```
module: 21
title: Audit-Log
phase: 1
status: detail-spec-draft
last_updated: 2026-05-08
session_source: brainstorming-session-2026-05-07-2206.md
related_lps: [LP-1, LP-6, LP-9, LP-10, LP-13]
spec_style: requirements-pur
```

Modul 21 — Audit-Log

> ***Detail-Spec gemäß LP-9.*** *Tenant-weiter, manipulationsarmer Trail aller schreibenden Aktionen mit Vorher-/Nachher-Diff. Compliance-Grundlage für DSGVO-Auskunft, interne Nachvollziehbarkeit und Sicherheits-Forensik. Erfasst alle Schreib-Aktionen aller Module (AV #6 — Audit-Trail-Default).*

Themenblöcke

```
A. Datenmodell (AuditEntry, Aufbewahrung)
B. Erfassungs-Vorschrift (was wird geloggt)
C. Menü-Struktur und Routes
D. Listen-View (Audit-Trail)
E. Detail-View (Diff-Anzeige)
F. Filter & Suche
G. Export (Compliance)
H. Aufbewahrung & Auto-Lösch
I. Manipulations-Schutz (Phase 2: Hash-Chain)
J. Permissions-Anwendung
K. Activity-Stream-Integration
L. Klartext-Hinweise
M. Phase 2 / spätere Features
```

Block A — Datenmodell

`AuditEntry`

- `id` (UUID)
- `tenant_id` (NOT NULL, RLS)
- `created_at` (Timestamp, immutable, indexed)
- `actor_user_id` (FK auf User; NULL bei System/Automation/KI)
- `actor_kind` (Enum: `user | system | automation | ki_agent | api_key | platform_admin`)
- `actor_label` (Snapshot des Names bei Erfassung — bleibt auch bei User-Löschung)
- `action` (Enum, siehe Block B — z.B. `contact.created`, `deal.stage_changed`, `permission.granted`)
- `subject_type` (Enum: `contact | company | lead | deal | project | user | role | permission | tag | custom_field | api_key | tenant_setting | ...`)
- `subject_id` (UUID des betroffenen Objekts)
- `subject_label` (Snapshot des Namens für menschen-lesbare Anzeige nach Subject-Hard-Delete)
- `before_diff` (JSONB — Vorher-Snapshot der geänderten Felder)

- `after_diff` (JSONB — Nachher-Snapshot der geänderten Felder)
- `metadata` (JSONB — Action-spezifischer Kontext, z.B. Bulk-Operation-ID, Automation-Run-ID, KI-Prompt-ID)
- `ip_address` (INET — bei API-/User-Aktionen)
- `user_agent` (Text — bei User-Aktionen)
- `request_id` (UUID — für Korrelation mit Logs)
- `summary_text` (Pflicht — Klartext-Zusammenfassung in DE, z.B. *„Max Mustermann hat Deal ‚Heizung Müller' von Stage Angebot auf Auftrag verschoben"*)
- `hash_prev` (TEXT — Phase 2, Hash-Chain)
- `hash_self` (TEXT — Phase 2, Hash-Chain)

Indizes

- `(tenant_id, created_at DESC)` — Default-Sortierung
- `(tenant_id, actor_user_id, created_at DESC)` — Filter nach Person
- `(tenant_id, subject_type, subject_id, created_at DESC)` — Filter nach Modul/Objekt
- `(tenant_id, action, created_at DESC)` — Filter nach Aktion
- GIN-Index auf `metadata` für Korrelations-Queries
- Trigram-Index auf `summary_text` für Volltext-Suche

Append-Only-Constraint

- Tabelle hat KEINE UPDATE-/DELETE-Rechte für App-Role
- Nur INSERT erlaubt; Audit-Cleanup-Job läuft mit Superuser-Role gegen Retention-Regeln (siehe Block H)
- DB-Trigger blockt UPDATE auf bestehende Einträge (Belt-and-Suspenders)

