



RPMC

RESSOURCE & PROCESS MANAGEMENT CONSOLE

PRODUKT-INFOMAPPE · VERSION 2.0 · STAND 22. JULI 2026

ORBIS-spezialisierte Access Governance für Krankenhäuser.

RPMC führt Identitäts- und Berechtigungsdaten aus ORBIS, HR, Active Directory und Dienstplan in einer modularen On-Premises-Plattform zusammen. Die Software unterstützt Lifecycle-Prozesse, Governance, Auswertungen und prüfbare Nachweisführung.

4 Quellen

ORBIS · HR · AD · DIENSTPLAN

On-Premises

BETRIEB IM KRANKENHAUSNETZ

Modular

LIZENZIERBARER FUNKTIONSUMFANG

ORBIS-Fokus

SPEZIALISIERTE GOVERNANCE

Dienstplan

GATEWAY RELEASED

KI-Arztbrief

SEPARATES MODUL · IN
ENTWICKLUNG

medivaris Software

Inhaber Karl-Heinz Roth · Rommerscheider Höhe 75
51465 Bergisch Gladbach

Hersteller, Anbieter
und Lizenzgeber von RPMC

Inhalt

Reifegrade sind im Dokument gekennzeichnet; Entwicklungsfunktionen gehören nicht zum aktuellen Produktumfang.

oder **IN ENTWICKLUNG** sind ehrlich gekennzeichnet. Alle Abbildungen stammen aus einer laufenden RPMC-Installation (Demo-Mandant „Demo Klinikum Musterstadt“).

01	Produktidentität — Ziel, Zweck, Hersteller	3
02	Marktpositionierung & Einordnung	7
03	Modulübersicht im Schnellzugriff	10
04	Match Center — die Daten-Zentrale	12
	Vier Quellen · Zwiebeln-Matching · Spaltenkonfiguration · sieben ORBIS-Anbindungswege · Sync-Steuerung	
05	Mitarbeiter-Verwaltung & Massen-Administration	17
06	Status Center — das tägliche Cockpit	21
07	Mehrsprachigkeit (DE/EN/FR/IT)	24
08	Rotationsmanager	25
09	Timeline & Aktivitätshistorie	26
10	Entscheiderboard — Gremien & OE-Anträge	27
11	Richtlinien-Center (Policy Center)	29
	SETs · Regelwerk in Fassungen · gefahrlose Simulation · JML-Automatik · Grace Period	
12	Governance & Compliance	34
13	Controlling & Analysen	42
	Report Studio · Report-Inspektor · Zugriffs-Analysen · Belegung & Bettsperren · TV-E/PPR · Kostenstellen · Kontakt-Tracing	
14	ITSM-Anbindung	51
15	MyIdentity-Portal — Self-Service mit Leitplanken	52
16	Datenschutz-Suite — jedes Werkzeug im Detail	57
17	Strukturen — OE-Baum, Editor, Notfall-OE-Automatik	63
18	Arzt-Abgleich mit LANR-Konsolidierung	67
19	Externe Identitäten	68
20	AD Center	71
21	HR & Personal — Anbindungen und Klärungsmappe	74
22	KI-Arztbrief-Pipeline — IN ENTWICKLUNG	77
23	RPMC-Assistent — die mitgelieferte KI	80
24	Benutzer, RBAC & Sicherheit — LDAP, SSO, MFA, SIEM	82
25	Plattform & Betrieb — ServerManager, Updates, Multi-Instanz	84
26	Editionen	87
27	Compliance-Mapping	88
28	Roadmap — kontinuierliche Weiterentwicklung	90
A	Glossar	91
B	Kontakt & nächste Schritte	92

Produktidentität — Ziel, Zweck, Hersteller

RPMC — Ressource & Process Management Console ist eine modular aufgebaute On-Premises-Plattform für Identity and Access Governance in Krankenhäusern mit Dedalus ORBIS als KIS. Sie verbindet ORBIS-bezogene Identitäts- und Berechtigungsprozesse mit Informationen aus HR, Active Directory und Dienstplan. Die KI-Arztbrief-Pipeline wird getrennt entwickelt und ist nicht Bestandteil des aktuellen RPMC-Produktumfangs.

1.1 Ziel und Zweck

RPMC verfolgt drei Kernziele, die sich in jedem Modul wiederfinden:

1 · Konsolidieren

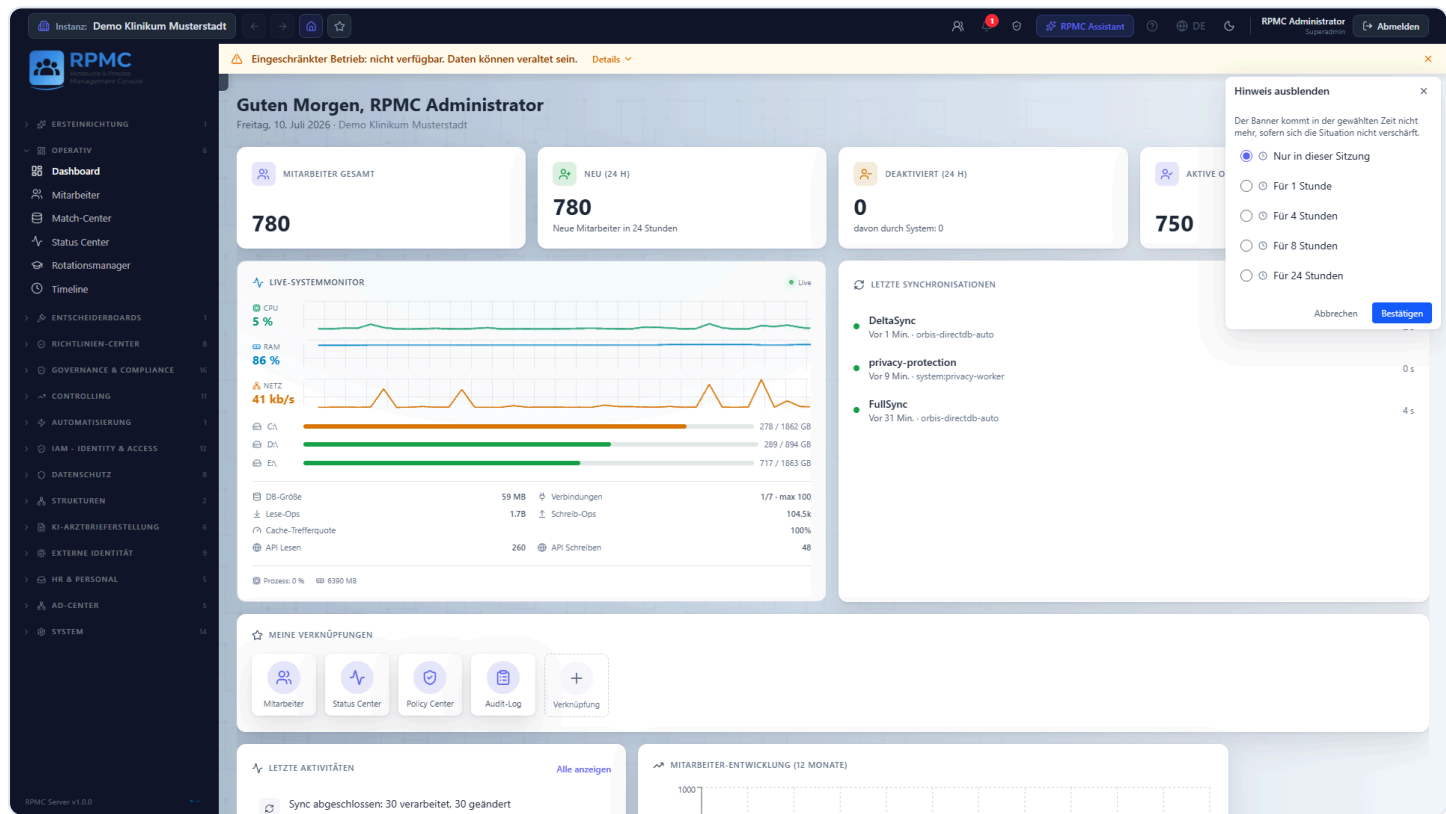
Identitäts- und Berechtigungsinformationen aus ORBIS, HR, Active Directory und Dienstplan in einer kontrollierten Sicht zusammenführen.

2 · Unterstützen

Lifecycle- und Governance-Prozesse durch Regeln, Simulationen und kontrollierte Änderungen unterstützen.

3 · Nachweisen

Berichte und Audit-Informationen für interne Kontrollen und Prüfungen strukturiert bereitstellen.



RPMC-Dashboard — zentraler Einstieg mit Kennzahlen (Mitarbeiter gesamt, aktive ORBIS-Benutzer), Live-Systemmonitor (CPU/RAM/Netz/Datenbank) und den letzten Synchronisationen. Dark-Chrome-Design: dunkle Navigations-Leisten, helle Inhaltsflächen.

1.2 Hersteller

Hersteller, Anbieter und Lizenzgeber ist medivaris Software, Inhaber Karl-Heinz Roth. Nikolas Roth wirkt ausschließlich in der Produktentwicklung mit. Vertragliche Erklärungen werden durch Karl-Heinz Roth abgegeben.

Hersteller, Anbieter & Lizenzgeber medivaris Software Inhaber Karl-Heinz Roth	Produktentwicklung Nikolas Roth
--	---

1.3 Technische Basis

Backend ASP.NET Core 8 / C# 12, PostgreSQL 16 mit Dapper-ORM, Oracle-Direktzugriff für ORBIS-DirectDB, HL7-/FHIR-Empfangsstrecken, Datei-Gateway.	Frontend React 19 / TypeScript / Vite / Tailwind 4 — moderner Web-Stack, läuft in jedem aktuellen Browser, kein Plugin, auch unter Citrix.
Echtzeit SignalR — Live-Updates ohne Browser-Refresh: Sync-Fortschritt, Worker-Status, Board-Bewegungen, proaktive KI-Hinweise.	Authentifizierung Lokal (BCrypt) + LDAP-Fallback + SSO (SAML2 / OIDC) + MFA (TOTP). Account-Lockout, Refresh-Token-Rotation, Audit je Login-Versuch.
KI Integrierte On-Premise-KI im eigenen Prozess — kein externer Dienst, kein offener Port, keine Cloud-Pflicht. Optional Cloud-LLM-Anbindung (u. a. Google Vertex AI) für Häuser, die das ausdrücklich wollen.	Lizenzierung ECDSA-P-256-signierte Lizenz-Dateien (.lic) als einzige Wahrheitsquelle für aktive Module — fälschungssicher, offline verifizierbar.

1.4 Deployment-Charakter

- **On-Premise · Datensouveränität:** RPMC läuft komplett im Krankenhaus-Netz — es besteht keine Cloud-Pflicht. Im Standardbetrieb verlassen keine Patientendaten das Haus. Wird die optionale Cloud-KI (Kapitel 23) aktiviert, werden ausschließlich pseudonymisierte Inhalte übermittelt; für diesen Fall ist ein Auftragsverarbeitungs-Vertrag nach DSGVO Art. 28 mit dem gewählten Anbieter erforderlich. Ohne aktivierte Cloud-KI arbeitet RPMC vollständig On-Premise.
- **Self-Contained Windows-Build:** Single-File-Deployment möglich, kein vorinstalliertes .NET nötig. Minimale Server-Voraussetzungen, einfaches Patch-Management.
- **RPKG-Patch-Pakete:** Updates kommen als integritätsgeprüftes RPKG-Paket (SHA-256-Manifest je Datei, Root-Hash, sequenzieller Versions-Guard) und werden vor Ort per ServerManager importiert. Der Import verifiziert die Prüfsummen fail-closed und begrenzt alle Datei-Pfade auf das Installationsverzeichnis — inklusive automatischer Datenbank-Migration im laufenden Betrieb (Kapitel 25). Eine asymmetrische Herausgeber-Signatur ist auf der Roadmap.
- **Multi-Instanz nativ:** Eine Installation verwaltet — je nach Edition — 1 bis 99 ORBIS-Instanzen mit Mandanten-Isolation auf Datenbank-Ebene. Neue Instanzen werden per Instanz-Provisioning vollautomatisch mit Mail-Vorlagen, Checklisten, Sync-Zeitplänen und Datenschutz-Konfiguration ausgestattet.

1.5 Aktuelle Größenordnung

185 REST-CONTROLLER	540+ SERVICE-KLASSEN	440+ FRONTEND-SEITEN	66 BACKGROUND-WORKER
-------------------------------	--------------------------------	--------------------------------	--------------------------------

533

DB-MIGRATIONEN

~2.290

API-ENDPUNKTE

20.000+

OBERFLÄCHEN-TEXTE JE
SPRACHE (DE/EN/FR/IT)

20+

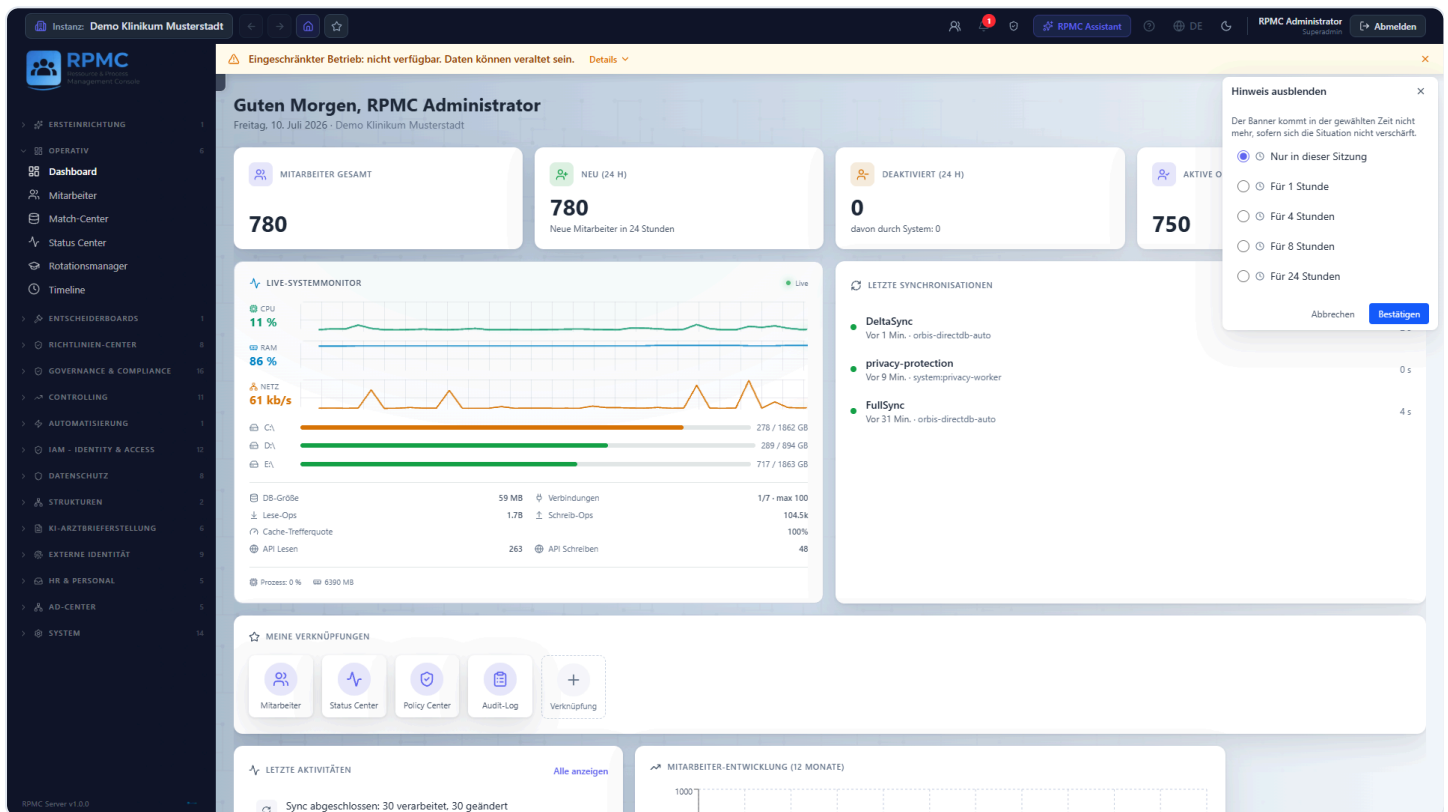
ORBIS-DIRECTDB-SUB-SYNCS

Stand 2026-07-10 — verifiziert durch automatisierten Code-Scan über das gesamte Produkt-Repository. Zum Vergleich: Anfang 2026 waren es 144 Controller und 274 Migrationen — das Entwicklungstempo ist Teil des Produkts.

