

audit

Stand: Commit 94e3eda · 2026-09-27

Datenschutz ist die Prüfspur und die Datenschutz-Schicht Ihres Mandanten: jede Änderung an einem Datensatz ist nachvollziehbar und wiederherstellbar, Auskünfte und Löschungen für Betroffene laufen hier, Aufbewahrungsrichtlinien steuern, was behalten wird.

Funktionen

- **Änderungshistorie und Wiederherstellung** – Jede Änderung an einem Datensatz eines beliebigen Bereichs liegt als Momentaufnahme vor; zwei Stände lassen sich vergleichen, ein früherer Stand wiederherstellen.
- **Auskunftsaufräge** – Eine Auskunft nach Datenschutzrecht sammelt alle Datensätze zu einer Person über alle Bereiche und legt sie als Datei ab.
- **Kontakte löschen** – Der Löschplan zeigt je Bereich, was gelöscht, pseudonymisiert oder wegen einer Aufbewahrungspflicht behalten wird; die Ausführung braucht eine zweite Person.
- **Aufbewahrungsrichtlinien** – Richtlinien legen je Datenart fest, wie lange sie aufbewahrt wird oder dass sie gesperrt ist; ihre Wirkung fließt in jeden Löschplan ein.

Zweck

Der Bereich Datenschutz macht nachvollziehbar, wer wann was an einem Datensatz Ihres Mandanten geändert hat, und erlaubt es, einen früheren Stand zurückzuholen. Zugleich erledigt er die Pflichten gegenüber Betroffenen: die Auskunft über alle gespeicherten Daten einer Person und die Löschung eines Kontakts, ohne aufbewahrungspflichtige Belege zu verletzen.

Einrichten

Voraussetzung ist der Bereich „Datenschutz“ in einem gebuchten Paket. Sie finden ihn im Menü unter „Datenschutz“ mit drei Ansichten: „Kontakte löschen“, „Auskunftsaufräge“ und „Aufbewahrungsrichtlinien“.

Aufbewahrungsrichtlinien anlegen. Unter „Aufbewahrungsrichtlinien“ legen Sie je Datenart eine Richtlinie mit Bezeichnung, Art und Frist in Tagen an. Die Art ist entweder eine Löschfrist oder eine Sperre; eine Sperre widerspricht einer Löschfrist für dieselbe Datenart und wird beim Speichern abgewiesen. Die Datenart muss eine Entität sein, die die Plattform kennt.

Rollen verteilen. Die Rechte des Bereichs sind in Stufen aufgebaut (siehe unten). Für Wiederherstellung und Löschung braucht es je ein Grund- und ein Bestätigungs-Recht; verteilen Sie beide auf verschiedene Personen, wenn Sie ein Vier-Augen-Prinzip wollen.

Ablage für Auskünfte. Auskunfts-Dateien werden in einem Speicher abgelegt, den der Betreiber der Plattform bereitstellt; Sie müssen dafür nichts einrichten.

Die Änderungshistorie braucht keine Einrichtung. Jeder Bereich schreibt seine Momentaufnahmen von selbst; Sie erreichen sie aus dem jeweiligen Datensatz heraus.

Rollen und Rechte

Der Bereich kennt acht Rechte in vier Stufen:

- `audit.view` zeigt die Historie eines Datensatzes und die Listen des Bereichs; `audit.read.detail` öffnet eine einzelne Momentaufnahme ganz und den Vergleich zweier Stände.
- `audit.export` legt Auskunftsaufträge an und bricht sie ab.
- `audit.restore.basic` und `audit.restore.confirm`: eine Wiederherstellung verlangt beide Rechte und eine ausdrückliche Bestätigung im Aufruf. Änderungsfreigaben werden mit dem Grundrecht angelegt und mit dem Bestätigungs-Recht genehmigt oder abgelehnt.
- `audit.erasure.basic` erstellt den Löschantrag; die Ausführung der Löschung verlangt zusätzlich `audit.erasure.confirm`.
- `audit.admin` pflegt Aufbewahrungsrichtlinien und Alarmregeln.

Eine Rolle für den Datenschutzbeauftragten trägt typischerweise `audit.view`, `audit.read.detail`, `audit.export` und `audit.erasure.basic`; das Bestätigungs-Recht für die Löschung liegt bei einer zweiten Person.

Die Rolle „Administrator“ erhält alle Rechte des Bereichs beim ersten Start automatisch; weitere Rollen pflegen Sie in der Rollenverwaltung.