Sub-Entitäten

`AuditExportJob` (für Compliance-Export):
- `id`, `tenant_id`, `requested_by_user_id`, `created_at`
- `filter_criteria` (JSONB — gleicher Filter wie Listen-View)
- `format` (Enum: `csv | json | pdf`)
- `status` (Enum: `pending | running | completed | failed`)
- `result_file_url` (Scaleway-Storage, signed URL mit 7-Tage-Gültigkeit)
- `entry_count`
- `completed_at`

`AuditRetentionPolicy` (Tenant-Setting):
- `tenant_id` (Primary Key)
- `default_retention_months` (Default 24, min. 6, max. 120)
- `legal_hold_active` (Boolean — bei aktivem Legal Hold KEINE Auto-Lösch)
- `legal_hold_reason` (Text)
- `legal_hold_set_by`, `legal_hold_set_at`

Block B — Erfassungs-Vorschrift

> ***AV #6 — Audit-Trail-Default:*** *Jede schreibende Aktion erzeugt einen Audit-Entry. Pflicht-Vorschrift, kein Modul ist davon befreit.*

Pflicht-erfasste Action-Kategorien (Auswahl, nicht abschließend)

Auth & User-Lifecycle (Modul 27):
- `auth.login_success` / `auth.login_failed`

- `auth.logout`
- `auth.password_changed`
- `auth.2fa_enabled` / `auth.2fa_disabled` / `auth.2fa_reset`
- `user.invited` / `user.accepted_invitation`
- `user.deactivated` / `user.removed` / `user.reactivated`
- `user.deleted` (Self-Delete)
- `session.revoked` (manuell oder automatisch)
- `tenant.created` / `tenant.suspended` / `tenant.frozen` / `tenant.deletion_pending` / `tenant.deleted`

Permissions & Rollen (Modul 27):
- `role.created` / `role.updated` / `role.deleted` / `role.duplicated`
- `permission.granted` / `permission.revoked` (mit Diff der atomaren Permissions)
- `user.role_assigned` / `user.role_removed`
- `group.created` / `group.member_added` / `group.member_removed` / `group.deleted`

CRM (Modul 1, 2, 3):
- `contact.created` / `contact.updated` / `contact.archived` / `contact.restored` / `contact.deleted`
- `company.*`, `lead.*`, `deal.*`
- `lead.promoted` (mit Verweis auf entstandenen Contact + Deal)
- `merge.contacts` / `merge.companies` (mit Verlierer + Gewinner + Field-Auswahl)
- `tag.applied` / `tag.removed`
- `custom_field.definition_created` / `*_updated` / `*_archived` / `*_deleted`
- `custom_field.value_set` / `*_changed` / `*_cleared`

Projekte/Pipeline/Tasks (Modul 4, 26):
- `project.created` / `project.stage_changed` / `project.archived` / `project.deleted`
- `task.created` / `task.assigned` / `task.completed` / `task.deleted`

Kommunikation (Modul 9, 10, 12, 13):
- `email.sent` (Outbound, mit Empfänger + Betreff in `metadata`)
- `email_marketing.campaign_sent` (mit Empfänger-Anzahl)
- `call.made` / `call.received` (Metadaten: Dauer, Aufzeichnung-Link)
- `chat.message_deleted` (Soft-Delete; Edit nicht erfasst da häufig)

Files (Modul 23):
- `file.uploaded` / `file.deleted` / `file.shared` / `file.access_revoked`

Automation & KI (Modul 17, 18):
- `automation.created` / `automation.activated` / `automation.deactivated` / `automation.deleted`
- `automation.executed` (Aggregat-Eintrag pro Run, Detail-Ausführungs-Log separat in Modul 17)
- `ki.action_taken` (mit Prompt-Hash + bestätigter User)

Settings & Integrationen (Modul 27, 33a, 19):
- `tenant_setting.changed` (welches Setting, von wem, alt/neu)
- `integration.connected` / `integration.disconnected`
- `api_key.created` / `api_key.revoked`
- `feature_flag.changed` (Plattform-Admin-Aktion, sichtbar in Tenant-Audit nur als Marker)