1.6 Systemarchitektur im Überblick

QUELLSYSTEME → RPMC → KONSUMENTEN

Eingang: ORBIS (DirectDB, REST, HL7/FHIR, Datei), Active Directory (LDAP inkl. Write-Back), HR-Systeme (Konnektoren, CSV/XLSX/SFTP, Watchfolder), Dienstplan. **Kern:** Match Center (4-Wege), Status Center, Governance & Audit-Kette, Richtlinien-Center, Workflow-Engine, integrierte KI — auf PostgreSQL 16 mit Append-only-Audit. **Ausgang:** SIEM (CEF, 30+ Event-Typen), ITSM (HMAC-Webhook), Mail/Teams, IdP/SSO (SAML2, OIDC, SCIM), Export-Schnittstellen (PDF/XLSX/CSV, Benchmark-Anbieter).



Widget-Dashboard — konfigurierbare Kacheln mit Verknüpfungen, letzten Aktivitäten und der Mitarbeiter-Entwicklung über 12 Monate. Jeder Anwender stellt sich seinen Einstieg selbst zusammen.



RPMC – Ressource & Process Management Console

Benutzername

☐ Benutzername merken

Passwort

Anmelden

[Passwort vergessen?](#)

RPMC Server v1.0.0



Gebrandete Anmeldung — RPMC-Login mit „Benutzername merken“ und Passwort-Wiederherstellung. Portale (MyIdentity, Supervisor) erhalten eigene, im Corporate Design des Hauses gebrandete Login-Seiten.

Marktpositionierung & Einordnung

RPMC richtet sich an Krankenhäuser und Verbünde, die Dedalus ORBIS einsetzen und ORBIS-bezogene Identitäten, Rollen, OEs und Berechtigungen mit weiteren Datenquellen zusammenführen möchten.

2.1 Zielgruppe und Einsatzanlass

- IT- und IAM-Verantwortliche mit hohem manuellem Abstimmungsaufwand
- Informationssicherheit und Datenschutz mit Bedarf an nachvollziehbaren Kontrollen
- Kliniken mit mehreren ORBIS-Instanzen oder heterogenen HR-/AD-Strukturen
- Häuser, die eine On-Premises-Lösung und modulare Einführung bevorzugen

2.2 Rolle im vorhandenen IT-Stack

RPMC ist als ORBIS-spezialisierte Governance-Schicht konzipiert. Bestehende Lösungen für SSO, MFA oder unternehmensweites Identity Management können unverändert ihre jeweilige Aufgabe erfüllen. RPMC ergänzt diese Landschaft um ORBIS-bezogene Abgleiche, Lifecycle-Unterstützung, Auswertungen und Nachweise. Der konkrete Integrationsumfang wird je Krankenhaus festgelegt.

POSITIONIERUNG IN EINEM SATZ

RPMC ist eine ORBIS-spezialisierte, modular aufgebaute On-Premises-Plattform, die Identitäts- und Berechtigungsdaten aus ORBIS, HR, Active Directory und Dienstplan zusammenführt und Krankenhäuser bei Lifecycle-Prozessen, Governance, Auswertungen und prüfbarer Nachweisführung unterstützt.

2.3 Differenzierung über Funktionen

- mehrere kombinierbare ORBIS-Datenwege und kontrollierte Schreibpfade
- konsolidierte Sicht über vier Datenquellen
- klinikspezifische Module für OEs, Rollen, Governance und Analysen
- modularer On-Premises-Betrieb mit konfigurierbarem Funktionsumfang

2.4 Funktionsprofil und Abgrenzung

RPMC verbindet ORBIS-spezifische Datenwege mit HR, Active Directory und dem freigegebenen generischen Dienstplan-Gateway für SP-Expert, Polypoint und ATOSS. Module für Richtlinien, Joiner-Mover-Leaver-Prozesse, Rezertifizierung, Audit-Informationen und kontrollierte Massенbearbeitung können abhängig von Edition und Konfiguration kombiniert werden.

Notfall-OE-Status auf OE-Ebene

Die reine Gruppenzuordnung setzt in angebundenen Verwaltungswegen nicht zwingend zugleich den fachlichen Notfallstatus auf OE-Ebene. RPMC kann definierte Notfall-OE-Gruppen mit dieser Kennzeichnung abgleichen und fehlende Kennzeichnungen im kontrollierten Lauf nachziehen.

Entwicklungsmodul außerhalb des aktuellen Produkts

KI-ARZTBRIEF-PIPELINE · IN ENTWICKLUNG

Die KI-Arztbrief-Pipeline ist ein separates Entwicklungsmodul. Sie ist weder Bestandteil des aktuellen RPMC-Produktumfangs noch der derzeit angebotenen Editionen.

Bewertung im konkreten Projekt

Zeitersparnis, Abdeckungsgrad und Nutzen hängen von Datenqualität, Ausgangssystemen, Prozessgestaltung, Lizenzumfang und Konfiguration ab. Quantitative Wirkungsversprechen werden deshalb nicht pauschal abgegeben, sondern anhand eines vereinbarten Pilotumfangs und gemeinsam definierter Erfolgskriterien bewertet.

HINWEIS

Verbindlich sind ausschließlich Angebot, Leistungsbeschreibung und Vertrag.

FALLBEISPIEL AUS DER PRAXIS

Nach einer Stations-Reorganisation im Demo Klinikum Musterstadt müssen 140 Pflegekräfte neue OE-Gruppen und ein angepasstes Rollen-SET erhalten. Der klassische Weg: zwei Vollzeittage ORBIS-Klickarbeit durch die IT. Mit RPMC: Filter setzen, 140 Zeilen markieren, SET anwenden — der gesamte Vorgang inklusive Plausibilitäts-Vorschau dauert unter fünf Minuten, jede Einzeländerung landet revisionssicher in der Audit-Kette.

Modulübersicht im Schnellzugriff

Die Tabelle kennzeichnet den dokumentierten Reifegrad der Module; Entwicklungsfunktionen sind nicht Teil des aktuellen Produktumfangs.

Beta- und Entwicklungs-Module sind ehrlich markiert. Jedes Modul wird in den Kapiteln 4 bis 25 ausführlich vorgestellt.

Modul	Kurzbeschreibung	Status
Match Center	4-Wege-Konsolidierung ORBIS/AD/HR/Dienstplan, Zwiebelschalen-Matching, 7 ORBIS-Anbindungswege	RELEASED
Mitarbeiter-Verwaltung	4-Quellen-Detailansicht, Spaltenkonfiguration, Massen-Administration mit Undo-Pfad	RELEASED
Status Center	13 Prüf-Kacheln (Eintritte, Austritte, Doubletten, Mover, direkte OE-Zuweisungen ...), HR-Klärungsmappe	RELEASED
Rotationsmanager	Rotations-/Einsatzpläne für Assistenzärzte, Schichten und Bereitschaften	RELEASED
Timeline & Aktivitätshistorie	Lebenslauf jedes Mitarbeiters über alle Quellen; Unified Audit Timeline (ORBIS + RPMC)	RELEASED
Entscheiderboard	Gremien-Kanban mit Vier-Augen, Quorum, E-Mail-Voting; OE-Board mit echtem OE-Antragsweg	RELEASED
Richtlinien-Center (Policy Center)	SETs, Zuteilungsregeln in Fassungen, gefahrlose Simulation, JML-Automatik, Grace Period	RELEASED
Governance & Compliance	Compliance-Score, Rezertifizierung, SoD, Audit-Kette, Login-Sicherheit, Unified Audit, OP-Management	RELEASED
Report Studio	Report-Bibliothek (180+), Builder, KI-Erstellung, RGEN-Center, ORBIS-Report-Inspektor	BETA
Zugriffs-Analysen	Gesamtübersicht, Cluster-Affinität, Zugriffs-Geflecht mit dynamischen OE-Gruppen, Verlegungs-Analytics	RELEASED
Raum-/Bettenbelegung & Kapazität	Live-Belegung bis auf Betten-Ebene, Bettsperren-Kontrolle, Soll/Ist-Kapazitäts-Reporting	RELEASED
TV-E / PPR-2.0-Dashboard	Pflegepersonal-Bemessung: Soll/Ist, Compliance-Rate, Unterschreitungs-Alarme	RELEASED
Kostenstellen	KST-Übersicht, OE-Zuordnung, Nutzungs-/Abrechnungsdaten je Periode	RELEASED
Patienten-Kontakt-Tracing	Exposure-Radar für Hygiene-Teams, pseudonymisiert (DSGVO Art. 9)	RELEASED
ITSM-Integration	Webhooks mit HMAC-Signatur, Zeitstempel und Replay-Schutz	RELEASED
MyIdentity-Portal	Self-Service: Profil, Rotationsplan, Rechte-Selbstbeantragung, Break-the-Glass	RELEASED
Pfortenauskunft / Auskunftssperre	DSGVO-Sperrstatus, Heatmaps, Nach-Todesdatum-Auswertung, Audit-of-Audit	RELEASED

Modul	Kurzbeschreibung	Status
Patientensuche-Überwachung	VIP-/Personenschutz mit Strict-Match, Scan-Panel und pseudonymisierten Treffern	RELEASED
Fall-Zugriffs-Audit (Forensik)	Fallbezogene Zugriffs-Forensik live aus ORBIS, inkl. Notfall-Kontext	RELEASED
Verarbeitungsverzeichnis (VVT)	DSGVO Art. 30 — Verarbeitungstätigkeiten direkt in RPMC gepflegt	RELEASED
Löschfristen-Verwaltung	Aufbewahrungs- und Löschregeln je Datenkategorie	RELEASED
OE-Struktur & Editor	Live-Baum (logisch/physisch), exklusiver Editor, Versionen, Diff, Import/Export	RELEASED
Notfall-OE-Automatik Abgleich definierter Notfall-OE-Gruppen mit dem Notfallstatus auf OE-Ebene; fehlende Kennzeichnungen können kontrolliert nachgezogen werden RELEASED		
Arzt-Abgleich (LANR)	ORBIS-vs.-HR-Prüfliste mit LANR-Konsolidierung und KBV-Prüfziffer	RELEASED
Externe Identitäten	Befristete ORBIS-Zugänge für Externe: Kategorien, Genehmigung, Auto-Ablauf	RELEASED
AD Center	AD/LDAP-Anbindung, SSO-Federation, AD-Administration aus RPMC heraus	IN ENTWICKLUNG
HR & Personal	HR-Connectoren (Personio, SAP, Workday ...), Multi-Source-Merge, Klärungsmappe, Watchfolder	RELEASED
KI-Arztbrief-Pipeline Separates Entwicklungsmodul für Entwurf, ärztliche Freigabe und geplanten HL7-Rückweg; nicht Bestandteil des aktuellen Produkts oder der Editionen IN ENTWICKLUNG		
RPMC-Assistent	Mitgelieferte On-Premise-KI: Chat, Aktionen, Report- und Workflow-Erstellung	RELEASED
RBAC, MFA, SSO, SIEM	Profile + Rollen + Direct-Grants, TOTP-MFA, SAML2/OIDC, SCIM 2.0, CEF-SIEM-Export	RELEASED
Workflow-Engine (DAG)	Visueller Editor, 55+ Node-Typen, Versionierung, KI-Workflow-Erstellung	RELEASED
Break-the-Glass	Notfall-Rechteerweiterung mit Doppelbestätigung, SIEM-Alarm, Auto-Entzug	RELEASED
ServerManager & RPKG	Installation, signierte Updates, Lizenz-Verwaltung vor Ort, DB-Migration im Betrieb	RELEASED
Multi-Instanz & Instanz-Provisioning	Bis 99 Instanzen je Installation, automatische Erstausrüstung neuer Instanzen	RELEASED
Dienstplan-Gateway Generisches Gateway für SP-Expert, Polypoint und ATOSS RELEASED		
Hochverfügbares Multi-Tenant-System HA-Architektur für Klinikverbünde IN ENTWICKLUNG		

Darüber hinaus enthält RPMC zahlreiche Basis-Module (Mail-System, Theme-Katalog, Anomalie-Erkennung, Analytics-Bibliothek, Auto-On-/Offboarding u. v. m.), die in den Fachkapiteln mitbeschrieben werden.

Match Center — die Daten-Zentrale

RELEASED

Alles in RPMC beginnt im Match Center. Hier laufen die vier Datenquellen des Krankenhauses zusammen, hier entsteht die eine konsolidierte Wahrheit über jeden Mitarbeiter — und hier wird konfiguriert, auf welchem der sieben Wege RPMC mit ORBIS spricht.

4.1 Warum vier Quellen?

In jedem Krankenhaus existiert jeder Mitarbeiter mehrfach: als ORBIS-Benutzer mit Rollen und OE-Zuordnungen, als Active-Directory-Konto mit Gruppenmitgliedschaften, als HR-Personalsatz mit Vertrag und Eintrittsdatum — und als Planstelle im Dienstplan. Diese vier Welten werden von vier verschiedenen Abteilungen gepflegt und laufen zwangsläufig auseinander: Namensschreibweisen differieren, Austritte erreichen die IT verspätet, AD-Konten überleben ihre Besitzer. Genau diese Drift ist das Einfallstor für verwaiste Konten, Überberechtigungen und Audit-Befunde.

ORBIS (KIS)

Die klinische Wahrheit: Benutzer, Rollen, OE-Gruppen, Einrichtungen, Sessions. RPMC liest sie in ORBIS-Tiefe — bis hinunter zu einzelnen Tabellenfeldern.

Active Directory

Die IT-Wahrheit: Konten, Gruppen, Anmeldedaten, letzte Logins. LDAP-Sync in beide Richtungen (Write-Back möglich).

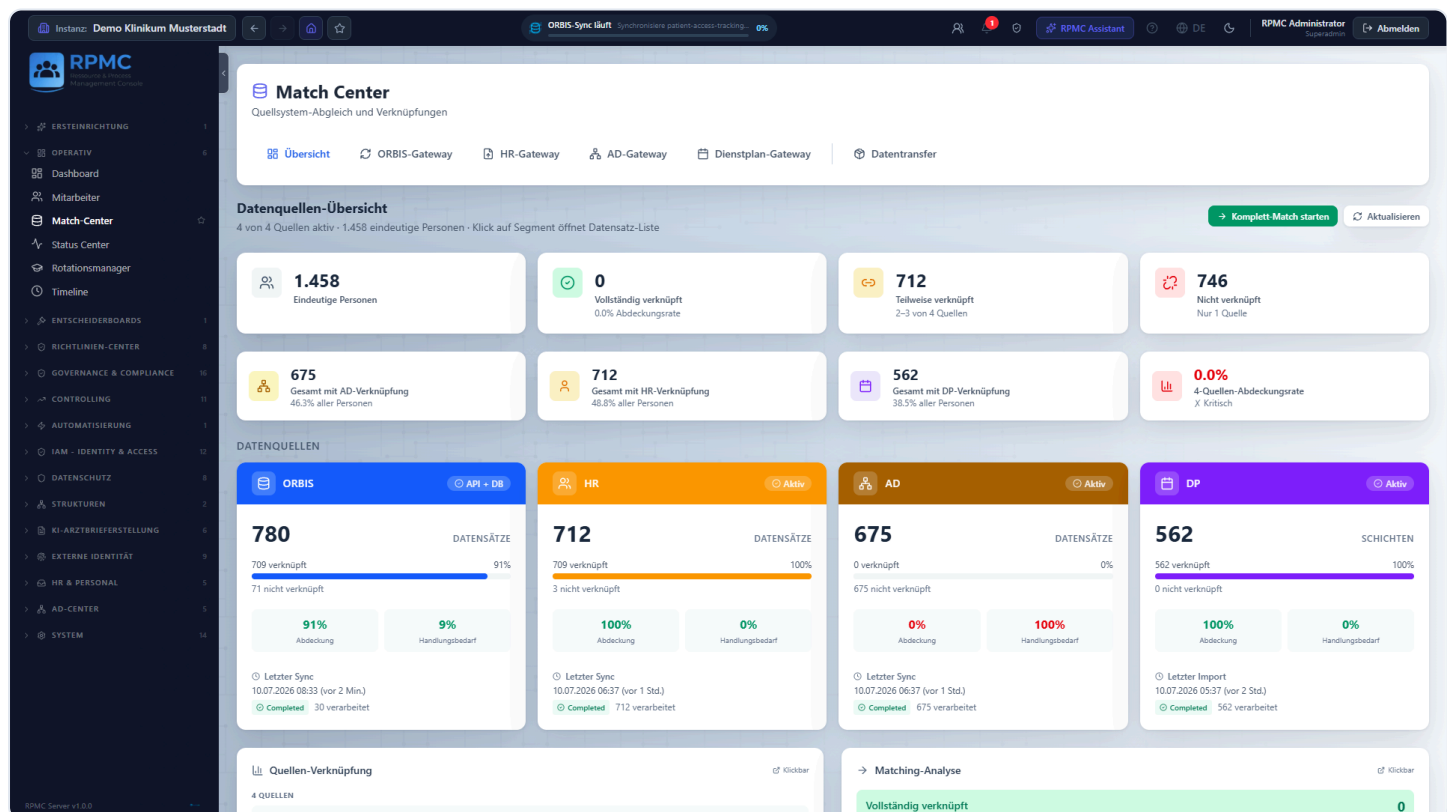
HR-System

Die arbeitsrechtliche Wahrheit: Personalnummer, Vertrag, Ein-/Austritt, Funktion, Einrichtung. Über Konnektoren, Dateien oder Watchfolder — auch aus mehreren HR-Quellen parallel.