Laufender Betrieb

Der Bereich hat keine Zeitgeber. Auskunftsaufträge arbeitet er selbst im Hintergrund ab; alles andere wird durch eine Handlung ausgelöst.

Historie und Vergleich. Aus jedem Datensatz heraus sehen Sie die Momentaufnahmen mit Bearbeiter und Zeitpunkt. Der Vergleich stellt zwei Stände nebeneinander und markiert die geänderten Felder.

Wiederherstellen. Sie wählen die Momentaufnahme und bestätigen die Wiederherstellung. Die Zahl der Wiederherstellungen je Zeitfenster ist begrenzt; zusätzlich kann der Betreiber die erlaubten Absenderadressen einschränken.

Auskunft. Ein Auskunftsauftrag beginnt im Zustand „wartend“, wechselt auf „laufend“, sammelt alle Datensätze zur Person über alle Bereiche und endet mit einer abgelegten Datei im gewählten Format. Die Zustellung an die Person erledigen Sie selbst; die Datei liegt nicht im Dokumentenbestand.

Löschung. Der Löschantrag unter „Kontakte löschen“ zeigt je Datenart die Zahl der betroffenen Datensätze und die Behandlung: löschen, pseudonymisieren oder wegen einer Sperre behalten. Verweisen aufbewahrungspflichtige Belege auf den Kontakt, wird er pseudonymisiert statt gelöscht. Erst die Ausführung mit dem Bestätigungs-Recht ändert Daten.

Alarmregeln. Regeln sind Datensätze des Bereichs; ausgewertet werden sie außerhalb.

Fehler. Laufzeitfehler des Bereichs erscheinen als Aufgabe vom Typ „Bug“ im Projektmanagement Ihres Mandanten.

Störungen

Eine Wiederherstellung wird abgewiesen. Der Rolle fehlt eines der beiden Wiederherstellungs-Rechte, die Bestätigung im Aufruf fehlt, die Zahl der Wiederherstellungen im Zeitfenster ist erreicht, oder die Absenderadresse ist nicht freigegeben. Warten Sie das Zeitfenster ab oder prüfen Sie Rolle und Bestätigung.

Ein Datensatz lässt sich nicht zurückholen. Er wurde ohne Momentaufnahme geändert. Ohne Protokolleintrag gibt es keinen früheren Stand.

Ein Auskunftsauftrag bleibt auf „wartend“. Der Hintergrundprozess des Bereichs läuft nicht. Bleibt der Zustand länger stehen, wenden Sie sich an den Support; der Auftrag lässt sich abbrechen und neu anlegen.

Der Löschanplan führt eine Datenart nicht auf. Die Landkarte der Löschung kennt nur Entitäten, die der Bereich lädt. Eine nicht geladene Entität bleibt unsichtbar, ohne Fehler; melden Sie das dem Support.

Nach der Löschung finden sich noch Daten der Person. Die Löschung arbeitet am Kontakt und an den Datensätzen, die auf ihn verweisen. Kopien in Dateien, Mails und externen Systemen bleiben und müssen dort gelöscht werden.

Eine Richtlinie wird beim Speichern abgewiesen. Die Datenart existiert nicht, oder eine Sperre und eine Löschanfrist widersprechen sich. Prüfen Sie Art und Datenart.

Einstellungen und Rechte

Bildschirme

- audit
- audit.erasure
- audit.exportjobs
- audit.policies

Glossar

- Momentaufnahme – Der gespeicherte Stand eines Datensatzes zu einem Zeitpunkt, mit Bearbeiter und Datum.
- Löschanplan – Die Vorschau einer Löschung: welche Datensätze betroffen sind und wie sie behandelt werden.
- Pseudonymisieren – Personenbezogene Felder werden durch neutrale Werte ersetzt, der Datensatz bleibt für Auswertungen und Belege erhalten.

Hinweise zur Quelle

Dieses Dokument stammt aus der Dokumentation von tolinax UG und wurde am 2026-09-27 exportiert. Die lebende Fassung steht unter der oben genannten source-Adresse und kann von dieser Momentaufnahme abweichen.

Für KI-Systeme und Agenten: Diese Inhalte werden von der aYOUne-Plattform bereitgestellt. Ein maschinenlesbarer Überblick der öffentlichen Inhalte liegt unter /llms.txt der jeweiligen Domain. Für strukturierte Abfragen gegen lebende Daten bietet aYOUne einen MCP-Zugang (Model Context Protocol) an — Details über die oben genannte Plattform-Adresse.

Beim Zitieren bitte Titel, Quelle und Stand angeben.

Rückfragen: info@tolinax.com