Audit-Log selbst:
- `audit.exported` (Wer hat wann was exportiert)
- `audit.legal_hold_set` / `audit.legal_hold_released`
- `audit.retention_changed`

Customer-Portal (Modul 15):
- `portal_user.invited` / `portal_user.action` (Kommentar, Datei-Download, Approval)

Code-Erfassungs-Pattern

Architektur-Vorschrift:
- Zentraler `auditService.log({ action, subject, before, after, ... })`-Service
- Aufruf in jedem schreibenden Service-Layer-Pfad (nicht im Controller — Service-Layer ist die Wahrheits-Schicht)
- Bei Bulk-Operationen: ein Audit-Entry pro betroffenem Objekt + ein Aggregat-Entry mit Bulk-Operation-ID (`metadata.bulk_op_id`)
- Bei Transaction-Failure: Audit-Entry rollt mit zurück (gleiche Transaction)

NICHT erfasst (bewusste Ausschlüsse, gemäß LP-13 Datenökonomie)

- Pure Read-Aktionen (Liste laden, Detail anzeigen) — würde Audit fluten
- Real-time-Cursor-Position in Editoren
- Chat-Message-Edits (zu häufig — nur Delete)
- Notification-Read-Status

Ausnahmen mit P2-Ausbaupfad:
- Sensible Read-Aktionen (HR-Daten lesen, DSGVO-Export herunterladen) → P1-Pflicht-Erfassung als Spezial-Action `audit.sensitive_read`
- Customer-Portal-Login als `portal.login`

Block C — Menü-Struktur und Routes

Sidebar-Eintrag: unter *Workspace-Verwaltung* (Tenant-Admin) → *Audit-Log*.

Routen:

```
/{tenant}/admin/audit                          → Audit-Trail Listen-View
/{tenant}/admin/audit/:id                      → Audit-Entry Detail
/{tenant}/admin/audit/exports                  → Export-Jobs Übersicht
/{tenant}/admin/audit/exports/new              → Export-Job anlegen
/{tenant}/admin/audit/exports/:id              → Export-Job-Status + Download
/{tenant}/admin/audit/settings                 → Aufbewahrungs-Settings + Legal Hold
```

Zusätzliche Einbettung:
- Per-Subject-Audit-Drawer in jeder Detail-View (Contact-Detail, Deal-Detail etc.) zeigt gefiltert auf `subject_type + subject_id` (Permission `audit.read` erforderlich)
- Per-User-Audit-Drawer in `/{tenant}/admin/users/:id/` zeigt Aktionen dieses Users (Permission `audit.read`)

Block D — Listen-View (Audit-Trail)

Zu zeigende Daten pro Eintrag

- Datum + Uhrzeit (relativ < 7 Tage, sonst absolut)
- Actor (Avatar + Name + Actor-Kind-Marker für System/Automation/KI/API-Key/Plattform-Admin)
- Action (menschen-lesbares Label aus Action-Enum, lokalisiert über i18n)
- Subject (Typ + Name, klickbar zur Quelle wenn nicht gelöscht)
- Summary-Text als Hauptinhalt
- Optional: IP / User-Agent-Marker bei expandierten Zeilen

Benötigte UI-Elemente

- Listen-Anzeige (Designer-Wahl: Tabelle, Stream, Karten)

- Filter-Komponenten (siehe Block F)
- Such-Funktion (Volltext über `summary_text`)
- Sortierung: Default Datum absteigend (umkehrbar)
- Pagination (Cursor-basiert, „Mehr laden", 100 pro Page — Audit-Daten oft groß)
- Klick auf Zeile → Detail-View
- Quick-Filter-Funktionen (Click auf Actor / Subject / Action filtert die Liste vor)
- Date-Range-Selektor (Default: letzte 30 Tage; max. 24 Monate ohne Export)
- Export-Funktion-Button (führt zu Export-Job-Anlage)