Dienstplan

Die operative Wahrheit: Wer ist wann wo eingeplant? Grundlage für Abweichungs-Prüfungen und künftig schichtbasierte Rechte.

Gateway · RELEASED



Match-Center-Übersicht — alle vier Datenquellen mit Datensatz-Zahlen (ORBIS 780, HR 712, AD 675, Dienstplan 562), Verknüpfungs-KPIs und Abdeckungs-Balken je Quelle. Der Konsolidierungsgrad des Hauses wird zur messbaren Kennzahl.

NUTZEN

Der Konsolidierungsgrad („x % der Mitarbeiter in allen Quellen sauber verknüpft“) ist eine direkt zitierfähige Kennzahl für NIS2- und DSGVO-Art.-32-Nachweise. Lücken sind kein Bauchgefühl mehr, sondern konkrete, exportierbare Listen — etwa „alle HR-Datensätze ohne ORBIS-Konto“ als Onboarding-Rückstand oder „alle AD-Konten ohne HR-Pendant“ als potenzielle Schatten-Accounts.

4.2 Das Zwiebelschalen-Prinzip

Herzstück der Konsolidierung ist der mehrstufige Matching-Algorithmus. RPMC arbeitet sich wie durch Zwiebelschalen von der härtesten zur weichsten Evidenz vor — jede Schale fängt nur das, was die härtere Schale davor nicht sicher zuordnen konnte, und jede Zuordnung trägt ihre Konfidenz sichtbar mit sich:



Das Ergebnis wird als Segment-Verteilung sichtbar: Jede Kombination der vier Quellen bildet ein eigenes Segment (15 mögliche Kombinationen). Unsichere Treffer landen nie stillschweigend im Bestand, sondern in der Prüf-Queue — der Mensch bestätigt, das System lernt.

FALLBEISPIEL

Eine examinierte Pflegekraft heißt in ORBIS „Müller-Schmidt“, im HR-Export „Mueller Schmidt“ und im AD „MSchmidt“. Kein exakter Schlüssel greift. Schale 2 normalisiert Umlaute und Bindestriche, Schale 3 bestätigt per Distanz-Vergleich, Schale 4 sichert über die AD-HR-Querreferenz ab: eine Person, ein konsolidiertes Profil — ohne dass jemand eine Mapping-Tabelle pflegen musste.

WAS KLASSISCHE IAM-SYSTEME HIER NICHT KÖNNEN

Generische Suites vergleichen typischerweise zwei Systeme über starre Schlüssel-Mappings. Ein deutschsprachiges 4-Wege-Matching mit Umlaut-Logik, medizinischen Titel-Synonymen und lernender Cross-Referenz — abgestimmt auf ORBIS-Namenskonventionen — gibt es dort nicht.

4.3 Spaltenkonfiguration & individuelle Ansichten

Konsolidierte Daten nützen nur, wenn jede Rolle im Haus *ihre* Sicht darauf bekommt. Überall in RPMC — von der Mitarbeiterliste bis zu den Analysen — lassen sich Tabellen frei konfigurieren: Felder aus allen vier Quellen wählbar, Reihenfolge per Drag-and-Drop, Profile speicherbar (persönlich oder global für alle). Die Personalabteilung arbeitet mit Vertrags-Spalten, die IT mit Konten- und Rollen-Spalten, das Controlling mit Kostenstellen — dieselben Daten, drei maßgeschneiderte Ansichten, einmal eingerichtet und dauerhaft gespeichert.

4.4 Die sieben ORBIS-Anbindungswege

Kein Krankenhaus gleicht dem anderen: Oracle-Lizenzlage, Netzwerk-Topologie und Sicherheitsrichtlinien unterscheiden sich fundamental. RPMC schreibt deshalb keinen Anbindungsweg vor, sondern bietet **sieben Wege**, die frei kombinierbar sind — der Betriebsmodus ergibt sich aus den aktivierten Quellen, pro Datendomäne ist immer genau ein „Owner“ definiert, sodass niemals zwei Wege dieselben Daten konkurrierend schreiben:

Weg	Beschreibung & typischer Einsatz
1 · REST-API	Die offizielle Dedalus User-Provisioning-API: Mitarbeiter, Benutzer, Rollen, OE-Gruppen, Kataloge, Adressen/Erreichbarkeiten — lesend und schreibend. Der lizenzschonende Standardweg; ein Fehlerquoten-Wächter stoppt Übernahmen automatisch, bevor fehlerhafte API-Antworten den Bestand verfälschen.
2 · Direct DB	Direkter Oracle-Lesezugriff auf die ORBIS-Datenbank mit 20+ feingranularen Sub-Syncs (Stammdaten, Sessions, Belegung, Ereignisprotokolle, Audit ...). Maximale Tiefe für Forensik, Belegung und Echtzeit-Auswertungen — inklusive expliziter Oracle-Lizenz-Bestätigung im Produkt, damit die Lizenzfrage dokumentiert entschieden ist.
3 · Schattendatenbank (Werkzeug)	Ein 1:1-Offline-Klon relevanter ORBIS-Strukturen, den RPMC per Werkzeug (OrbisDumper) aus einem Massenexport aufbaut und bei Bedarf neu zieht (kein automatischer Live-Abgleich). Analysen und Reports können gegen den Klon laufen — null Last und null Risiko auf der produktiven ORBIS-Datenbank; ideal für rechenintensive Auswertungen, Test- und Schulungsstellungen.
4 · HL7 (MLLP)	Empfang von ADT-/ORU-/MFN-Nachrichten über einen eigenen MLLP-Listener je Instanz (ACK-Handling, IP- u. a. als vorgesehener Datenweg für die in Entwicklung befindliche KI-Arztbrief-Pipeline DB-Zugriff gewünscht ist.
5 · FHIR	Moderne FHIR-Ressourcen (u. a. Practitioner) werden in Staging-Bereiche übernommen und über einen Match-Report kontrolliert zugeführt — nie als Blind-Import. Zukunftsweg Richtung Interoperabilitäts-Vorgaben.
6 · DCS-Kopplung (in Klärung)	Vorgesehene Anbindung über die Dedalus-Kommunikations-Infrastruktur des Hauses. Das konkrete DCS-Exportformat wird je Kundensituation evaluiert; derzeit noch kein produktiver Datenweg — als Import-Profil vorbereitet, sobald das Format feststeht.
7 · Datei-Gateway	Acht Profiltypen für Datei-basierte Übernahmen (Rollen-Transfer, Kostenstellen-Stamm, Stagings) per CSV/XLSX — der pragmatische Weg für Alt-Systeme, Übergangsphasen und Häuser mit strikter Netztrennung.

EINORDNUNG

Die kombinierbaren ORBIS-Datenwege ermöglichen eine Anpassung an Lizenz-, Infrastruktur- und Datenschutzvorgaben des jeweiligen Hauses. Welche Wege eingesetzt werden, wird projektspezifisch festgelegt.

Match Center
Quellsystem-Abgleich und Verknüpfungen

Übersicht ORBIS-Gateway HR-Gateway AD-Gateway Dienstplan-Gateway Datentransfer

Synchronisation Verbindungsmodi Direct DB API-Verbindung Snapshots & Verlauf Kataloge

Testlauf Delta-Sync Voll-Sync

Sync-Verlauf 4

ID	Typ	Status	Gestartet	Dauer	Gesamt	Neu	Aktualisiert	Ausgelöst von	Detail
#11	Delta Sync	Completed	10.7.2026, 08:33:12	2.3s	30	—	~30	orbis-directdb-auto	
#6	Full Sync	Completed	10.7.2026, 08:02:14	4.4s	30	+30	—	orbis-directdb-auto	
#2	Delta Sync	Completed	10.7.2026, 07:05:45	2m 0s	150	—	~3	demo-seed	
#1	Full Sync	Completed	10.7.2026, 05:32:45	5m 0s	150	+150	—	demo-seed	

Seite 1 von 1 · 4 Einträge 25 pro Seite

ORBIS-Gateway — Synchronisation, Verbindungsmodi, Direct DB, API-Verbindung und Kataloge in einem Bereich; Testlauf, Delta-Sync und Voll-Sync per Klick, darunter der aufgeklappte Sync-Verlauf mit Ergebnis je Lauf.

Synchronisation aktiviert (Master)
Alle aktivierten Sync-Typen laufen automatisch nach ihren individuellen Zeitplänen.

Live-Abgleich (near-real-time)
Erkennt Stammdaten-Änderungen in ORBIS über die LDAT-Spalte und gleicht betroffene Mitarbeiter automatisch ab. Zuordnungen (Rollen/OE/Einrichtungen) bleiben am periodischen Sync.

Intervall: 30 s

☒ Alle aktiv Alle jetzt ausführen

SYNC-TYP	AKTIV	INTERVALL	LETZTER LAUF	STATUS	NÄCHSTER LAUF	AKTION
Mitarbeiter-Hauptsync employee-main	☒	30 min	vor 5 min 2.7s	success	in 24 min	Jetzt
Kalenderzugriff calendar-access	☒	24 h	vor 35 min 0.0s	partial ORBIS calendar read failed: ORBIS Dire...	in 23 h	Jetzt
capacity-snapshot capacity-snapshot	☒	5 min	vor 35 min 0.0s	partial ORBIS Direct DB not available for this L...	17.07, 08:03	Jetzt
Cross-OE-Anforderungen cross-oe-request	☒	24 h	vor 35 min 0.0s	partial ORBIS Direct DB not available for this L...	in 23 h	Jetzt
Verteilerguppen distribution-groups	☒	30 min	vor 4 min 0.0s	success	in 25 min	Jetzt
Effektive Berechtigungen effective-permissions	☒	30 min	vor 5 min 0.0s	partial SEC_F_CATEGORIZATION/SEC_F_CATEG...	in 24 min	Jetzt
Erweiterte MA-Daten employee-extended	☒	30 min	vor 5 min 0.0s	failed ORBIS Direct DB not available for this L...	in 24 min	Jetzt
Login-Präsenz keycloak-presence	☒	30 min	vor 5 min 0.0s	success	in 24 min	Jetzt
Kostenstellen kostenstellen	☒	30 min	vor 4 min 0.0s	failed ORBIS Direct DB not available for this L...	in 25 min	Jetzt
Raum-/Bettenbelegung occupancy	☒	30 min	vor 3 min 0.0s	failed ORBIS Direct DB not available for this L...	in 26 min	Jetzt
occupancy-daily occupancy-daily	☒	24 h	vor 35 min 0.0s	success	in 23 h	Jetzt
OE-Gruppen oe-groups	☒	30 min	vor 5 min 0.0s	failed ORBIS Direct DB not available for this L...	in 24 min	Jetzt
OE-Struktur oe-structure	☒	30 min	vor 5 min 0.0s	failed ORBIS Direct DB not available for this L...	in 24 min	Jetzt
patient-access-tracking patient-access-tracking	☒	24 h	—	—	vor 36 min	Jetzt

Direct-DB-Einstellungen — Master-Schalter, Live-Abgleich und Zeitpläne pro Sync-Typ (20 Typen einzeln aktivier- und planbar). Jeder Sub-Sync zeigt seinen letzten Status; auf der Demo-Instanz ohne Oracle-Verbindung weisen einzelne Typen ehrlich „failed/partial“ aus, statt Fehler zu verschweigen.

4.5 Sync-Steuerung: Diagnose, Abbruch, Locks

Synchronisation ist bei RPMC kein Blackbox-Job, sondern ein steuerbarer Prozess. Die Verbindungsdiagnose prüft jeden Anbindungsweg per Klick; die Live-Sync-Aktivität zeigt laufende Phasen in Echtzeit. Zwei Funktionen, die Administratoren besonders schätzen:

- **Synchronisation vorzeitig beenden:** Ein laufender Voll-Sync lässt sich kontrolliert abbrechen — der Lauf endet sauber als „cancelled“, ohne halbfertige Datenstände zu hinterlassen. Kein Warten auf das Ende eines versehentlich gestarteten Groß-Syncs.
- **Locks entfernen:** Bleibt nach einem Server-Neustart ein Sync-Lock stehen („Sync läuft bereits“), löst ihn der Administrator per Knopfdruck — ohne Datenbank-Konsole, ohne Support-Ticket.

The screenshot displays the RPMC Administrator interface. The top navigation bar includes the instance name 'Demo Klinikum Musterstadt', user 'RPMC Administrator', and a 'Logout' button. A left sidebar lists various system components like 'ERST-EINRICHTUNG', 'OPERATIV', 'MATCH-CENTER', etc. The main content area is divided into two sections.

The upper section is a table of sync tasks:

Task Name	Status	Frequency	Last Sync	Next Sync	Action
OE-Struktur	failed	30 min	vor 6 min 0.0s	in 23 min	Jetzt
patient-access-tracking	—	24 h	—	vor 37 min	Jetzt
Ärzte-Verzeichnis	failed	30 min	vor 6 min 0.0s	in 23 min	Jetzt
Qualifikationen	success	30 min	vor 6 min 0.0s	in 23 min	Jetzt
Service-Anforderungen	partial	24 h	vor 36 min 0.0s	in 23 h	Jetzt
TV-E Auslastung	success	30 min	vor 4 min 0.0s	in 25 min	Jetzt
Unified Audit	partial	30 min	vor 4 min 0.1s	in 25 min	Jetzt
user-context	failed	30 min	vor 6 min 0.0s	in 23 min	Jetzt

The lower section, titled 'Verbindungsdiagnose & Sync-Monitor', contains three buttons: 'Verbindung prüfen', 'Live-Monitor AUS', and 'Synchronisation vorzeitig beenden'. Below these is a 'Sync-Aktivität' log showing recent sync events with details like status (partial, success, failed), task name, timestamp, and duration. At the bottom, there are two toggle switches for 'Aktivierte Module': 'Live OE-Struktur' and 'OE-Gruppen-Mapping'.

Verbindungsdiagnose & Sync-Monitor — „Verbindung prüfen“, „Synchronisation vorzeitig beenden“ und „Locks entfernen“ direkt neben der Live-Sync-Aktivität: Betriebssicherheit als Bedienkonzept.

