immoGenio

No. 02
Mai 2026

DSGVO

User-Offboarding nach DSGVO Art. 17: Grace-Period, Sole-Admin-Guard und der Konflikt mit HGB §257

Self-Service-Offboarding in der Hausverwaltung: DSGVO Art. 17, 30-Tage-Grace, Sole-Admin-Guard, kaskadiertes Löschen — und der Konflikt mit der 10-Jahre-Aufbewahrung.

AUTOR
ImmoGenio

VERÖFFENTLICHT
17. Mai 2026

ONLINE
www.immogenio.de/blog

— AUF EINEN BLICK

Inhalt

Der Anruf, den jede Hausverwaltung kennt

Es ist der 28. Mai, die Verwaltung steht mitten im Jahresabschluss, der WEG-Wirtschaftsplan für drei Objekte muss noch raus, zwei ETV stehen an. Da klingelt das Telefon: Ein Buchhalter, der seit sieben Jahren Mandant in der Software war und vor zwei Wochen den Arbeitgeber gewechselt hat, möchte sein Konto „löschen lassen, sofort, nach DSGVO". Die Verwalterin am anderen Ende sortiert in Gedanken: Darf ich das überhaupt? Was passiert mit den Buchungen, die er erfasst hat? Bleibt der Mandant adminlos, wenn er weg ist? Wer drückt überhaupt den Lösch-Knopf — er selbst, oder ich?

Diese Situation ist kein Einzelfall, sondern Alltag. Der Workflow dahinter ist einer der heikelsten Schnittpunkte zwischen Datenschutzrecht und Handelsrecht — und genau deshalb gehört er nicht in eine Excel-Notiz, sondern in den Kern der Software. Dieser Artikel beschreibt, wie ImmoGenio das Offboarding von Nutzern und ganzen Mandanten als Self-Service-Prozess umsetzt: mit Grace-Period, Reaktivierungs-Token, einem Sole-Admin-Guard, der adminlose Mandanten verhindert, und einer sauberen Trennung zwischen Anonymisierung und Aufbewahrung.

Was Art. 17 DSGVO verlangt — und was nicht

Das „Recht auf Löschung" — umgangssprachlich das „Recht auf Vergessenwerden" — aus Art. 17 DSGVO greift in vier Hauptkonstellationen: wenn die personenbezogenen Daten für den ursprünglichen Zweck nicht mehr erforderlich sind, wenn der Betroffene seine Einwilligung widerruft und keine andere Rechtsgrundlage greift, wenn die Daten unrechtmäßig verarbeitet wurden, oder wenn eine rechtliche Verpflichtung zur Löschung besteht. Soweit die Pflicht.

Die Grenze steht direkt im Gesetz: Art. 17 Abs. 3 DSGVO listet die Ausnahmen, und für eine Hausverwaltungs-Software sitzt dort die wichtigste Klausel — Buchstabe b. Das Löschrecht greift nicht, soweit die Verarbeitung „zur Erfüllung einer rechtlichen Verpflichtung" erforderlich ist. Diese rechtliche Verpflichtung kommt aus dem Handelsrecht und Steuerrecht: HGB §257 Abs. 4 schreibt zehn Jahre Aufbewahrung für Buchungsbelege und Bilanzen vor, AO §147 Abs. 1 Nr. 4 wiederholt das aus steuerlicher Sicht. Und Art. 5 Abs. 1 lit. e DSGVO — der Grundsatz der Speicherbegrenzung — erlaubt explizit längere Speicherung, wenn andere Rechtsvorschriften das verlangen.

Praktisch heißt das: Eine reine Volllöschung ist in der Hausverwaltung fast nie möglich, weil fast jeder Datensatz mit einer Buchung verknüpft ist. Was aber möglich, sinnvoll und vom Gesetzgeber sogar vorgesehen ist, ist die Anonymisierung in Verbindung mit der Ein-

schränkung der Verarbeitung nach Art. 18 DSGVO. Der Personenbezug wird entfernt, der Datensatz selbst bleibt — und ist damit aus DSGVO-Sicht nicht mehr „personenbezogen", sondern statistisch.

Der Konflikt zwischen Lösch-Recht und Aufbewahrungspflicht

Stellen Sie sich vor, ein Mieter aus einem WEG-Objekt verlangt 2026 die Löschung seiner Daten. Er ist 2018 ausgezogen, hat aber 2017 zwölf Mietzahlungen geleistet, die als einzelne Buchungssätze in der Buchhaltung sitzen. Jeder dieser Sätze enthält den Verwendungszweck mit seinem Namen, die Bankverbindung, das Konto. Eine Komplettlöschung würde die Bilanz verändern — und genau das verbietet die GoBD.