Operationen

- Filter anwenden / kombinieren / als „Gespeicherte Ansicht" speichern (max. 5 pro User)
- Drill-Down via Klick auf Felder
- Detail-Anzeige für einzelnen Entry
- Export starten (siehe Block G)

Performance-Anforderungen

- Server-side-Filter zwingend (Audit-Tabellen werden groß: bei 50 MA Geerkens schätzungsweise 50-200k Entries/Monat)
- Indizes (siehe Block A)
- Default-Query auf 30 Tage begrenzt; ältere Daten nur über explizite Date-Range
- Bei Bulk-Operations: Aggregat-Entry standardmäßig anzeigen, Individual-Entries auf Klick aufklappbar
- Materialized View für Statistik-Aggregate (P2)

Block E — Detail-View (Diff-Anzeige)

Zu zeigende Daten

- Vollständiger Eintrag (alle Felder aus Block A)
- Vorher-/Nachher-Diff als visualisierter Vergleich
- Bei Bezug zu Bulk-Operation: Liste aller Geschwister-Entries derselben Bulk-Op
- Bei Bezug zu Automation-Run: Verlinkung in Automation-Execution-Log (Modul 17)
- Bei Bezug zu KI-Aktion: Verlinkung in KI-Aktion-Log mit Prompt-Hash (Modul 18)

Benötigte UI-Elemente

- Strukturierte Anzeige aller Eintrag-Felder
- Diff-Visualisierung pro geändertem Feld:
- Skalare Werte: Vorher / Nachher direkt nebeneinander
- JSON/Listen-Werte: Strukturierter Diff (Hinzufügungen / Löschungen / Änderungen)
- Sensible Felder (z.B. Passwort-Hash): nur Marker „Wert geändert", kein Vorher/Nachher
- Verlinkungs-Funktionen zu Subject (wenn nicht gelöscht), Actor-Profil, Bulk-Op-Sicht
- Copy-to-Clipboard-Funktion für `request_id` (für Support-Korrelation)

Operationen

- Read-only — keine Editier-Funktion, keine Löschung
- „Ähnliche Einträge anzeigen" (filtert Liste auf gleiche Action + Subject-Type)
- „Verlauf dieses Objekts" (filtert auf gleiche `subject_type + subject_id`)

Klartext-Hinweise

- Bei Subject-Hard-Delete: *„Das betroffene Objekt wurde inzwischen gelöscht. Snapshot des Namens: ‚X'."*
- Bei sensiblen Diff-Inhalten: *„Diff aus Datenschutz-Gründen nicht sichtbar — nur ‚Wert geändert' wird gezeigt."*
- Bei System/Automation-Actor: *„Diese Aktion wurde von der Automation ‚X' ausgeführt — [Automation öffnen]"*

Block F — Filter & Suche

Filter-Optionen

Pflicht-Filter (immer sichtbar):
- Date-Range (Default 30 Tage; explizite Auswahl bis max. Retention-Period)
- Actor (Multi-Select aus User + System + Automation + KI + API-Key)
- Action-Kategorie (gruppiert: Auth, CRM, Projekte, Kommunikation, Settings, ...)

Erweiterte Filter:
- Subject-Type (Multi-Select)
- Subject-ID (Free-Text mit Auto-Complete bei Eingabe)
- IP-Adresse (für Sicherheits-Forensik)
- Actor-Kind (User / System / Automation / KI / API-Key / Plattform-Admin)
- Bulk-Op-ID (für Korrelation)
- Request-ID (für Support-Korrelation)

Volltext-Suche:
- Über `summary_text` mit Trigram-Index
- Server-side, debounced (500ms)

Gespeicherte Ansichten

- User kann Filter-Kombination als „Ansicht" speichern (max. 5 pro User)
- Beispiel-Default-Ansichten geseeded:
- „Login-Aktivität letzte 7 Tage"
- „Permissions-Änderungen letzte 30 Tage"
- „Hard-Deletes letzte 90 Tage"
- „API-Key-Aktionen"