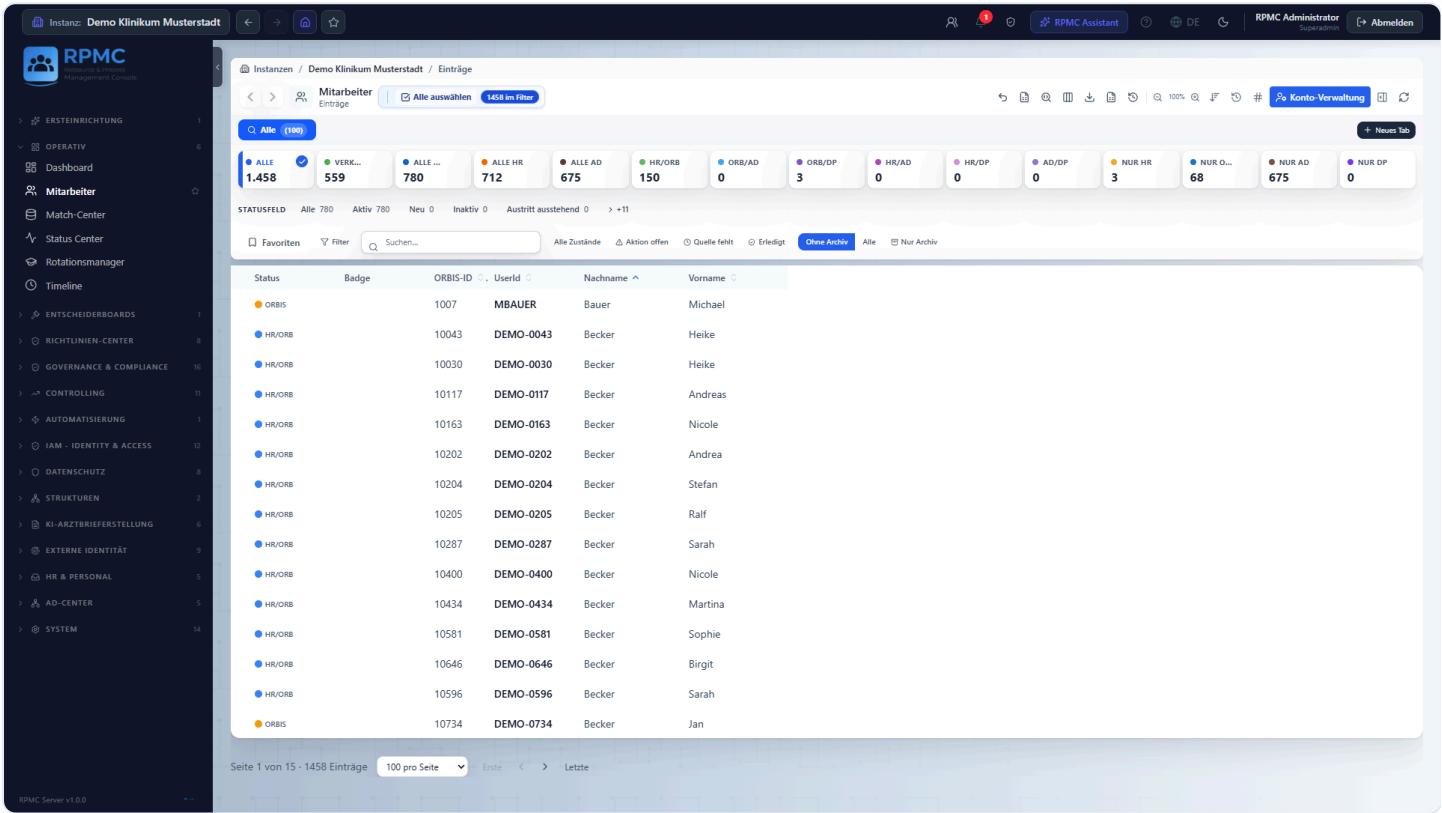
FALLBEISPIEL

Freitagnachmittag startet ein Kollege versehentlich einen Voll-Sync über alle Sub-Syncs. Früher hieß das: warten oder Dienst durchstarten und Daumen drücken. In RPMC: „Synchronisation vorzeitig beenden“ — der Lauf schließt kontrolliert ab, der geplante Delta-Sync übernimmt am Abend regulär. Der abgebrochene Lauf steht mit Status „cancelled“ nachvollziehbar im Verlauf.

Mitarbeiter-Verwaltung & Massen-Administration RELEASED

Die Mitarbeiter-Verwaltung ist die zentrale Arbeitsfläche für alle Personen-Daten des Hauses. Jeder Mitarbeiter erscheint konsolidiert aus allen vier Quellen — und alles, was in ORBIS nur einzeln und mühsam geht, geht hier gebündelt, gefiltert und in Sekunden.

5.1 Die Liste: eine Sicht auf alle Quellen



Mitarbeiterliste — 1.458 Einträge mit Quellen-Filterkarten (alle Kombinationen aus HR/ORBIS/AD/Dienstplan), Status-Filtern und frei konfigurierbarer Tabellenansicht. Ein Klick auf eine Quellen-Kombination filtert exakt das zugehörige Segment.

Filter nach Quellen-Kombination, Status, Einrichtung, Funktion und Freitext lassen sich beliebig verketteten. Badges zeigen Mehrfach-Verträge, Doubletten und Quellen-Konflikte direkt in der Zeile. Die Spaltenkonfiguration (Kapitel 4.3) macht aus der einen Liste beliebig viele rollenspezifische Arbeitslisten — inklusive CSV-Export für Controlling und Audit.

5.2 Die Detailansicht: das 4-Quellen-Dossier

Dr. med. Heike Becker, ACTIVE
DEMO-0043 · PNr: 1000043 · ORBIS: DEMO-0043

PDF XLSX

Übersicht ORBIS-Stammdaten Adressen & Erreichbarkeiten Rollen OE-Gruppen Einrichtungen Virt. Einz. Funktionen Qualifikationen SETs Mitarbeiterstatus Kalender OE-Zugriff

Effektive Berechtigungen Passwort Sync Notizen Timeline Aktivitäts-Log Konto-Verwaltung Risiko AD

Doubletten-Vergleich In Klärungsmappe Felder

HR	ORBIS
Personalnummer 1000043	Name Becker
Vorname Demo	Vorname Heike
Nachname MA-42	Titel Dr. med.
Funktion —	MA-Kürzel DEMO-0043
Status —	Geburtsname —
Einrichtung —	Geburtsdatum —
OE-Gruppe Demo	Eintritt 21.4.2020, 02:00:00
E-Mail —	Austritt —
Telefon —	Berufsbezeichnung Assistenzarzt
Eintrittsdatum —	Haupt-OE Kürzel —
Austrittsdatum —	Haupt-OE Name —
	Letzte ORBIS-Änderung —
	Letzte ORBIS-Anmeldung —

Active Directory	Dienstplan
Keine Daten aus dieser Quelle	Schichtdatum 4.7.2026
	Schichttyp Bereitschaft
	Abteilung CH
	Station CH-5A
	Rolle/Funktion —
	Letzter Import 10.7.2026, 07:37:41

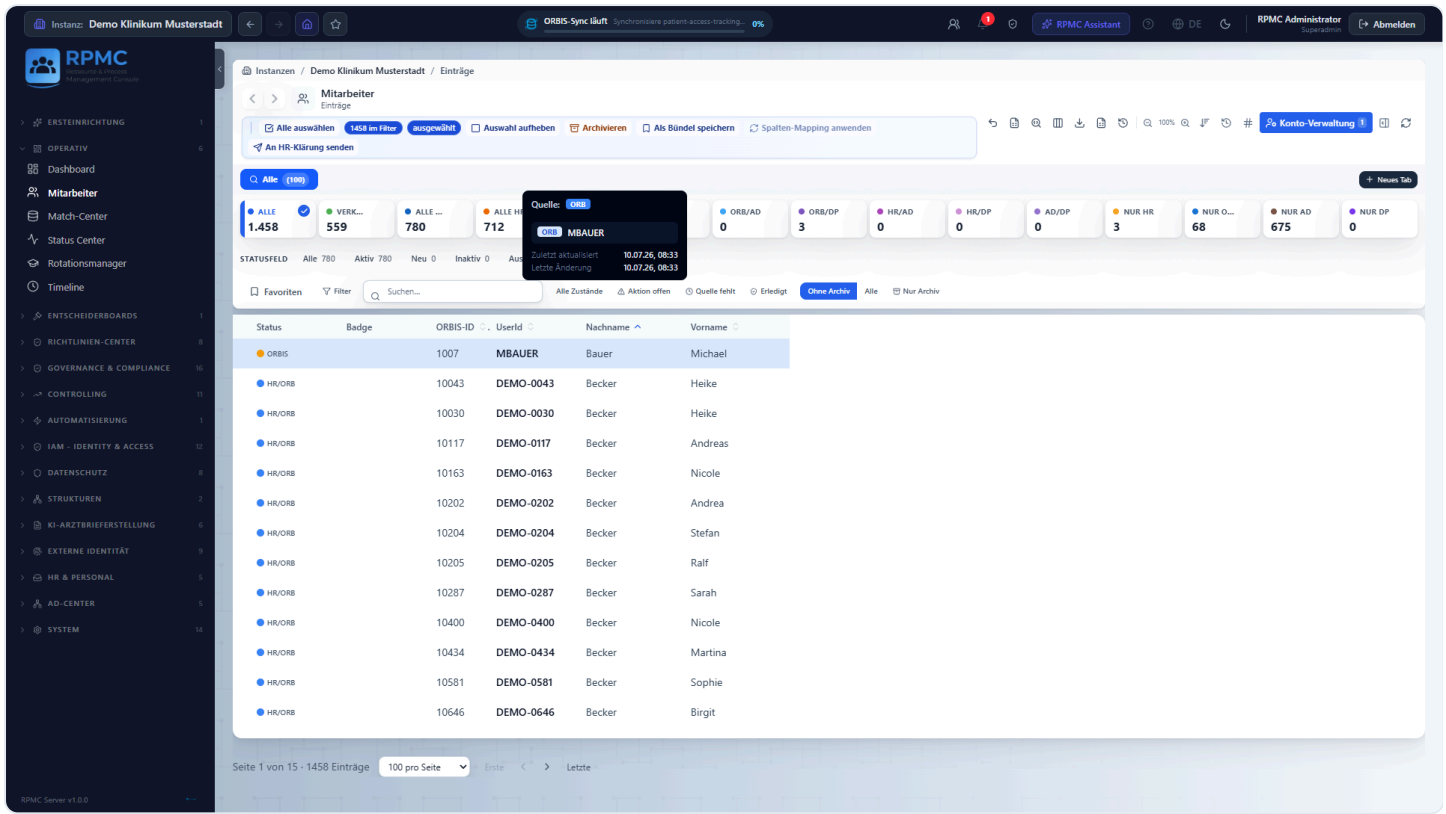
Mitarbeiter-Detail — der 4-Quellen-Vergleich (HR / ORBIS / AD / Dienstplan) nebeneinander, darunter über 20 Fach-Reiter: Rollen, OE-Gruppen, Kalender, Effektive Berechtigungen, Kontakt, Timeline, Sync-Verlauf u. v. m.

Die Detailansicht zeigt jeden Mitarbeiter als vollständiges Dossier: Stammdaten aus allen Quellen im direkten Vergleich (Abweichungen werden markiert, nicht stillschweigend überschrieben), dazu Fach-Reiter für Rollen, OE-Gruppen, effektive Berechtigungen, Qualifikationen, Adressen und Erreichbarkeiten (mit ORBIS-Schreibweg über die REST-API), Kalender, Aktivitäts-Timeline und den kompletten Sync-Verlauf. ORBIS-Konto-Operationen — Anlegen, Sperren, Reaktivieren, Deaktivieren — laufen direkt aus dem Dossier, ohne Wechsel ins KIS.

FALLBEISPIEL

Ein Mitarbeiter erscheint doppelt mit unterschiedlichen Personalnummern. Im Dossier zeigt der Quellen-Vergleich: ORBIS und HR führen den Nachnamen in Umlaut-Varianten. Der Duplikat-Abgleich führt beide Datensätze kontrolliert unter einer Personen-Gruppe zusammen — die Historie beider Ursprünge bleibt erhalten.

5.3 Massen-Administration: kontrollierte Sammelvorgänge

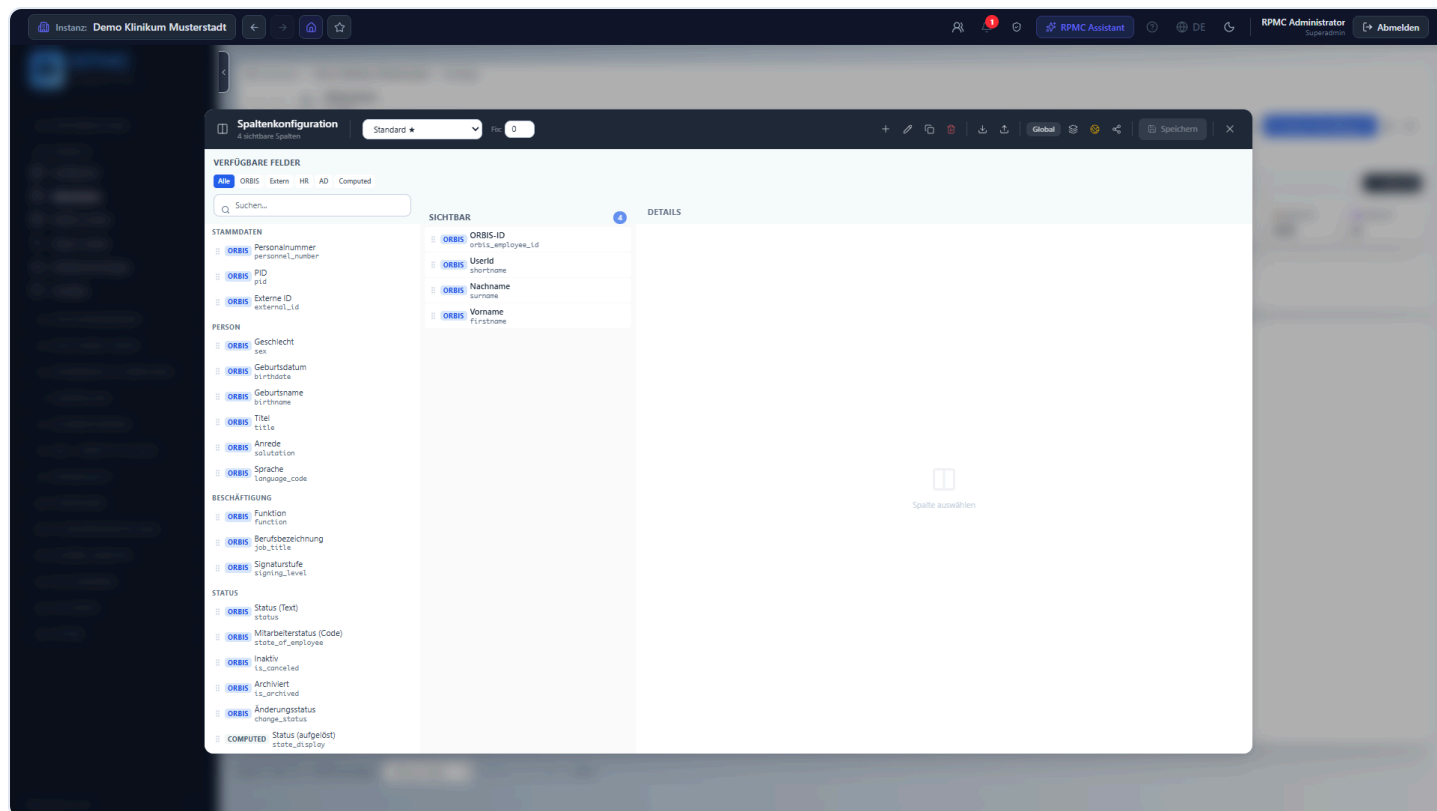


Massen-Aktionen — nach der Zeilen-Auswahl erscheint die Aktionsleiste: Alle auswählen, Archivieren, Als Bündel speichern, Spalten-Mapping anwenden, An HR-Klärung senden. Jede Aktion wirkt auf die gesamte Auswahl.

Das Herzstück für den Betriebsalltag: Beliebige Filter-Ergebnisse werden markiert und in **einem** Vorgang bearbeitet — Rollen und OE-Gruppen zuweisen oder kopieren, SETs anwenden, Status setzen, archivieren, deaktivieren, reaktivieren, an die HR-Klärungsmappe übergeben. Vor der Ausführung zeigt RPMC eine Vorschau; nach der Ausführung existiert ein vollständiger Snapshot mit Feld-Diff je Mitarbeiter. **In zwei Sekunden ist erledigt, was zuvor Stunden dauerte** — und anders als bei manueller Klickarbeit ist jeder Einzelschritt auditiert und rücknehmbar.

RETURN ON INVEST

Praktikanten-Welle zum Semesterende: 40 Konten deaktivieren. Manuell in ORBIS: ein guter halber Arbeitstag. In RPMC: Filter „Funktion = Praktikant · Eintritt vor 6 Monaten“, alle markieren, Batch-Deaktivierung — unter einer Minute, inklusive Audit-Eintrag pro Konto und gesperrten (nicht gelöschten) ORBIS-Benutzern. Bei nur einer solchen Welle pro Quartal amortisiert sich das Modul über die eingesparte IT-Zeit; der eigentliche Wert liegt im Sicherheitsgewinn: keine vergessenen Konten mehr.