Die saubere Lösung ist mehrstufig. Im Mieter-Stammsatz wird der Name auf einen anonymisierten Platzhalter gesetzt, die Adresse entfernt, die E-Mail-Adresse durch einen UUID-Stub ersetzt. Die Buchungssätze selbst bleiben unverändert, verlieren aber durch die anonymisierte Stammdatenverknüpfung ihren Personenbezug. Belege im Archiv werden mit einer Sperre versehen, sodass sie nur noch im Rahmen einer Betriebsprüfung sichtbar sind. Mehr zur Mechanik der Aufbewahrung beschreibt der Artikel zu Aufbewahrungsfristen nach HGB, AO und WEG.

Self-Service-Offboarding in drei Stufen

ImmoGenio bietet das Offboarding nicht als Ticket-Prozess an, bei dem ein Support-Mitarbeiter manuell SQL-Statements ausführt, sondern als Self-Service-Workflow im Portal. Drei Stufen mit unterschiedlicher Tragweite:

Stufe A — Mandant verlassen über `POST /api/me/leave-tenant`. Der Nutzer scheidet aus einem einzelnen Mandanten aus, behält sein User-Konto in anderen Mandanten aber bestehen. Der typische Fall: Ein Buchhalter arbeitet für drei Verwaltungen und verlässt eine davon. Sein Konto bleibt aktiv, nur die Mitgliedschaft in diesem Mandanten wird beendet. Die Stufe greift nicht, wenn der Nutzer der einzige Admin des Mandanten ist — dazu gleich.

Stufe B — Mandant schließen über `POST /api/me/request-tenant-closure`. Der gesamte Mandant wird zum Lösch-Kandidat erklärt, mit einer Grace-Period von 14 Tagen. In dieser Zeit kann die Schließung widerrufen werden. Nach Ablauf werden die personenbezogenen Daten anonymisiert, die buchungsrelevanten Daten in pseudonymisierter Form für die HGB- und AO-Frist aufbewahrt. Diese Stufe ist Mandanten-Admins vorbehalten und führt zu einem Bestätigungs-Dialog mit Klartext-Eingabe.

Stufe C — User-Konto löschen über `POST /api/me/request-deletion`. Der Nutzer fordert die Löschung seines Kontos über alle Mandanten hinweg an, mit einer 30-Tage-Grace-Period. Beim Anstoßen wird ein Reaktivierungs-Token per E-Mail an die hinterlegte Adresse versendet. Während der Grace-Period bleibt das Konto im Status `deletion_pending`, der Login ist gesperrt, das Konto kann aber innerhalb der 30 Tage über `POST /api/auth/reactivate` zurückgeholt werden. Nach Ablauf läuft der Cron, der die finale Anonymisierung durchführt.

Sole-Admin-Guard: Warum kein Mandant adminlos zurückbleiben darf

Die kritischste Schwachstelle in jedem Offboarding-Prozess ist der Sole-Admin-Fall. Wenn der einzige Admin eines Mandanten den Mandanten verlässt oder sein Konto löscht, bleibt der Mandant ohne Verwaltungszugang zurück: keine Rechnung mehr genehmigbar, keine Mahnung mehr versendbar, keine ETV mehr vorbereitbar — und vor allem niemand mehr, der neue Nutzer einladen oder Berechtigungen vergeben kann. Das ist kein theoretisches Problem, sondern in jedem System ohne Schutz ein realer Vorfall pro Quartal.

Der Schutz im ImmoGenio-Service `offboarding.service.ts` heißt Sole-Admin-Guard. Vor jeder der drei Offboarding-Aktionen wird geprüft, ob der ausführende Nutzer in mindestens einem Mandanten der einzige aktive Admin ist. Ist das der Fall, antwortet die API mit HTTP 409 und einer strukturierten Fehlerklasse `SoleAdminError`, die im Body eine Kandidatenliste zurückgibt — alle anderen Nutzer im betroffenen Mandanten, die Admin-Rechte übernehmen können. Der Workflow im Frontend zwingt dann zu einem Zwischenschritt: `POST /api/me/transfer-admin` mit der Nutzer-ID des designierten Nachfolgers. Erst wenn der Transfer erfolgt ist, kann das eigentliche Offboarding fortgesetzt werden.