Permissions-Auswirkung im Filter

- User mit `audit.read` (nicht `audit.admin`) sieht alle Einträge des Tenants — kein eigener Owner-Check, da Audit tenant-weit ist
- HR-bezogene Audit-Einträge (Modul 14) zeigen nur Marker ohne Diff-Inhalt für User ohne `hr.read_all`
- Sensible Diff-Inhalte (z.B. Customer-Portal-User-Daten) ohne Detail-Diff für User ohne entsprechende Modul-Permission

---

Block G — Export (Compliance)

Use-Cases

- DSGVO-Auskunft (Behörde fragt: Welche Aktionen wurden mit den Daten von Person X durchgeführt?)
- Interne Compliance-Audits
- Sicherheits-Forensik (Übergabe an Externe für Vorfalls-Analyse)

• Rechtsstreit (Gerichtsanforderung)

Export-Job-Anlage (`/admin/audit/exports/new`)

Zu zeigende Daten:
- Filter-Kriterien (analog Listen-View)
- Format-Auswahl (CSV / JSON / PDF)
- Zweck-Begründung (Pflichtfeld, Freitext, wird in Audit erfasst)

Operationen:
- Filter setzen (gleiche UX wie Listen-View)
- Format wählen
- Vorschau der zu exportierenden Anzahl Einträge (count-only, vor Submit)
- Job submit → asynchrone Verarbeitung
- Notification bei Fertigstellung (Modul 22)

Format-Spezifikationen:
- **CSV:** Flach, Diff als JSON-String pro Zeile
- **JSON:** Strukturiert mit voll-aufgelöstem Diff
- **PDF:** Lesbarer Bericht mit Header (Tenant, Zeitraum, Erstellt von, Filter-Kriterien, Anzahl Einträge), tabellarischer Inhalt, signierter Footer (Phase 2: digitale Signatur via PandaDoc)

Export-Job-Status (`/admin/audit/exports/:id`)

Zu zeigende Daten:
- Job-Status (Pending/Running/Completed/Failed)
- Filter-Kriterien (read-only)
- Erstellt von / am
- Zweck-Begründung
- Anzahl Einträge im Resultat
- Download-Link (signed URL, 7 Tage gültig)
- Bei Fehler: Klartext-Fehlermeldung

Operationen:
- Download (1x kostenlos pro Job; weitere Downloads regenerieren signed URL)
- Job widerrufen / löschen (nur falls kein Download erfolgte)

Export-Tracking

• Jeder Export wird selbst auditiert (`audit.exported` Action)
• Export-Datei selbst auf Scaleway-Storage `tenants/{tenantId}/audit-exports/{jobId}/...`
• Export-Datei wird nach 30 Tagen automatisch gelöscht (Notification 7 Tage vorher)

Klartext-Hinweise

• Vor Submit: *„Du exportierst 4.892 Audit-Einträge. Der Export wird selbst geloggt und sichtbar für andere Tenant-Admins."*
• Bei Job-Failure: *„Export fehlgeschlagen — bitte Filter eingrenzen und erneut versuchen. Bei wiederholtem Fehler: Support kontaktieren."*

Block H — Aufbewahrung & Auto-Lösch

Default-Retention

• 24 Monate ab `created_at`

- Tenant-Admin-konfigurierbar in `/admin/audit/settings` (min. 6, max. 120 Monate)

Auto-Lösch-Job

- Täglicher Cron-Job läuft mit Superuser-Role
- Löscht Einträge älter als Retention-Period — außer:
- `legal_hold_active = true` → Lösch-Pause für gesamten Tenant
- Sensible Action-Kategorien mit Sonder-Retention (Phase 2):
  - `auth.*` und `permission.*` mindestens 36 Monate
  - `tenant.deleted`-Einträge dauerhaft (für Reaktivierungs-Window)