Spaltenkonfiguration — verfügbare Felder nach Quelle gefiltert, Sichtbar-Liste per Drag-and-Drop sortierbar, Profile speicherbar (persönlich, global, Standard). Einmal konfiguriert, immer wieder abrufbar.

5.4 Weitere Werkzeuge

- **Mitarbeiter vergleichen:** bis zu vier Mitarbeiter nebeneinander — ideal, um Berechtigungs-Unterschiede innerhalb eines Teams aufzuklären.
- **Bündel („Als Bündel speichern“):** eine Auswahl wird als benanntes Arbeitspaket gesichert und später weiterbearbeitet.
- **Instanzübergreifendes Kopieren:** Mitarbeiter samt Zuordnungen kontrolliert in eine andere ORBS-Instanz übernehmen — für Verbünde mit Personal-Rotation zwischen Häusern.
- **Auto-Onboarding/Offboarding:** Template-basierte Ketten (ORBS-Konto, Rollen, OE-Gruppen, AD-Verknüpfung, Checkliste, Mail) laufen pro Mitarbeiter oder als Bulk aus dem Status Center.

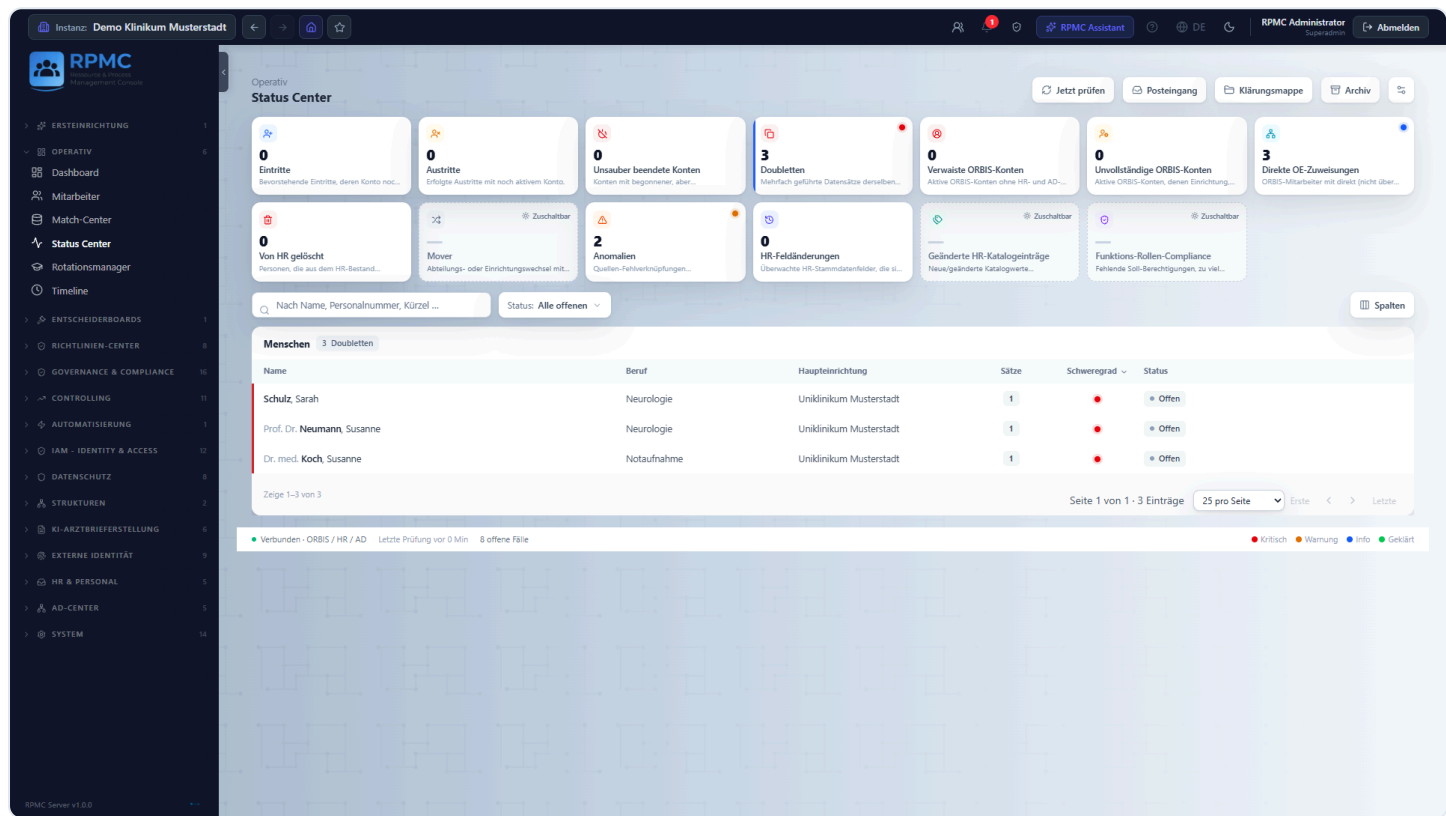
WAS KLASSISCHE IAM-SYSTEME HIER NICHT KÖNNEN

Generische IGA-Suiten provisionieren asynchron über Connectoren — Ergebnis-Kontrolle erst Minuten später, Rücknahme als neues Ticket. RPMC arbeitet interaktiv direkt am konsolidierten ORBS-Bestand: Vorschau vor der Änderung, Snapshot nach der Änderung, Undo-Pfad inklusive. Diese Kombination aus Tempo und Sicherheitsnetz ist im Krankenhausmarkt einzigartig.

Status Center — das tägliche Cockpit RELEASED

Das Status Center ist das zentrale Arbeitswerkzeug für den IAM-Alltag: Es überwacht die vier Datenquellen kontinuierlich, verdichtet jede Auffälligkeit zu einer Prüf-Kachel und macht aus Beobachtungen bearbeitbare Fälle mit Zuständigkeit, Status und Frist — statt Mail-Erinnerungen und Excel-Listen.

6.1 Dreizehn Prüf-Kacheln



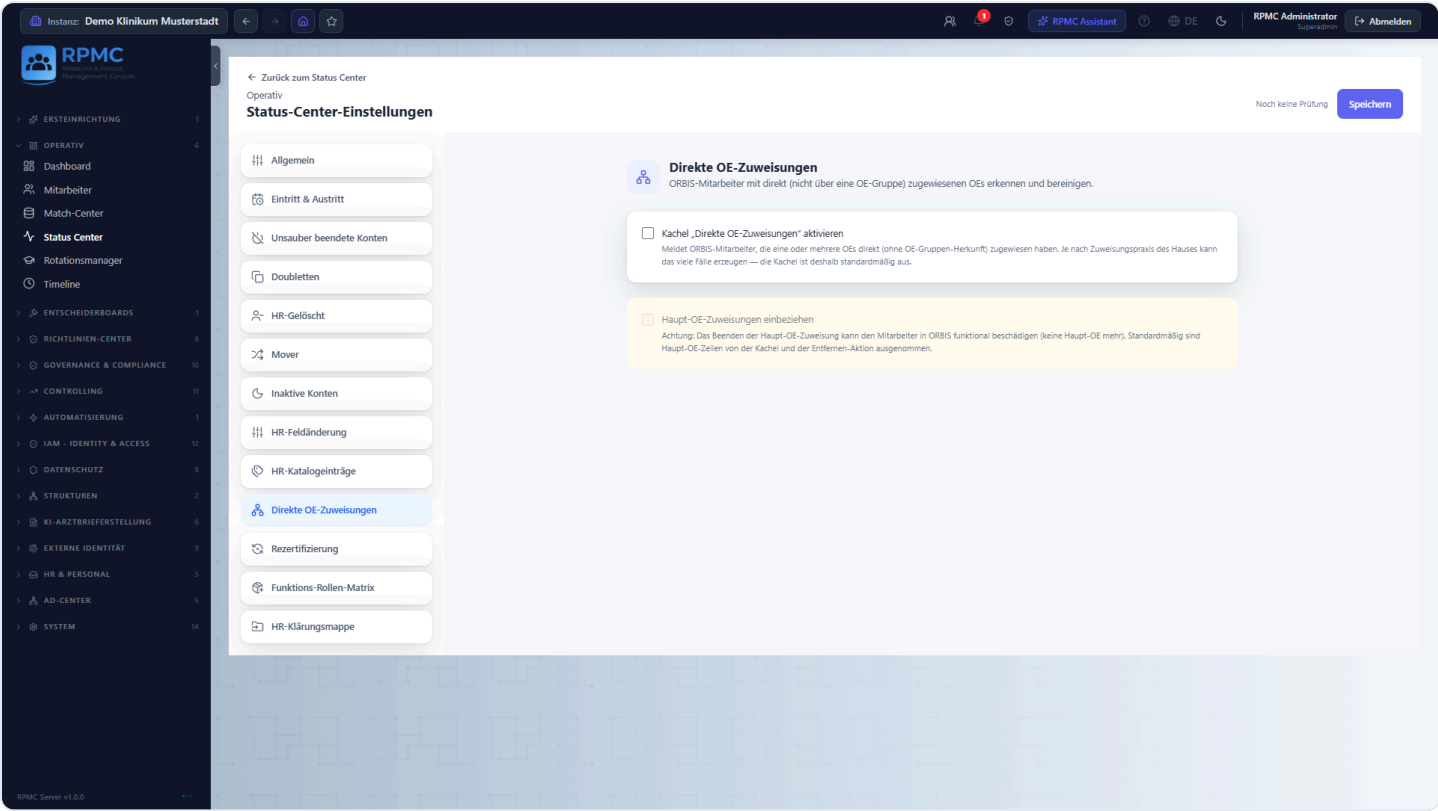
Kachelübersicht — Prüf-Kacheln für Eintritte, Austritte, Doubletten, verwaiste und unvollständige ORBIS-Konten, Abteilungswechsler (Mover), Anomalien, HR-Feldänderungen u. a.; Kacheln sind je Haus zuschaltbar. Im Demo-Bestand melden die Kacheln 3 Doubletten, 3 direkte OE-Zuweisungen und 2 Anomalien — darunter öffnet sich direkt die Fallliste mit den offenen Fällen.

Jede Kachel beantwortet eine Frage, die sonst niemand systematisch stellt: Wer ist laut HR eingetreten, hat aber noch kein ORBIS-Konto? Wessen AD-Konto lebt weiter, obwohl der Austritt längst vollzogen ist? Wo weicht die ORBIS-OE von der HR-Stammabteilung ab? Welche HR-Felder haben sich seit gestern geändert? Ein Klick öffnet die Fall-Liste mit Massen-Aktionen: bestätigen, Offboarding auslösen, an HR-Klärung übergeben, Notiz anheften.

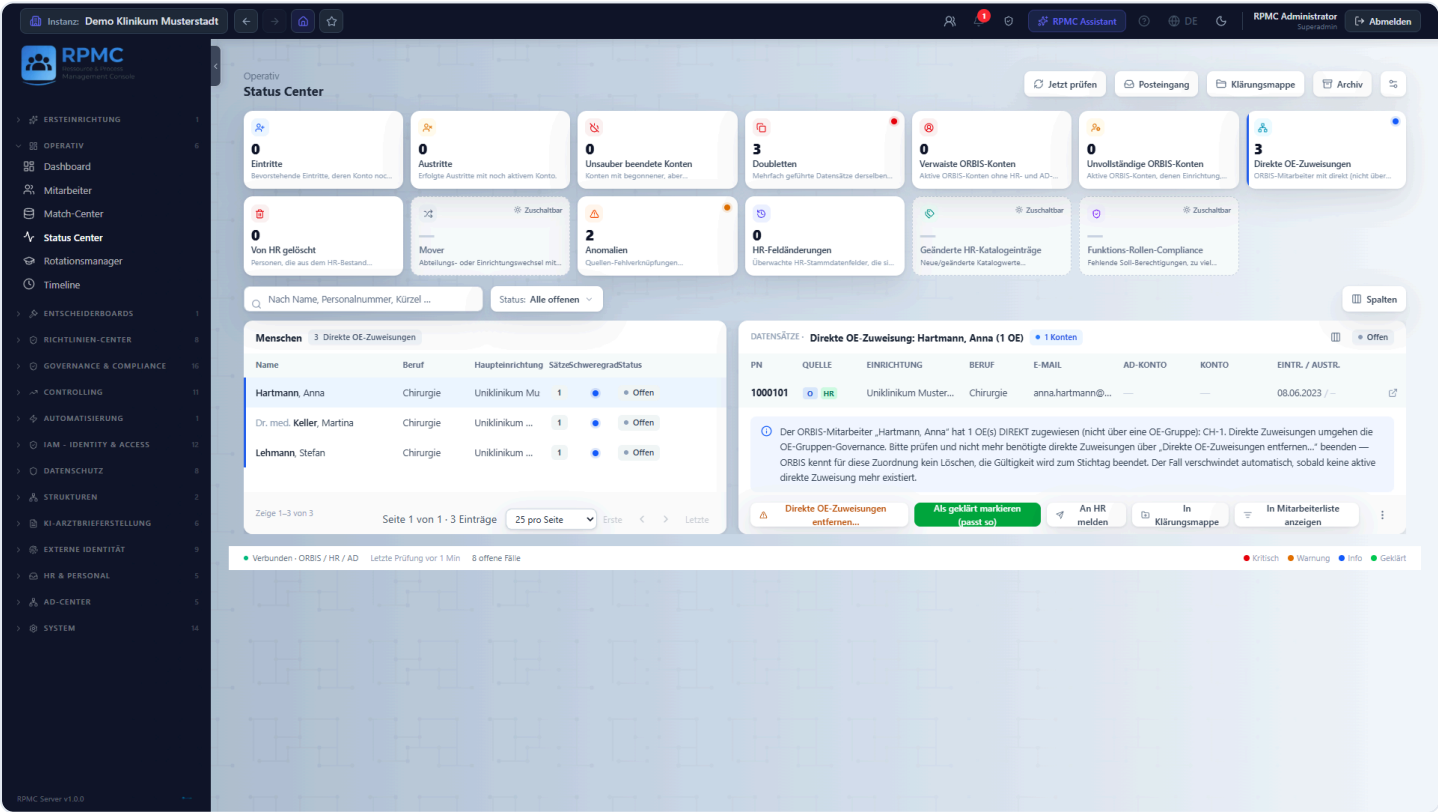
FALLBEISPIEL

Montagsmorgen zeigt die Kachel „Austritte“ drei Fälle: Mitarbeiter, die laut HR ausgeschieden sind, deren ORBIS-Rollen aber noch aktiv sind. Der Administrator öffnet die Fälle, löst direkt aus der Liste die Offboarding-Kette aus — Rollen entzogen, AD deaktiviert, Vorgesetzten-Mail versendet, Fall geschlossen. Zeitaufwand: zwei Minuten. Ohne Status Center wären diese Konten typischerweise erst beim nächsten Audit aufgefallen — als Befund.

6.2 Neu: Kachel „Direkte OE-Zuweisungen“



Einstellungen · Direkte OE-Zuweisungen — die optionale Kachel erkennt Mitarbeiter, die OEs direkt (statt über OE-Gruppen) zugewiesen bekamen, und entfernt sie kontrolliert über Gültigkeits-Beendigung — mit Vorschau, Bestätigung, Audit und Schutz der Haupt-OE.