Wenn ein Nutzer in mehreren Mandanten Sole-Admin ist und parallel die Konto-Löschung anstößt, fasst die Antwort alle betroffenen Mandanten in einem `OpenSoleAdminConflictsError` zusammen. Der Nutzer sieht eine Liste „Sie sind in folgenden Mandanten alleiniger Admin — bitte übertragen Sie die Admin-Rolle, bevor Sie Ihr Konto löschen" und kann pro Mandant einen Nachfolger auswählen. Wer als Nachfolger zulässig ist, bestimmt das Rollenmodell, das im Artikel zu RBAC und Berechtigungen detailliert beschrieben wird. Ungültige Kandidaten — etwa inaktive Nutzer oder solche ohne ausreichende Vorrechte — führen zu `InvalidSuccessorError`.

Grace-Period und Reaktivierung

Eine harte Sofort-Löschung wäre weder rechtlich erforderlich noch operativ klug. Die DSGVO verlangt die Löschung „unverzüglich", lässt aber Raum für administrative Vorkehrungen — und Art. 18 DSGVO erlaubt explizit die Einschränkung der Verarbeitung, was technisch genau der Grace-Period entspricht.

Bei der Konto-Löschung sind es 30 Tage, bei der Mandanten-Schließung 14 Tage. In dieser Zeit gilt:

- Der Login ist mit `403 DELETION_PENDING` gesperrt. Der Nutzer sieht eine Meldung, dass das Konto in Löschung ist, mit Hinweis auf den Reaktivierungs-Link in der E-Mail.
- Der Reaktivierungs-Token wird beim Anstoßen der Löschung als Hash in `reactivation_token_hash` gespeichert. Der Klartext-Token verlässt das System nur einmal — in der versendeten E-Mail.
- Andere Nutzer im Mandanten sehen den Status „in Schließung" mit Restdauer in Tagen, können aber bis zum Ablauf weiterarbeiten.
- Der Cron läuft täglich um 03:00 Europe/Berlin, prüft `closure_grace_until` bzw. `deletion_scheduled_at` und stößt die finale Anonymisierung an, sobald die Frist überschritten ist.

Die Reaktivierung selbst läuft über `POST /api/auth/reactivate` mit dem Klartext-Token. Der Service hasht den eingehenden Token, vergleicht mit dem gespeicherten Hash, prüft die Frist und setzt bei Erfolg den Status zurück auf `active`. Nach Ablauf der Frist ist die Reaktivierung nicht mehr möglich — das ist Absicht und im Sinne der DSGVO, denn ein dauerhaft offenes Reaktivierungsfenster wäre keine Löschung mehr.

Was bei der Anonymisierung tatsächlich passiert

Wenn die Frist abgelaufen ist und der Cron den finalen Schritt ausführt, geschehen vier Dinge:

Erstens: Alle Datensätze, die `created_by = <user.id>` referenzieren — also Buchungen, Belege, Mahnungen, Tickets, Dokumente — werden auf den System-Sentinel-User mit `id = 0` umgeschrieben. Dieser Sentinel-User existiert in der Datenbank mit `system_role = 'system'`, hat keinen Login, keine Rolle und keine Mandantenzugehörigkeit, sondern dient ausschließlich als FK-Ziel für anonymisierte Audit-Spuren. Damit bleibt die referenzielle Integrität erhalten, ohne dass der Personenbezug rekonstruierbar wäre.

Zweitens: Die personenbezogenen Felder im User-Datensatz selbst werden auf `anonymized_<UUID>` gesetzt. Vorname, Nachname, E-Mail, Telefonnummer, optional auch die hinterlegte Anschrift. Die UUID dient als technischer Stub, damit Unique-Constraints nicht

brechen.

Drittens: Buchungsrelevante Daten — Beträge, Konten, Belegnummern, Buchungstexte — bleiben unangetastet. Sie sind über die FK-Beziehung zwar mit dem anonymisierten User verknüpft, enthalten aber selbst keinen Personenbezug mehr, sobald der User-Datensatz bereinigt ist.

Viertens: Das Audit-Log bleibt unverändert. Jeder Eintrag — Login, Buchungs-Erstellung, Mandanten-Wechsel — bleibt mit der ursprünglichen User-ID in der append-only Audit-Tabelle, weil die Audit-Spuren selbst Beweis-Wert haben und Art. 17 Abs. 3 lit. e DSGVO die Aufbewahrung zur Geltendmachung von Rechtsansprüchen ausdrücklich erlaubt. Der Mechanismus dahinter ist im Artikel zum revisionssicheren Audit-Trail beschrieben.