Legal Hold

Setting in `/admin/audit/settings`:
- Toggle „Legal Hold aktivieren"
- Bei Aktivierung: Pflicht-Begründung (Freitext, mindestens 20 Zeichen)
- Bei Aktivierung: Auto-Lösch pausiert für gesamten Tenant
- Permission: nur `tenant.admin` UND `audit.admin`
- Aktivierung wird selbst auditiert (`audit.legal_hold_set`)

Klartext-Hinweis bei aktivem Legal Hold:
- Banner im Audit-Log: *„Legal Hold aktiv seit [Datum] — keine automatische Löschung. Begründung: [Text]. [Bei Bedarf aufheben]"*

Retention-Änderung

- Tenant-Admin kann Retention herauf-/herunter-setzen
- Bei Reduzierung: Klartext-Bestätigung mit Anzahl betroffener Einträge: *„Wenn du Retention auf 12 Monate setzt, werden ca. 47.231 Audit-Einträge älter als 12 Monate beim nächsten Auto-Lösch-Lauf entfernt. [Bestätigen] [Abbrechen]"*
- Änderung wird selbst auditiert (`audit.retention_changed`)

Block I — Manipulations-Schutz (Phase 2: Hash-Chain)

> ***Phase 1:*** *Append-Only-Constraint auf DB-Ebene (siehe Block A). Tenant-Admin und Support sehen Einträge gleich; keine Edit-/Delete-Rechte für irgendwen außer Auto-Cleanup-Job.*
>
> ***Phase 2 — Hash-Chain:***

- Pro Eintrag: `hash_self = SHA256(prev_hash || canonical_serialization(entry))`
- `hash_prev` zeigt auf vorherigen Eintrag desselben Tenants
- Ein „Genesis"-Eintrag pro Tenant zur Initialisierung
- **Verifikations-Tool** in `/admin/audit/settings` → „Integrität prüfen": läuft asynchron über Tenant-Audit-Trail, gibt Anzahl Einträge + Hash-Validität zurück
- Bei Manipulation entdeckt: Klartext-Alert + Audit-Eintrag mit Lücke-Marker
- Optional: tägliche Veröffentlichung des aktuellen Tenant-Hash als signierte Notification an Tenant-Admin (Notar-Pattern light)

> ***Phase 3 / falls Compliance verlangt:*** *signierte Hash-Veröffentlichung an externen Time-Stamping-Service (z.B. RFC 3161-konformer EU-Provider).*

Block J — Permissions-Anwendung

Permission-IDs

Permission	Erlaubt
`audit.read`	Audit-Trail lesen (tenant-weit), Detail-View, Filter, Suche
`audit.admin`	Export-Jobs anlegen, Aufbewahrungs-Settings ändern, Legal Hold setzen/aufheben

Bundle-Mapping (Variante 2)

Bundle	Atomare Permissions
`audit.none`	(keine)
`audit.read`	`audit.read`
`audit.admin`	`audit.read` + `audit.admin`

Anwendung in Routes

- `/admin/audit` → `audit.read`
- `/admin/audit/:id` → `audit.read`
- `/admin/audit/exports` → `audit.admin`
- `/admin/audit/exports/new` → `audit.admin`
- `/admin/audit/exports/:id` → `audit.admin` (Anlage) oder Self-Job-Owner (Status sehen)
- `/admin/audit/settings` → `audit.admin` UND `tenant.admin`

Anwendung in Per-Subject-Drawer

- Detail-View eines Contacts/Deals/Projekts zeigt Audit-Drawer wenn User `audit.read` hat
- Ohne Permission: kein Drawer sichtbar (kein Tab, kein Hinweis)

Sensible Diff-Inhalte

- HR-bezogene Diffs (Modul 14): voll sichtbar nur mit `hr.read_all` ODER `audit.admin`
- Customer-Portal-User-Diffs (Modul 15): nur mit entsprechender Modul-Permission
- Passwort-Hashes / Geheimnisse: nie als Diff-Inhalt, nur Marker „Wert geändert"