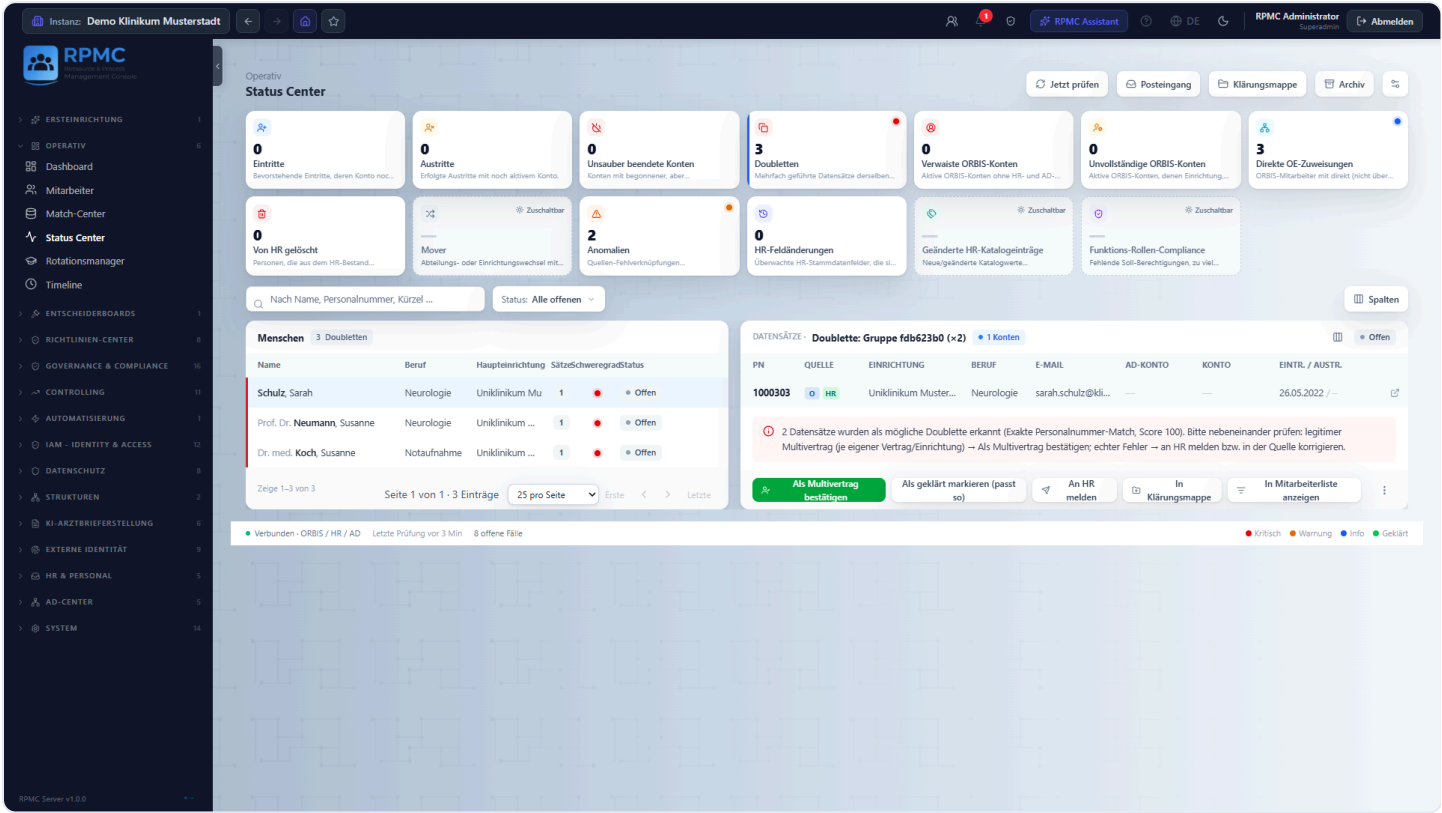


Kachel-Detail „Direkte OE-Zuweisungen“ — drei erkannte Fälle; der geöffnete Fall zeigt das Datensatz-Panel mit der direkt zugewiesenen OE, einen Governance-Hinweis und die Aktion „Direkte OE-Zuweisungen entfernen...“ — Bereinigung mit einem Klick, aber nie ohne Bestätigung und Audit.

Direkte OE-Zuweisungen am Gruppenmodell vorbei sind ein klassisches Governance-Leck: schwer zu finden, nie rezertifiziert. Die neue Kachel spürt sie systematisch auf und bietet die kontrollierte Bereinigung an — die Haupt-OE bleibt dabei grundsätzlich geschützt.

6.3 HR-Klärungsmappe: der geordnete Draht zur Personalabteilung

Nicht jede Auffälligkeit kann die IT selbst entscheiden. Unklare Fälle — widersprüchliche Stammdaten, fragliche Austritte, Doubletten mit HR-Bezug — wandern per Klick in die **HR-Klärungsmappe**: einen Posteingang für die Personalabteilung mit eigenem Status-Workflow (offen → in Klärung → beantwortet → erledigt). HR arbeitet die Mappe in ihrem eigenen Bereich ab; die Antwort fließt dokumentiert zurück in den Fall. Schluss mit Zuruf-Klärungen per Telefon und verlorenen Mail-Threads (Details und Screenshot in Kapitel 21).



Kachel-Detail „Doubletten“ — drei offene Fälle; der geöffnete Fall zeigt die Doubletten-Gruppe (exakter Personalnummer-Match, Score 100) mit den Aktionen „Als Multivertrag bestätigen“, „Als geklärt markieren“, „An HR melden“ und „In Klärungsmappe“: Erkennung und Behebung in einer Ansicht.

FUNKTIONSPROFIL

Cross-Source-Erkennung verbindet ORBIS, Active Directory, HR und Dienstplan mit fallbezogenen Klärungsaktionen und einem HR-Klärungsworkflow.

Mehrsprachigkeit (DE/EN/FR/IT) RELEASED

RPMC ist von Grund auf viersprachig: Deutsch, Englisch, Französisch und Italienisch — vollständig, nicht nur die Startseite.

Über **20.000 Oberflächen-Texte je Sprache** decken jede Seite, jeden Dialog, jede Fehlermeldung und jede Mail-Vorlage ab. Die Sprache wird pro Benutzer gewählt; ein Schweizer Verbund kann also Deutsch, Französisch und Italienisch parallel im selben System betreiben, ohne dass ein einziger Anwender auf eine Fremdsprache ausweichen muss. Korrekte Umlaute und typografische Sonderzeichen (ä/ö/ü/ß, Accents) sind durchgängig gewährleistet — auch in Exporten, PDFs und Mails.

NUTZEN

Für Häuser in der Schweiz, in Österreich und Südtirol sowie für internationales Personal entfällt die Sprachbarriere als Einführungs-Hürde. Schulungsaufwand sinkt messbar, wenn jeder Anwender in seiner Arbeitssprache bedient — und die KI-Funktionen (Kapitel 23) antworten ebenfalls in der Sprache des Anwenders.

Rotationsmanager

RELEASED

Assistenzärzte rotieren durch Fachabteilungen, Pflegekräfte wechseln zwischen Stationen, Bereitschaften folgen Wochenplänen — der Rotationsmanager macht diese Bewegungen planbar und verbindet sie mit dem Berechtigungs-Lebenszyklus.

Rotations- und Einsatzpläne werden je Mitarbeiter oder je Bereich gepflegt: Zeiträume, Ziel-Abteilungen, Funktionen. RPMC kennt damit nicht nur den Ist-Zustand, sondern die **geplante Zukunft** jedes Mitarbeiters — und genau daraus entsteht der Mehrwert:

- **Rechtzeitige Rechte-Vorbereitung:** Der anstehende Wechsel in die Chirurgie ist sichtbar, bevor er passiert — die Zielrechte können vorab geprüft und zum Stichtag automatisch aktiviert werden (JML-Automatik, Kapitel 11).
- **Grace Period statt hartem Schnitt:** Die Rechte der alten Abteilung laufen kontrolliert über eine Übergangsfrist aus, statt am Wechseltag Arbeitsunterbrechungen zu erzeugen.
- **Transparenz für den Mitarbeiter:** Jeder sieht seinen eigenen Rotationsplan im MyIdentity-Portal (Kapitel 15) — keine Nachfragen bei der Personalabteilung.
- **Kalender-Integration:** Rotationen erscheinen im Kalender-Reiter des Mitarbeiter-Dossiers neben Abwesenheiten und Einsätzen.

FALLBEISPIEL

Ein Assistenzarzt rotiert zum Quartalswechsel von der Inneren in die Notaufnahme. Der Rotationsmanager kennt den Termin seit Monaten; zwei Wochen vorher erzeugt RPMC den Mover-Fall mit vorgeschlagenem Ziel-SET, die alte Berechtigung erhält eine 14-tägige Grace Period. Am Stichtag arbeitet der Arzt ohne einen einzigen Anruf bei der IT — und der Datenschutz sieht im Audit, dass die alten Rechte fristgerecht ausliefen.

Timeline & Aktivitätshistorie

RELEASED

Wer hat wann was geändert — und wie kam dieser Mitarbeiter zu diesem Rechte-Stand? Die Timeline beantwortet die Frage, an der Audits sonst scheitern: über alle Quellen, chronologisch, lückenlos.

Jeder Mitarbeiter besitzt eine **Cross-Source-Timeline**: Eintritt, Funktions- und Abteilungswechsel, Rollen-Zuweisungen und -Entzüge, ORBIS-Sync-Ereignisse, Konto-Operationen und Austritt — in einer Zeitleiste, gespeist aus ORBIS, AD, HR und RPMC selbst. Ergänzend führt die **Unified Audit Timeline** (Kapitel 12) die Ereignisse beider Welten — ORBIS-Änderungshistorie und RPMC-Audit-Kette — in einem gemeinsamen Strom zusammen, filterbar nach Quelle, Akteur und Zeitraum.

- **„Geändert durch“-Attribution:** Auch für Änderungen, die in ORBIS selbst vorgenommen wurden, rekonstruiert RPMC den Verursacher aus der ORBIS-Objekt-Historie — Änderungen bleiben Personen zuordenbar.
- Gezielte Abfrage: Rollen- und Änderungshistorien lassen sich je Mitarbeiter filtern und exportieren.
- Nachvollziehbar: Die RPMC-Anteile der Timeline stammen aus einer HMAC-verketteten Append-only-Auditspur.

NUTZEN

Die Timeline unterstützt die strukturierte Aufbereitung von Rechtehistorien. Umfang und Aussagekraft hängen von den angebundenen Quellen und der Datenqualität ab.

Entscheiderboard — Gremien & OE-Anträge RELEASED

Krankenhäuser entscheiden in Kommissionen: OE-Reorganisationen, Betten-Umwidmungen, Berechtigungs-Grundsatzfragen. Das Entscheiderboard bringt diese Gremienarbeit aus Mail-Verteilern und Sitzungsprotokollen in einen revisionssicheren, digitalen Prozess.

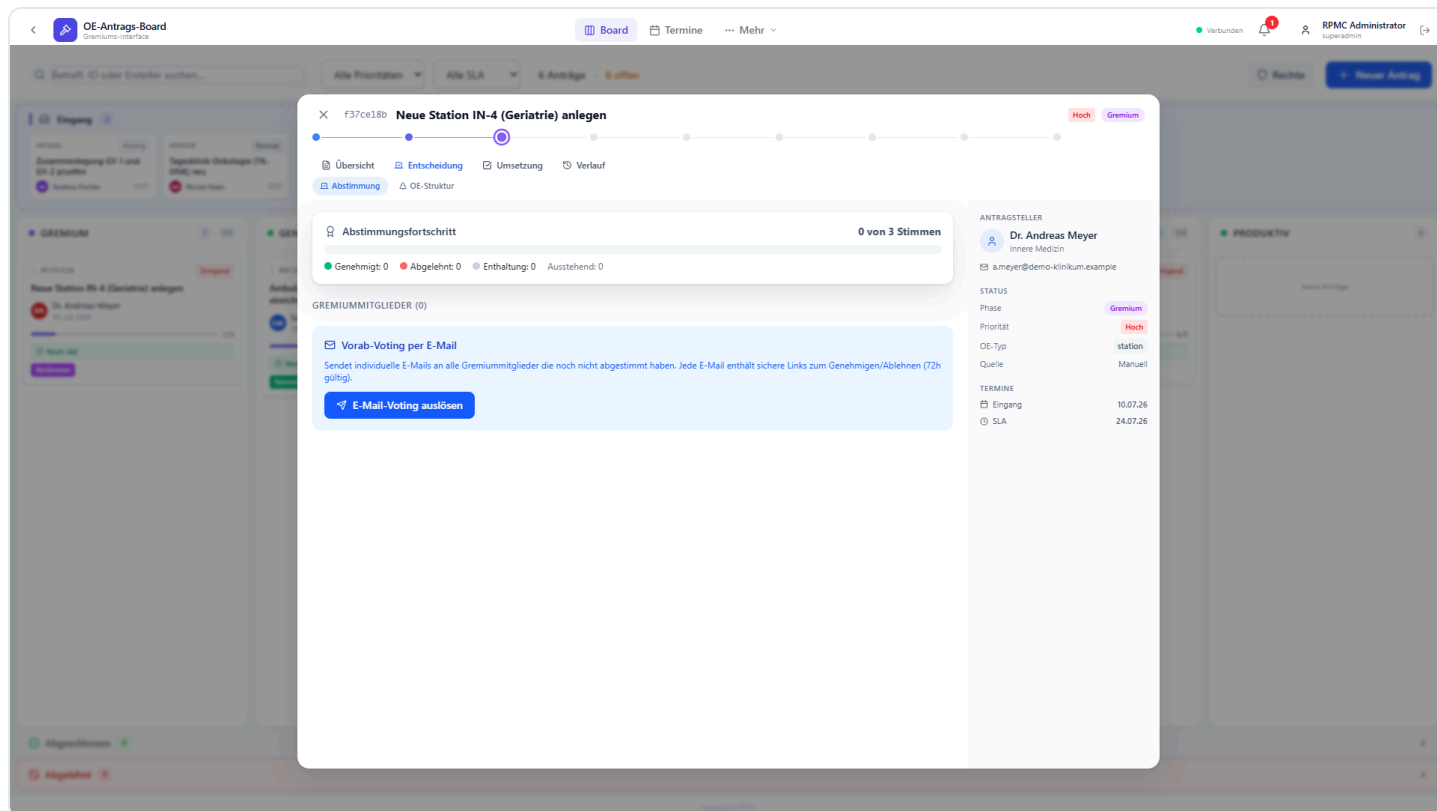
10.1 Kanban für Gremien

Jedes Gremium erhält ein eigenes Board mit konfigurierbaren Spalten (z. B. Eingegangen → Agenda → Abstimmung → Genehmigt → In Umsetzung → Test → Produktiv), WIP-Limits und SLA-Fristen je Spalte. Die Governance-Mechanik ist eingebaut, nicht angeflanscht:

- **Vier-Augen-Prinzip** pro Status-Übergang: kritische Spaltenwechsel verlangen eine zweite Zustimmung.
- **Quorum-Abstimmung** mit konfigurierbarer Mindest-Stimmenzahl — Beschlüsse sind erst mit erreichtem Quorum gültig.
- **E-Mail-Voting mit Tracking-Code:** Gremienmitglieder ohne RPMC-Konto stimmen per Antwort-Mail ab; die Stimme wird dem Vorgang revisionssicher zugeordnet.
- **Teams-Einladungen und SignalR-Live-Updates:** Kartenbewegungen erscheinen bei allen Beteiligten sofort, ohne Neuladen.
- **ITSM- und Audit-Anbindung:** jeder Beschluss, jede Bewegung, jede Stimme landet in der Audit-Kette; optional wird das Ticketsystem synchron gehalten.

The screenshot displays the 'OE-Antrags-Board' interface, a Kanban-style workflow management tool. At the top, there's a navigation bar with 'Board', 'Termine', and 'Mehr' options. A search bar is present, along with filters for 'Alle Prioritäten' and 'Alle SLA'. The main area is divided into seven columns representing different stages of the process: 'Eingang' (2 items), 'GREMIUM' (1/5), 'GENEHMIGT' (1), 'STAMMDATEN' (0/3), 'UMSETZUNG' (1/3), 'TEST' (1/2), and 'PRODUKTIV' (0). Each column contains cards representing requests, with details like priority (e.g., 'Dringend', 'Normal'), assignee, and progress bars. The bottom of the interface shows a status bar with 'Abgeschlossen' and 'Abgelehnt' indicators.

OE-Antrags-Board (Kanban) — sechs Anträge über die Spalten Eingang, Gremium, Genehmigt, Stammdaten, Umsetzung, Test und Produktiv — mit Prioritäts-Badges, SLA-Countdown und Fortschrittsbalken je Karte. Der Bereich umfasst zudem Konfiguration, Rollen & Mitglieder, ITSM-Kopplung und Audit-Trail.



Antragskarte im Detail — „Neue Station IN-4 (Geriatric) anlegen“: Phasen-Stepper, Reiter für Übersicht, Entscheidung, Umsetzung, Verlauf, Abstimmung und OE-Struktur, Abstimmungsfortschritt mit Vorab-Voting per E-Mail sowie Antragsteller- und Status-Panel.

