführt, wessen Daten entfernt wurden, ist selbst die Aufbewahrung, die es beenden soll.

Achtung: Nach dem ersten Tag nachsehen. Dort muss eine Zeile stehen. Steht keine, läuft der Takt nicht; steht `gelungen = false`, hat er es versucht und ist gescheitert.

Beides sieht in der Anwendung gleich aus: Es passiert nichts. Legen Sie deshalb einen Prüfpunkt in die Überwachung (ID-52 §3).

4 · Welche Daten wo liegen

Ort	Was
PostgreSQL	Vorgänge mit Name, Anschrift, Erreichbarkeit, Anlass; Verlauf; Konten; Spiegel
Exchange-Kalender	Termine — der Anlass ist der einzige Personenbezug
Funktionspostfach	jede Standesänderung mit allen Daten und dem Termin
Dateisystem	Bilder der Einrichtungen, Vorlagen, erzeugte Verträge und Abrechnungen
Öffentlicher Webserver	die Momentaufnahme — nur frei/belegt, ohne Personendaten
Antragswarteschlange	versiegelte Anträge — unlesbar ohne den privaten Schlüssel
Protokoll	Vorgangsnummern und Kennungen, keine Namen

Wichtig: Das Funktionspostfach ist eine eigene Verarbeitung. Dort liegen vollständige Daten in einem Postfach, dessen Aufbewahrung dieses System nicht steuert. Es gehört ins Verarbeitungsverzeichnis, und seine Aufbewahrung gehört mit dem DSB abgestimmt.

5 · Die Stellen, an denen ein Personenbezug entstehen kann

Nicht alles folgt aus dem Datenmodell. Drei Felder tragen Freitext und stehen öffentlich:

Feld	Wo
Pflichten	Steckbrief der Einrichtung
Verbote	Steckbrief der Einrichtung
Grund einer Sperrzeit	Belegungskalender

Achtung: „Schlüssel bei Frau Muster, 0170 ...“ wäre ein Personendatum auf einer öffentlichen Seite — und kein Test findet es. Die Ansprechperson gehört an den Standort (ID-11 §1), wo sie hingehört und wo sie gepflegt wird.

Dazu kommen:

- **Bilder** — ein Foto vom Vereinsfest zeigt Menschen. Nehmen Sie Aufnahmen des leeren Raums.
- **Der Anlass eines Vorgangs** — er steht im Exchange-Termin und ist damit für jeden lesbar, der den Kalender sehen darf. Der Löschlauf schreibt ihn beim Anonymisieren heraus.
- **Recht: Prüfung Barrierefreiheit** — Freitext auf einer öffentlichen Seite. Eine Prüfstellung hineinschreiben, keine Person (ID-14 §5).

6 · Was das System zum Schutz tut

Maßnahme	Wirkung
Kein Personenbezug im Spiegel	Was nach außen geschoben wird, trägt nur Zeiträume und Zustand
Anträge versiegelt	Der private Schlüssel liegt ausschließlich intern (ID-51)
Anmeldemarken als Abdruck	In der Datenbank steht kein funktionierender Anmeldelink, nur SHA-256
Exchange-Kennwort verschlüsselt	AES-GCM; auslesen kann es niemand (ID-42 §5)
Kein Zwischenspeicher für Daten	Die PWA hält nur die Hülle — keine Löschfrist reicht in ein fremdes Gerät (ID-14 §4)
Schriften im Paket	Keine Fremdschrift, keine IP-Adresse an ein CDN
Vorgangskennung statt Nummer	256 Bit für den Link, damit niemand fremde Vorgänge durchprobiert
Konto-Zuordnung über die Kennung	Nicht über die E-Mail-Adresse — sonst zeigte ein Familienpostfach fremde Anträge (ID-13 §5)
Auswertung ohne Personendaten	Was weitergegeben wird, trägt keine (ID-24 §4)

7 · Betroffenenrechte

Recht	Wo im System
Auskunft (Art. 15)	Vorgangsliste, Vorgangsverlauf, Konto
Berichtigung (Art. 16)	Die Akte lässt sich ergänzen; der Verlauf nicht ändern — der richtige Eintrag tritt daneben
Löschung (Art. 17)	Anonymisierung eines abgeschlossenen Vorgangs; Konto löschen
Einschränkung (Art. 18)	organisatorisch
Beschwerde (Art. 77)	Recht:Datenschutzaufsicht — steht auf der Datenschutzseite

Achtung: Ein Löschverlangen zu einem *unentschiedenen* Vorgang ist ein Widerspruch in sich — der Antrag wäre danach nicht mehr zu bescheiden. Klären Sie, ob der Antrag zurückgenommen werden soll; dann wird er storniert und fällt später unter die Frist.

8 · Was noch aussteht

Achtung: Ein liegengelassener Antragsentwurf enthält Name, Adresse und Telefonnummer und verfällt von selbst nicht. Er verschwindet, wenn der Antrag abgeschickt oder verworfen wird — und mit dem Konto, das ihn trägt (also mit **LoeschfristKontenMonate**). Ein eigener Löschlauf für Entwürfe steht noch aus.

9 · Die Pflichtseiten

/datenschutz, **/impressum**, **/barrierefreiheit**, **/kontakt** — gefüllt aus **Recht:*** und **Traeger:*** (ID-40 §§2–3).

Wichtig: Die Rechtstexte gehören vom Rechtsamt bestätigt. Bis dahin tragen sie einen sichtbaren Entwurfshinweis.

Rufen Sie **/datenschutz** nach dem Setzen der Fristen auf. Dort müssen die Zahlen stehen und nicht mehr „noch nicht festgelegt“ (ID-55).

Verwandte Themen

- ID-11 — Die Freitextfelder auf dem Steckbrief
- ID-14 — Barrierefreiheitserklärung, PWA und Zwischenspeicher
- ID-40 — **Recht:*** und **Fristen:***
- ID-52 — Überwachung: der Prüfpunkt auf das Löschprotokoll

- ID-55 — Prüfliste vor der Freischaltung