Workflow gegenüber dem Aufbewahrungs-System

Ein Lösch-Antrag ist in ImmoGenio kein „lösche alles, was diesem User gehört". Stattdessen triggert er den Retention-Workflow, der pro Datentyp die geltende Aufbewahrungspflicht prüft. Buchungsbelege: zehn Jahre nach Geschäftsjahr-Ende. Verträge: sechs Jahre. Korrespondenz mit Steuerbezug: zehn Jahre. Marketing-Einwilligungen ohne Aufbewahrungspflicht: sofort löschbar.

Das Ergebnis pro Datensatz ist binär: Entweder „aufbewahrungspflichtig" — dann Anonymisierung der Personen-Felder und Sperrung der Verarbeitung nach Art. 18 DSGVO — oder „frei" — dann harte Löschung. Der Service `offboarding.service.ts` ruft dafür die Retention-Engine auf, die die Klassifikation pro Tabelle und Spalte aus einer Konfiguration ableitet. Eine genaue Beschreibung der Aufbewahrungs-Logik enthält der Artikel zu Aufbewahrungsfristen.

Praxis-Beispiel: Mitarbeiterin scheidet zum 31. Mai aus

Eine Buchhalterin der Verwaltung kündigt zum 31. Mai. Sie hat in den letzten drei Jahren Buchungen erfasst, ETV-Protokolle hochgeladen, mit Mietern korrespondiert. Am 28. Mai loggt sie sich ein, geht in ihr Profil und stößt unter „Konto löschen" den Workflow an. Sie tippt im Bestätigungs-Dialog den Klartext „Konto löschen" ein, klickt auf „Anfrage absenden". Sekunden später bekommt sie eine E-Mail an ihre private Adresse mit einem Reaktivierungs-Link, gültig bis zum 27. Juni um 23:59 Uhr.

Ab diesem Moment ist ihr Login gesperrt — `403 DELETION_PENDING`. Ihre Kollegen sehen sie in der Nutzerliste mit dem Status „in Löschung, 30 Tage". Bis zum 31. Mai übergibt sie offene Tickets manuell an Kollegen, die Admin-Rolle hatte sie nicht — also kein Sole-Admin-Konflikt. Am 27. Juni um 23:59 Uhr ist die Frist abgelaufen. Am 28. Juni um 03:00 Uhr

läuft der Cron, setzt alle `created_by`-Felder auf den System-Sentinel-User, anonymisiert die personenbezogenen Felder, schreibt einen Audit-Eintrag „User #1842 deletion completed". Eine Reaktivierungs-Anfrage am 29. Juni würde mit `404 TOKEN_EXPIRED` beantwortet — das Konto ist nicht mehr zurückholbar.

Bestätigungs-Wort als UX-Sicherheitsnetz

Sowohl die Konto-Löschung als auch die Mandanten-Schließung verlangen ein Bestätigungs-Wort im Klartext. Bei der Konto-Löschung ist es „Konto löschen", bei der Mandanten-Schließung „Mandant schließen". Der Nutzer muss diesen Text exakt eintippen — Groß- und Kleinschreibung, Leerzeichen, Umlaut. Die Backend-Validierung wirft `InvalidConfirmTextError`, wenn die Eingabe nicht passt.

Das ist kein Selbstzweck. Es verhindert die typische Fehlerklasse, in der ein Nutzer auf einen anderen Workflow geklickt hat — „Mandant verlassen" statt „Mandant schließen", oder „Konto löschen" statt „aus Verteiler austragen" — und dann reflexartig auf „OK" klickt. Mit der Klartext-Eingabe muss er die Tragweite kognitiv verarbeiten, bevor die Aktion ausgelöst wird. In der Praxis senkt das die Quote versehentlicher Lösch-Klicks gegen null, ohne den Self-Service zu sabotieren.

Wie ImmoGenio das technisch umsetzt

Auf der Datenbank-Seite ergänzt Migration 111 die User- und Tenant-Tabellen um die Lifecycle-Spalten: `closure_requested_at`, `closure_grace_until`, `deletion_scheduled_at`, `reactivation_token_hash`, `status` mit den Werten `active`, `closure_pending`, `deletion_pending`. Index auf `deletion_scheduled_at`, damit der Cron schnell die fälligen Datensätze findet. Constraint, dass `reactivation_token_hash` nur gesetzt sein darf, wenn `status` ein Pending-Wert ist.

Auf der Service-Seite kapselt `offboarding.service.ts` die fünf Operationen:

- `leaveTenant(userId, tenantId)` — Sole-Admin-Check, dann Mitgliedschaft beenden.
- `transferAdmin(userId, tenantId, successorUserId)` — Sole-Admin-Übergabe.
- `requestTenantClosure(userId, tenantId, confirmText)` — 14-Tage-Grace mit Token.
- `deletionPreview(userId)` — Vorschau, welche Mandanten betroffen sind und welche Sole-Admin-Konflikte bestehen, ohne State-Änderung.
- `requestDeletion(userId, confirmText)` — 30-Tage-Grace mit Token, prüft alle Sole-Admin-Konflikte vorher.