10.2 Das OE-Entscheidungsboard: Anträge auf der echten Struktur

Das Besondere am OE-Board: Anträge sind keine Freitext-Tickets, sondern **strukturierte Änderungsanträge auf der echten OE-Struktur des Hauses**. Der Antragsteller öffnet einen geführten Editor, der auf dem Live-OE-Baum arbeitet (Kapitel 17): Er verschiebt, teilt oder benennt Organisationseinheiten direkt am realen Modell — der Antrag *ist* die gewünschte Zielstruktur, nicht deren Prosa-Beschreibung.

1 Antrag im Editor Antragsteller modelliert die Änderung am echten OE-Baum — geführter Modus, keine Vorkenntnisse nötig	2 Gremienlauf Kanban-Weg mit Agenda, Quorum-Abstimmung und Vier-Augen-Freigabe	3 Umsetzung Beschlossene Struktur wird als Entwurf übernommen, geprüft und produktiv gesetzt	4 Fertige Exporte Die beschlossene OE-Struktur steht sofort als Export (Voll/Diff) für ORBIS-Pflege und Doku bereit
--	---	---	--

FALLBEISPIEL

HNO und Augenklinik sollen zu einem Kopfbereich fusionieren. Die Fachbereichsleitung modelliert den Zusammenschluss im geführten Editor — Stationen, Ambulanzen, Zuordnungen. Der Antrag durchläuft das Gremium mit Quorum; zwei Mitglieder stimmen per E-Mail-Voting aus dem Urlaub ab. Nach der Vier-Augen-Freigabe liegt die neue Struktur als geprüfter Entwurf samt Diff-Export vor — die ORBIS-Pflege arbeitet eine exakte Vorlage ab statt ein Sitzungsprotokoll zu interpretieren.

WAS KLASSISCHE IAM-SYSTEME HIER NICHT KÖNNEN

Gremien-Workflows mit Quorum und Vier-Augen bieten manche Suiten — aber ein Antragsweg, der direkt auf der realen Organisationsstruktur des Krankenhauses modelliert wird und am Ende fertige, importierbare OE-Exporte liefert, ist ein RPMC-Unikat.

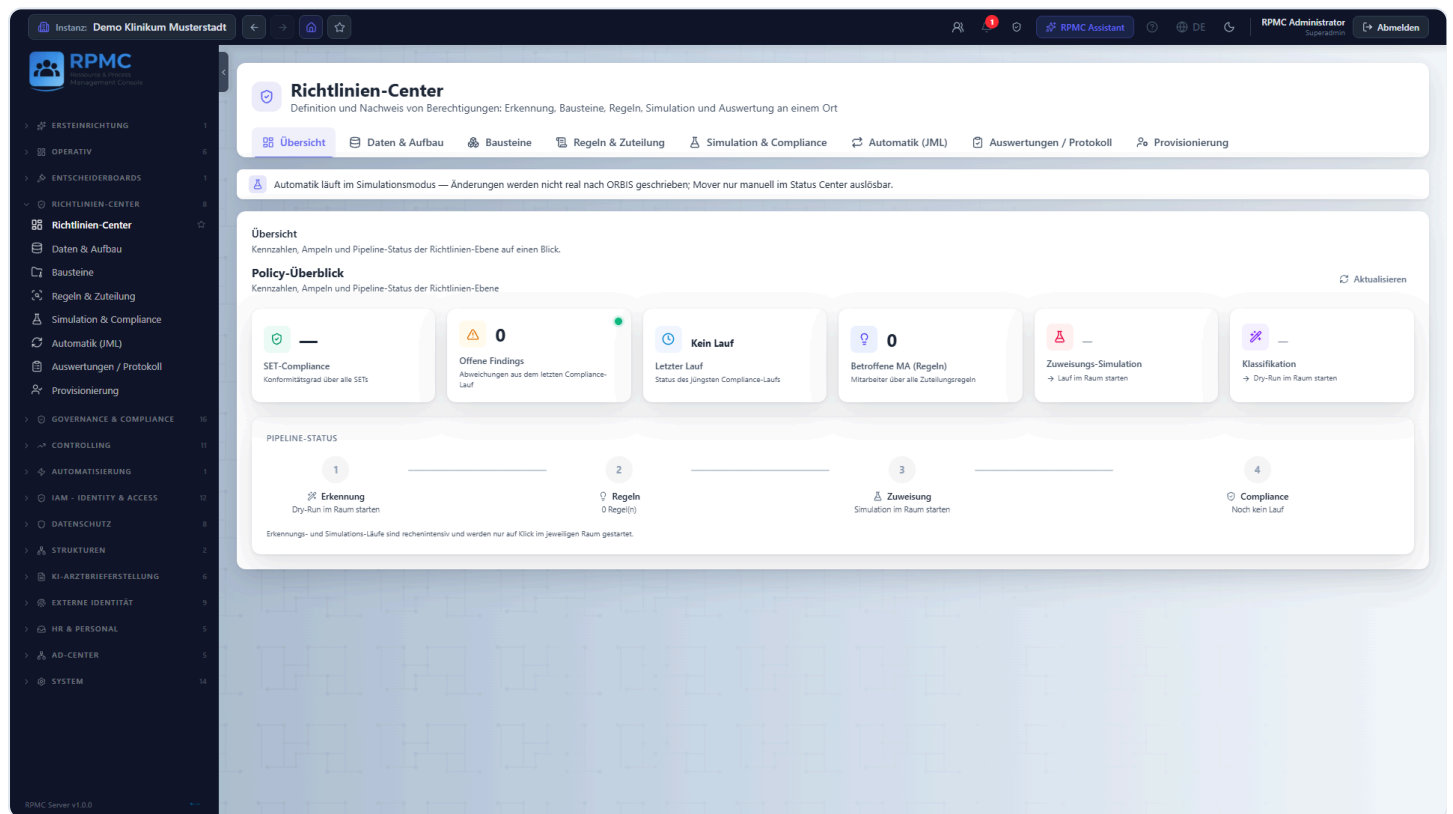
Richtlinien-Center (Policy Center) RELEASED

Wer bekommt was — und warum? Das Richtlinien-Center macht aus gewachsener Berechtigungs-Praxis ein erklärbares Regelwerk: SETs als wiederverwendbare Bausteine, WENN/DANN-Regeln in mehreren Fassungen, eine völlig gefahrlose Simulation und auf Wunsch die Vollautomatik für Eintritt, Wechsel und Austritt.

11.1 Das Problem: schwierige HR-Datensätze

Die Theorie sagt: „Funktion + Abteilung = Rechteprofil.“ Die Praxis sagt: Chefarzt-Sekretariat mit Sonderrechten, geteilte Stellen über zwei Fachabteilungen, Honorarkräfte, Hebammen mit Belegvertrag, MFA in Teilzeit auf drei Stationen. HR-Datensätze sind unscharf, historisch gewachsen und widersprüchlich — genau daran scheitern starre Rollenkonzepte klassischer IAM-Systeme.

RPMC geht den umgekehrten Weg: Das Richtlinien-Center analysiert zunächst den **Ist-Zustand** — welche Berechtigungs-Muster existieren tatsächlich? Die **KI-gestützte Analyse** gruppiert vergleichbare Mitarbeiter (gleiche Funktion, gleiche OE), erkennt die real gelebten Standard-Bündel und schlägt daraus SETs und Zuteilungsregeln vor. Statt monatelanger Rollen-Workshops: ein datengetriebener Startpunkt in Tagen — und die schwierigen Datensätze werden als Ausnahmen sichtbar, statt das ganze Konzept zu sprengen.



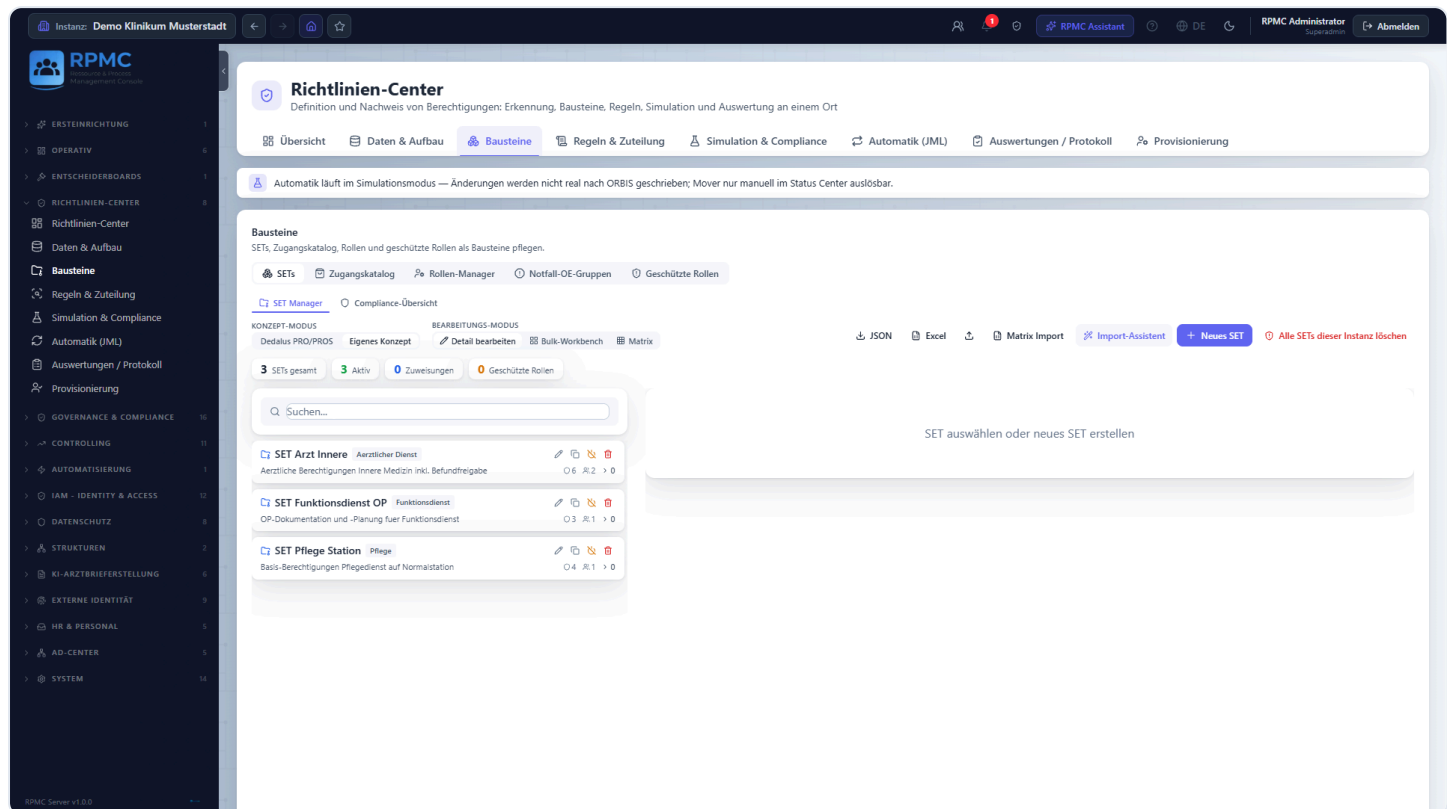
Richtlinien-Center — die Räume „Daten & Aufbau“, „Bausteine“, „Regeln & Zuteilung“, „Simulation & Compliance“, „Automatik (JML)“, „Auswertungen“ und „Provisionierung“ mit Policy-KPIs und vierstufigem Pipeline-Status: vom Datenfundament bis zur Automatik ein geführter Weg.

11.2 SETs — Berechtigungs-Bündel als Norm

Ein SET bündelt alles, was eine Funktion an Ausstattung braucht: ORBIS-Rollen, OE-Gruppen, Einrichtungen, Funktions- und Status-Vorgaben. SETs werden einmal definiert und überall angewendet — im SET-Manager, in der Massen-Administration, im Self-Service-Katalog, in der JML-Automatik. Und: SETs sind die **Norm**, gegen die RPMC Abweichungen misst — wer mehr hat als sein SET, fällt auf (Kapitel 15.3).

- **Aufbau & Editor:** SETs werden visuell zusammengestellt; die Wirkung (effektive Rechte) ist vor dem Speichern sichtbar.

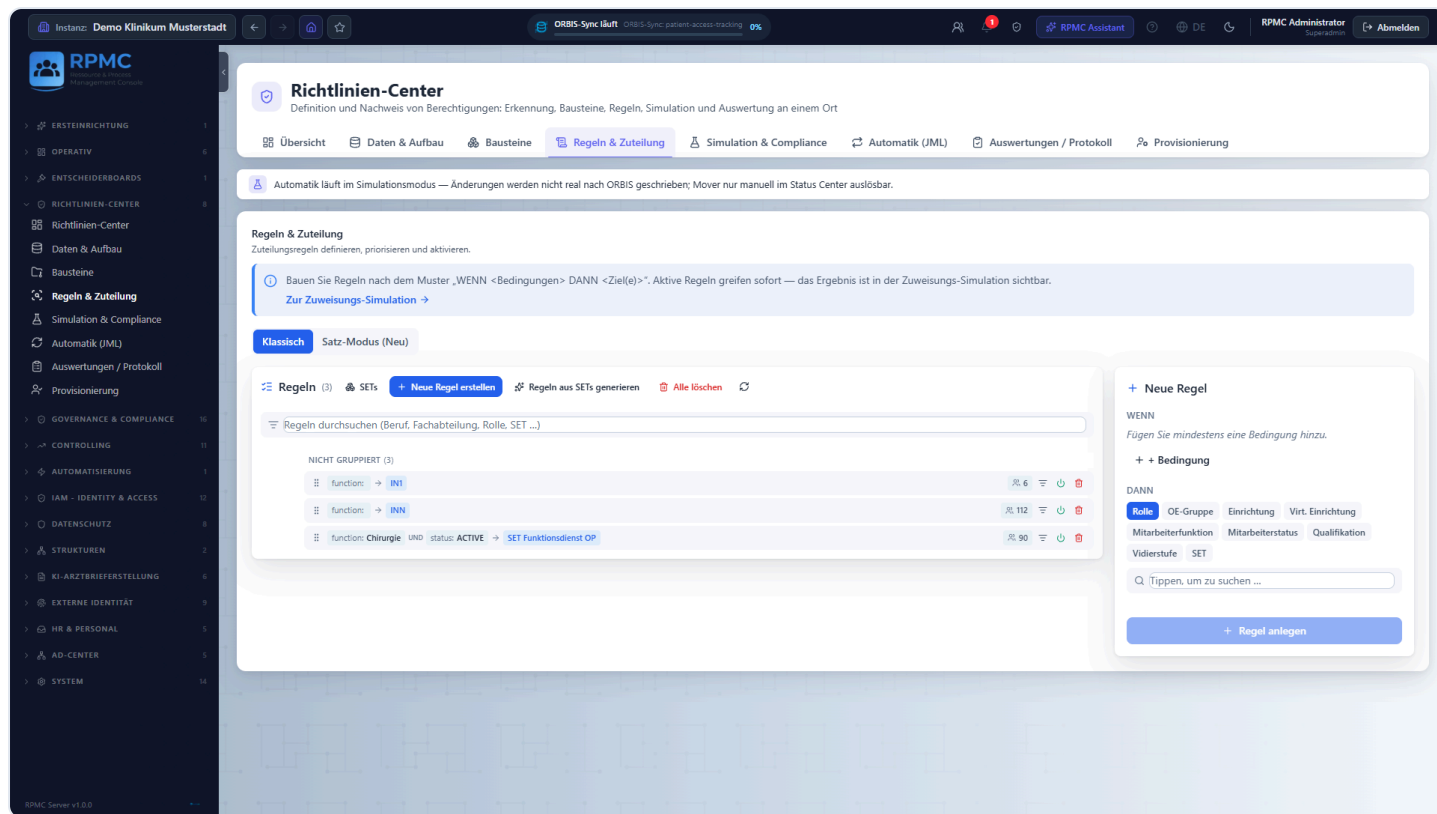
- **Import:** bestehende Konzepte kommen per JSON-, Excel- oder Matrix-Import ins System — auch Dedalus-Konzeptwelten (PRO/PROS) oder ein komplett eigenes Konzept des Hauses werden abgebildet.
- **Kein Zwang:** Ein Mitarbeiter kann jederzeit auch ohne SET nur mit Stammdaten geführt werden — das SET ist Hilfsmittel, kein Pflichtfeld (anders als in manchen Healthcare-Suiten, wo ein Bündel bei der Anlage erzwungen wird).