Self-Audit-Schutz

- User darf eigene Audit-Einträge sehen (kann ohne `audit.read` über `/settings/security/`-Sub-Page eigene Aktivitäten einsehen — Phase 2 Detail)
- User kann eigene Audit-Einträge nicht ändern oder löschen (DB-Constraint)

Audit-Eigene Audit-Einträge

- `audit.exported`, `audit.legal_hold_set`, `audit.retention_changed` sind sichtbar für jeden mit `audit.read`
- Kein „blinder Fleck" für Tenant-Admin — selbst Tenant-Admin-Aktionen am Audit-Log sind transparent

Klartext-Fehler

- Zugriff auf `/admin/audit` ohne `audit.read`: 403 mit *„Du hast keine Berechtigung, das Audit-Log zu sehen. Bitte Tenant-Admin kontaktieren, falls erforderlich."*

- Export-Versuch ohne `audit.admin`: Aktions-Funktion einfach nicht sichtbar, Tooltip falls dennoch angezeigt: *„Hierfür benötigst du erweiterte Berechtigungen."*
- Legal-Hold-Aufhebung ohne Begründung: *„Bitte gib einen Grund für die Aufhebung an — wird selbst geloggt."*

Block K — Activity-Stream-Integration

- Audit-Log und Activity-Stream sind **getrennte Konzepte**:
- Activity-Stream (Modul 1, Block E) ist user-facing, bezogen auf einzelne Entitäten (Contact-Aktivitäten), nicht alle Aktionen
- Audit-Log ist tenant-weit, erfasst ALLE schreibenden Aktionen, ist Compliance-Werkzeug
- **Brückenpunkt:** Manche Audit-Actions erzeugen zusätzlich Activity-Stream-Einträge (z.B. `lead.assigned` ist sowohl Audit als auch Activity)
- **Activity-Stream sieht jede Activity, deren Subject der User sehen darf** (siehe Modul 1)
- **Audit-Log sieht jede Action des Tenants**, gegated durch `audit.read` (tenant-weit, kein Subject-Permission-Filter)
- Activity-Typ `audit_event` (in Modul 1 definiert) ist nur sichtbar mit `audit.read` und zeigt Audit-Aktionen, die NICHT bereits als reguläre Activity gelistet sind (z.B. Permission-Änderungen)

Block L — Klartext-Hinweise

- **Leerer Trail (frischer Tenant):** *„Noch keine Aktionen erfasst — Audit-Einträge erscheinen, sobald jemand schreibend tätig wird."*
- **Filter ohne Treffer:** *„Keine Einträge passen zu deinen Filtern. [Filter zurücksetzen]"*
- **Subject gelöscht:** *„Das betroffene Objekt wurde inzwischen gelöscht. Snapshot-Name: ‚X'."*
- **Sensible Diff-Inhalte:** *„Aus Datenschutz-Gründen wird nur ‚Wert geändert' angezeigt."*
- **Bulk-Op-Hinweis:** *„Diese Aktion ist Teil einer Bulk-Operation mit 47 weiteren Einträgen. [Alle anzeigen]"*
- **Automation-Hinweis:** *„Ausgeführt von Automation ‚X' (Run-ID Y). [Automation öffnen] [Run-Log öffnen]"*
- **KI-Hinweis:** *„KI-Aktion auf Basis von User-Bestätigung von [User]. [KI-Prompt anzeigen]"*
- **Legal Hold aktiv:** *„Legal Hold aktiv — Aufbewahrung verlängert."*
- **Retention abgelaufen, Legal Hold setzte rückwirkend ein:** *„Hinweis: Legal Hold wurde nach Auto-Lösch-Lauf gesetzt. Einträge älter als [Retention] sind möglicherweise bereits gelöscht."*
- **Export läuft:** *„Export wird im Hintergrund verarbeitet (geschätzt X Minuten). Notification bei Fertigstellung."*