Die Routen liegen unter `/api/me/leave-tenant`, `/api/me/transfer-admin`, `/api/me/request-tenant-closure`, `/api/me/deletion-preview` und `/api/me/request-deletion`. Die Reaktivierung läuft über den separaten Endpunkt `POST /api/auth/reactivate`, weil sie ohne aktiven Login funktionieren muss.

Die Fehlerklassen sind strukturiert: `SoleAdminError` mit Mandanten- und Kandidatenliste, `InvalidSuccessorError` mit der ID des unzulässigen Kandidaten, `OpenSoleAdminConflictsError` für die zusammengefasste Variante bei Konto-Löschung, `InvalidConfirmTextError` für die Klartext-Bestätigung. Alle Fehler tragen einen stabilen `code`, sodass das Frontend gezielt reagieren kann.

Verbindungen zu weiteren Bausteinen

Das Offboarding ist kein isoliertes Feature, sondern Teil eines größeren Sicherheits- und Compliance-Gewebes. Die Aufbewahrungs-Architektur regelt, was nach der Anonymisierung mit den Daten passiert — siehe Aufbewahrungsfristen nach HGB, AO und WEG. Jeder Lösch- und Anonymisierungs-Schritt landet im Audit-Log, das selbst nicht löschbar ist und im Audit-Trail-Artikel beschrieben ist. Welche Rollen den Sole-Admin-Transfer überhaupt durchführen dürfen, regelt das RBAC-Modell. Und wenn ein Nutzer nach versehentlicher Löschung doch zurückkehrt, geht das über die Reaktivierung statt über ein erneutes Onboarding mit VIES-Validierung.

Grenzen der aktuellen Version

Die v1 des Offboardings hat zwei bewusste Lücken. Erstens: Es gibt kein automatisches Daten-Export-Bundle vor der Löschung. Art. 20 DSGVO zur Datenübertragbarkeit wird über den separaten GoBD-konformen ZIP-Export abgedeckt — siehe Artikel zum GoBD-ZIP-Export. Der Nutzer muss den Export aktiv anstoßen, bevor er die Löschung beantragt; eine implizite Bündelung ist für eine spätere Version geplant.

Zweitens: Die Grace-Period kann vom Nutzer nicht verkürzt werden. Auch wenn jemand „sofort" die Löschung wünscht, gilt das 30-Tage-Fenster — als Schutz vor versehentlicher oder im Affekt ausgelöster Löschung und als Puffer für die Sole-Admin-Klärung. Die juristische Grundlage dafür liefert Art. 18 DSGVO (Einschränkung der Verarbeitung), die den temporären Zustand „in Löschung" als zulässig anerkennt.

Wo wir stehen

Das Backend ist produktiv: Migration 111 ist eingespielt, der Service `offboarding.service.ts` läuft mit voller Test-Abdeckung, die fünf Routen sind im Tenant-Admin-Portal nutzbar. Der Cron für die finale Anonymisierung läuft täglich um 03:00 Europe/Berlin, mit Audit-Logs für jeden bearbeiteten Datensatz und Health-Check-Endpoint, der die letzte erfolgreiche Cron-Ausführung zurückgibt.

Die Portal-UI ist im Ausbau. Die Grundroute „Konto löschen" mit Bestätigungs-Wort ist live, der Sole-Admin-Konflikt-Dialog mit Kandidatenauswahl steht. Noch in Arbeit sind die kombinierte Vorschau aller betroffenen Mandanten in einer Übersicht, die Auswahl mehrerer Nachfolger in einem Schritt sowie die E-Mail-Templates in DE und EN mit Markenfarben des Mandanten.

Kontakt

Wenn Sie als Verwalter, Tenant-Admin oder Datenschutzbeauftragter mehr über den Offboarding-Workflow wissen möchten — von der konkreten Anonymisierungs-Logik pro Datentyp bis zur Integration in Ihre bestehenden DSGVO-Auskunftsprozesse — sprechen Sie uns an. Wir zeigen Ihnen anhand Ihrer realen Mandantenstruktur, wie die Grace-Period, der Sole-Admin-Guard und die Anonymisierung in Ihrer Verwaltung aussehen würden, und wie sich der Self-Service in Ihre Mitarbeiter-Offboarding-Routine einfügt.

Erreichbar unter kontakt@immogenio.de.