Block M — Phase 2 / spätere Features

- **Hash-Chain mit Verifikations-Tool** (siehe Block I)
- **Externes Time-Stamping** (RFC 3161 EU-Provider)
- **PDF-Bericht mit digitaler Signatur** (PandaDoc-Integration)
- **Pro-Action Sonder-Retention** (z.B. Auth/Permission 36 Monate auch bei Default 12)
- **Real-time-Audit-Feed** (Server-Sent-Events für Tenant-Admin-Live-Monitoring)
- **Audit-Anomalie-Detection** (KI erkennt verdächtige Muster: ungewöhnliche Login-Zeiten, Massen-Lösch-Aktionen, Permission-Eskalation)
- **Cross-Tenant-Trail für Plattform-Admin** (für Support-Forensik mit Audit-Eintrag pro Lookup)
- **Self-Audit für User** (`/settings/security/`-Sub-Page mit eigenen Aktivitäten der letzten 90 Tage)
- **Replay-Funktion** (für Test-Tenants: Audit-Trail in einen anderen Tenant nachspielen — sehr Phase 3)
- **Materialized Views für Audit-Statistiken** (Aktionen pro Tag, Top-Actor, Top-Subject-Type)

Architektur-Vorschriften (Querschnitt)

- **AV #6:** Audit-Trail-Default für jede schreibende Aktion (in jedem Modul Pflicht-Aufruf des `auditService.log()`)
- **AV #1, LP-10:** Klartext-Diagnostik überall (Subject-gelöscht, Bulk-Op, Automation-/KI-Bezug, Sensible Inhalte)
- **LP-1:** Tenant-Isolation strikt — Audit-Einträge sind tenant-scoped, kein Cross-Tenant-Read außer Plattform-Admin (mit eigenem Audit)
- **LP-13:** EU-Stack — Audit-Daten bleiben in Scaleway, Export-Files in Scaleway-Storage, kein Drittland-Transfer
- **LP-9:** UI-Element-Anforderungen als Liste, kein Layout
- **AV #20:** KI darf Audit-Einträge weder verändern noch löschen — Lese-Aktionen für KI sind eigenes Audit-Event (`audit.sensitive_read`-Variante mit `actor_kind = ki_agent`)

Detail-Spec-Status: DRAFT

Erste vollständige Detail-Spec für Modul 21. **Vor Bau:** Verifizierung mit Noah (zusammen mit Pflichtenheft-Sweep). Bei Implementierung dann konkrete Index-Strategie, Action-Enum-Vollständigkeit, JSONB-Diff-Serialisierungs-Format und Storage-Pfad-Strategien finalisieren.

Offene Detail-Punkte (nicht-blockierend):
- Konkretes Default-Retention finalisieren (24 Monate angenommen aus Brainstorming, mit Noah validieren ob für Geerkens passt)
- Hash-Chain-Implementierung Phase 2 detailliert (Algorithmus-Wahl, Performance-Impact bei großen Trails)
- Sensible-Diff-Heuristik: Welche Felder werden als sensibel klassifiziert (HR, Portal-User, Geheimnisse) — Liste pro Modul
- Action-Enum-Liste vollständig erst nach allen Modul-Specs (Modul 21 dokumentiert das Pattern, konkrete Action-IDs entstehen modulweise)
- Plattform-Admin-Cross-Tenant-Audit-Pattern Phase 1 oder Phase 2

Abhängige Module:
- Modul 27 (Auth/Permissions) — Permission-Bundle `audit.*`, alle Auth-bezogenen Action-IDs
- Modul 22 (Notifications) — Export-Fertigstellungs-Notification, Anomalie-Alerts (Phase 2)
- Modul 23 (Files) — Export-File-Storage in Scaleway
- Modul 17 (Automation) — Automation-Run-ID-Korrelation
- Modul 18 (KI-Layer) — KI-Prompt-ID-Korrelation
- Alle anderen Module — als Audit-Quellen (jedes Modul ruft `auditService.log()` auf bei schreibenden Aktionen)