Raum „Bausteine“ — SET-Manager mit drei aktiven SETs („SET Arzt Innere“ für den Ärztlichen Dienst, „SET Funktionsdienst OP“, „SET Pflege Station“) und Import-Wegen (JSON, Excel, Matrix, Import-Assistent). SETs sind die wiederverwendbaren Bausteine des gesamten Regelwerks — auch Dedalus-Konzeptwelten (PRO/PROS) oder ein eigenes Konzept des Hauses werden abgebildet.

11.3 Regeln & Zuteilung — Fassungen statt Bauchgefühl

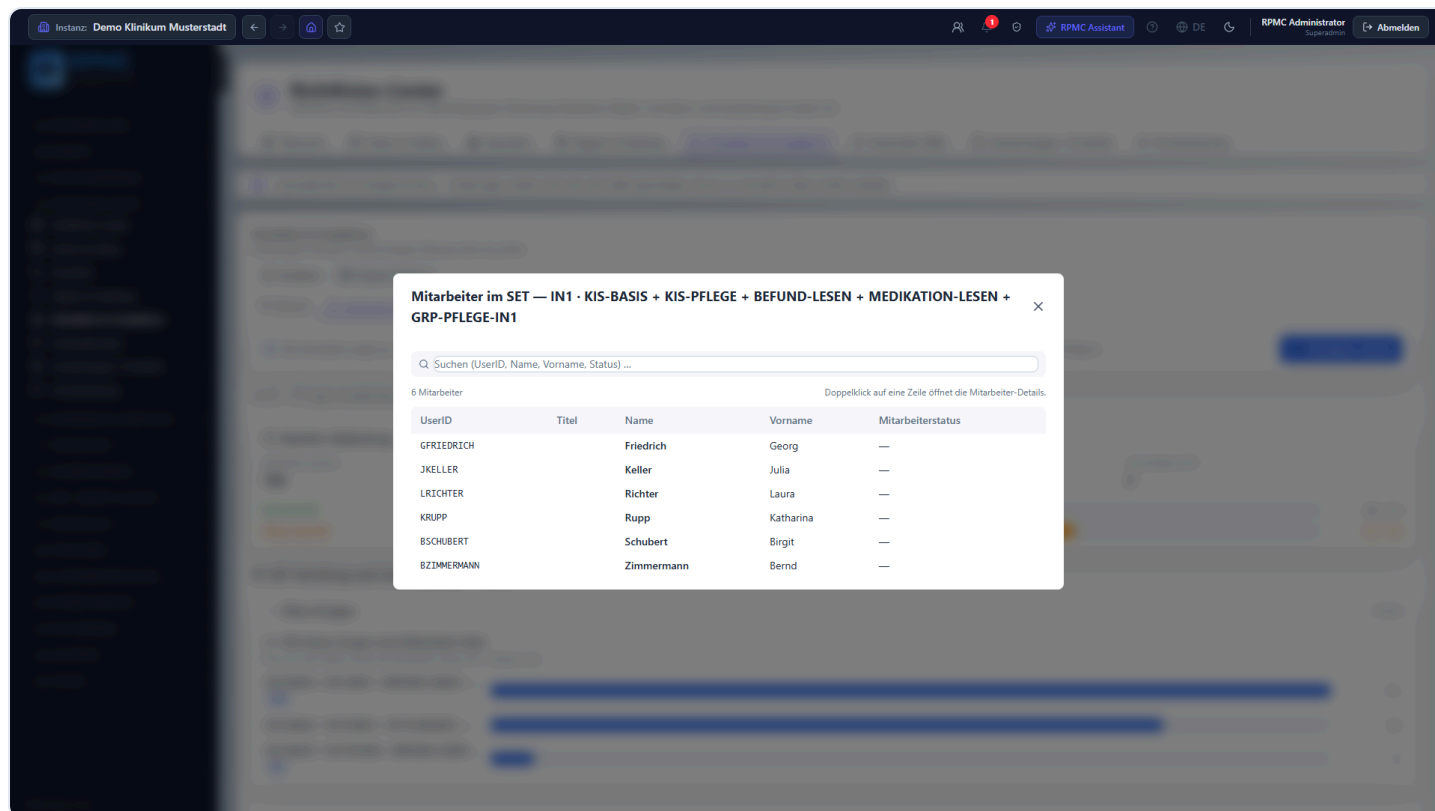
Zuteilungsregeln folgen dem WENN/DANN-Prinzip: *Wenn* Funktion, Einrichtung, Vertragsmerkmal oder ein beliebiges HR-Rohfeld bestimmte Bedingungen erfüllt (kombinierbar mit UND/ODER, Wildcards), *dann* erhält der Mitarbeiter Rolle, OE-Gruppe, Einrichtung oder ein ganzes SET. Das Entscheidende: Regeln existieren in **mehreren Fassungen**. Eine neue Fassung wird entworfen, simuliert und erst nach Prüfung scharf geschaltet — die alte bleibt dokumentiert. Regelwerks-Änderungen werden damit so beherrschbar wie Software-Releases: nachvollziehbar, vergleichbar, rückholbar.



Raum „Regeln & Zuteilung“ — drei aktive Zuteilungsregeln mit Live-Trefferzahlen (6, 112 und 90 Mitarbeiter; u. a. „Funktion Chirurgie UND Status aktiv → SET Funktionsdienst OP“), rechts der WENN/DANN-Regeleditor: Bedingungen, Ziele, Gültigkeit — und sofort sichtbar, wenn die Regel trifft.

11.4 Gefahrlose Simulation: „Was wäre wenn“ — ohne einen einzigen Schreibzugriff

Die größte Angst vor jeder Berechtigungs-Automatik: „Was, wenn die Regel morgen 800 Konten umschreibt?“ Die Antwort des Richtlinien-Centers ist die **Simulation über Zeit**: Das komplette Regelwerk läuft gegen den echten Datenbestand — vorwärts über Tage, Wochen, simulierte Ein- und Austritte — und erzeugt dabei **keinen einzigen ORBIS-Schreibzugriff**. Das Ergebnis ist ein vollständiger Differenz-Bericht: Wer würde was bekommen, wer würde was verlieren, welche Regeln kollidieren, welche Mitarbeiter bleiben unversorgt.



Raum „Simulation & Compliance“ — eine gelaufene Zuweisungs-Simulation: das geöffnete Treffer-Modal zeigt die sechs Mitarbeiter eines SETs namentlich, im Hintergrund Baseline-Abdeckung und SET-Verteilung nach Regel-Gruppen. Alles read-only — das Regelwerk wird gegen Echtdaten geprüft, bevor es live geht.

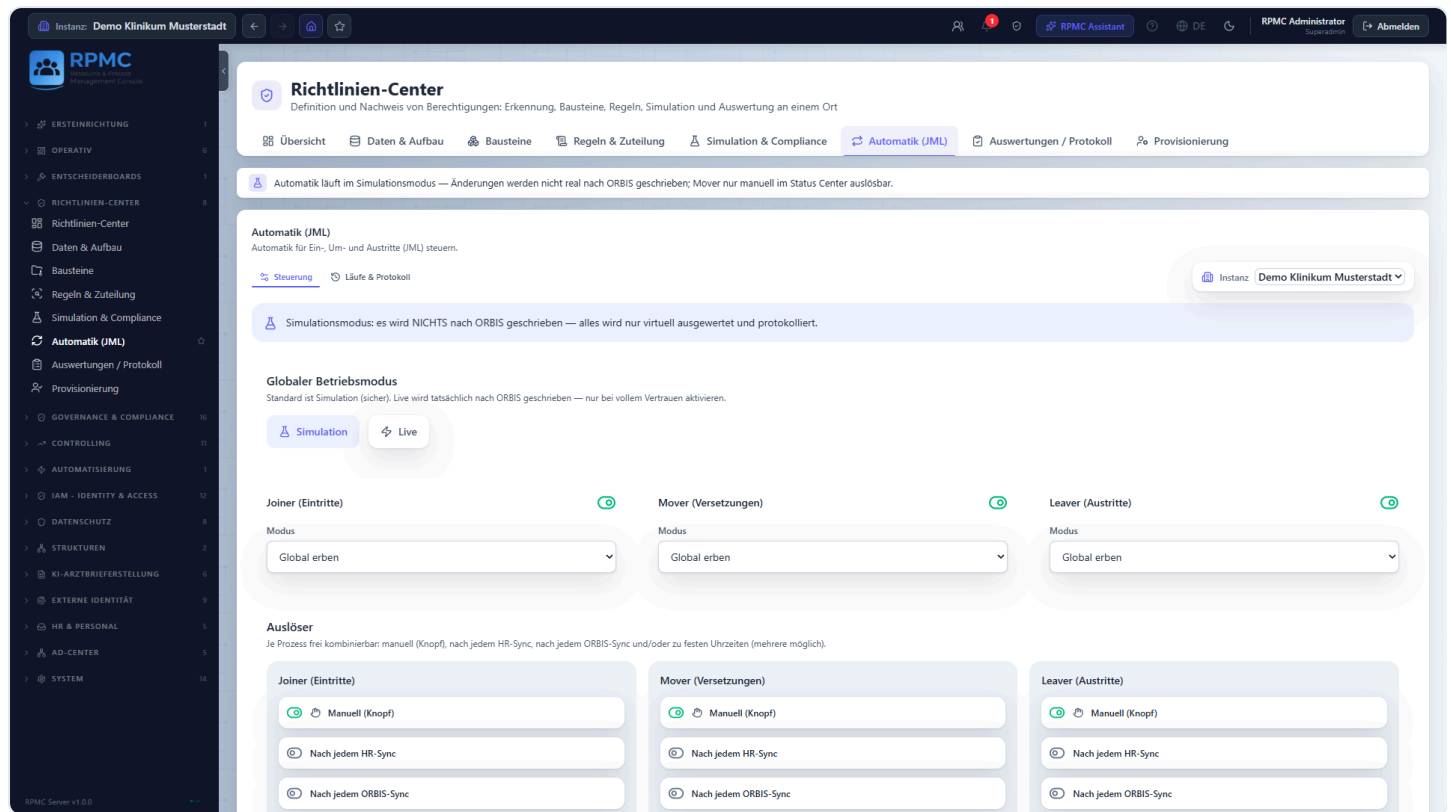
FALLBEISPIEL

Das Haus will die Pflege-Grundrechte neu schneiden. Fassung 2 des Regelwerks wird gebaut und über einen simulierten Monat laufen gelassen — inklusive der 12 Eintritte und 7 Wechsel aus dem echten HR-Bestand. Die Simulation zeigt: 96 % der Pflege wäre korrekt versorgt, 14 Sonderfälle (geteilte Stellen) brauchen eine Zusatzregel. Erst nach deren Ergänzung — und einer zweiten, sauberen Simulation — wird Fassung 2 aktiviert. ORBIS hat von alldem nichts bemerkt.

WAS KLASSISCHE IAM-SYSTEME HIER NICHT KÖNNEN

Regel-Simulationen generischer Suites prüfen meist nur einzelne Policies gegen Einzelpersonen. Eine Zeitraum-Simulation des kompletten Regelwerks gegen den echten Klinik-Bestand — garantiert schreibfrei gegenüber dem KIS — nimmt der Einführung von Berechtigungs-Automatik das Risiko, an dem solche Projekte sonst scheitern.

11.5 JML-Automatik & Grace Period



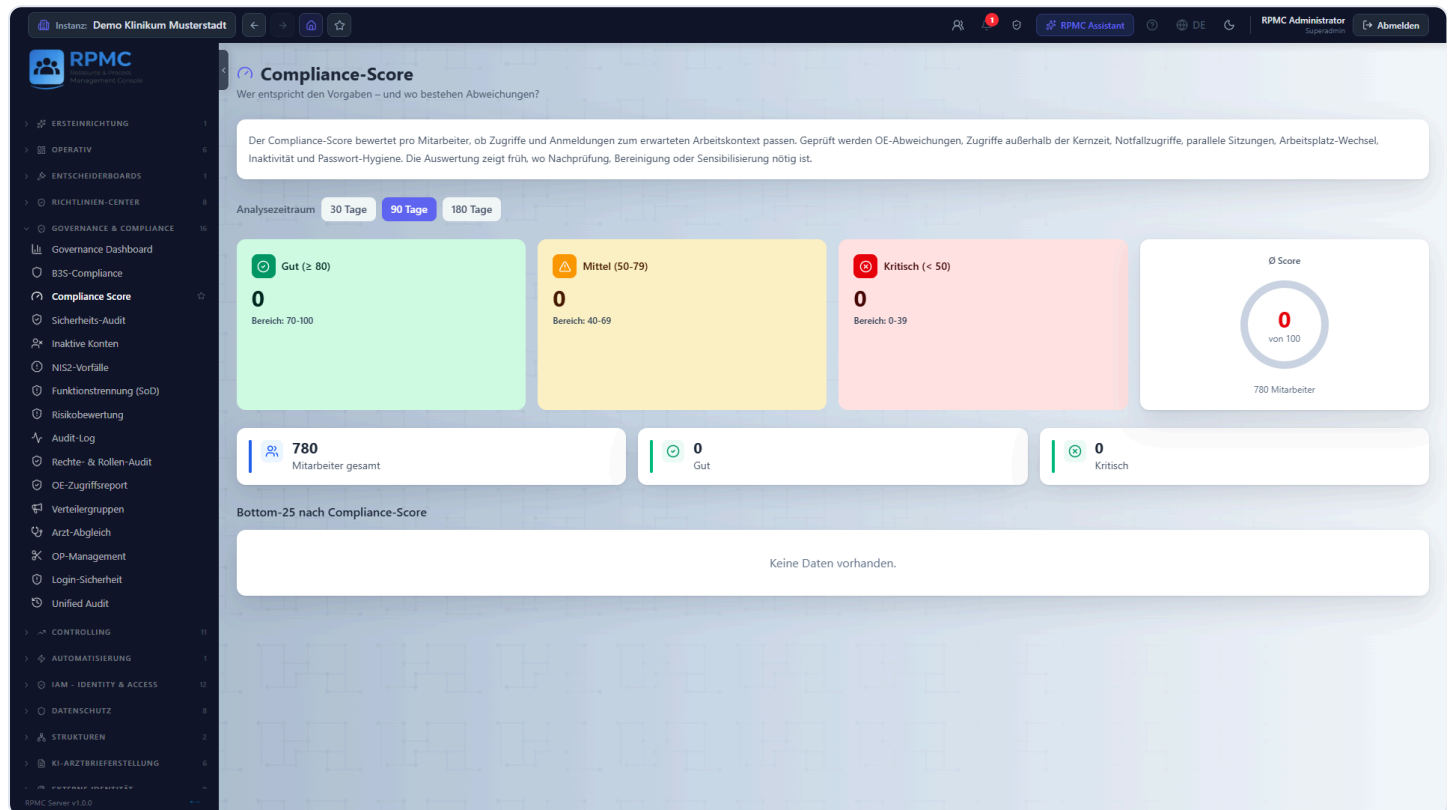
Raum „Automatik (JML)“ — globaler Betriebsmodus Simulation/Live, getrennte Steuerung für Joiner, Mover und Leaver sowie Auslöser (manuell, nach HR-/ORBIS-Sync, feste Uhrzeiten). Jedes Haus wählt sein Tempo — von der reinen Vorschlagsliste bis zur Vollautomatik.

- **Joiner:** Neueintritte aus HR erhalten automatisch ihr SET gemäß Regelwerk — als Vorschlag oder vollautomatisch.
- **Mover:** Abteilungswechsel lösen die Neuberechnung aus; alte Rechte laufen in eine konfigurierbare **Grace Period** (verlängerbar, vorzeitig widerrufbar) statt hart zu enden — keine Arbeitsunterbrechung, keine Dauer-Überberechtigung.
- **Leaver:** Austritte deprovisionieren kontrolliert: Rollen, OE-Gruppen, AD-Konto, Checkliste, Benachrichtigung — jeder Schritt auditiert.
- **Sicherheitsnetz:** Der globale Simulation/Live-Schalter gilt je Prozess; jede Automatik-Aktion ist einzeln nachvollziehbar und im Fehlerfall rücknehmbar.

Governance & Compliance RELEASED

Governance und Compliance bilden eine durchgehende Funktionsebene mit Score-Werten, Berichten, einer HMAC-verketteten Auditspur und fachlichen Auswertungen.

12.1 Compliance-Score: eine Zahl für die Geschäftsführung

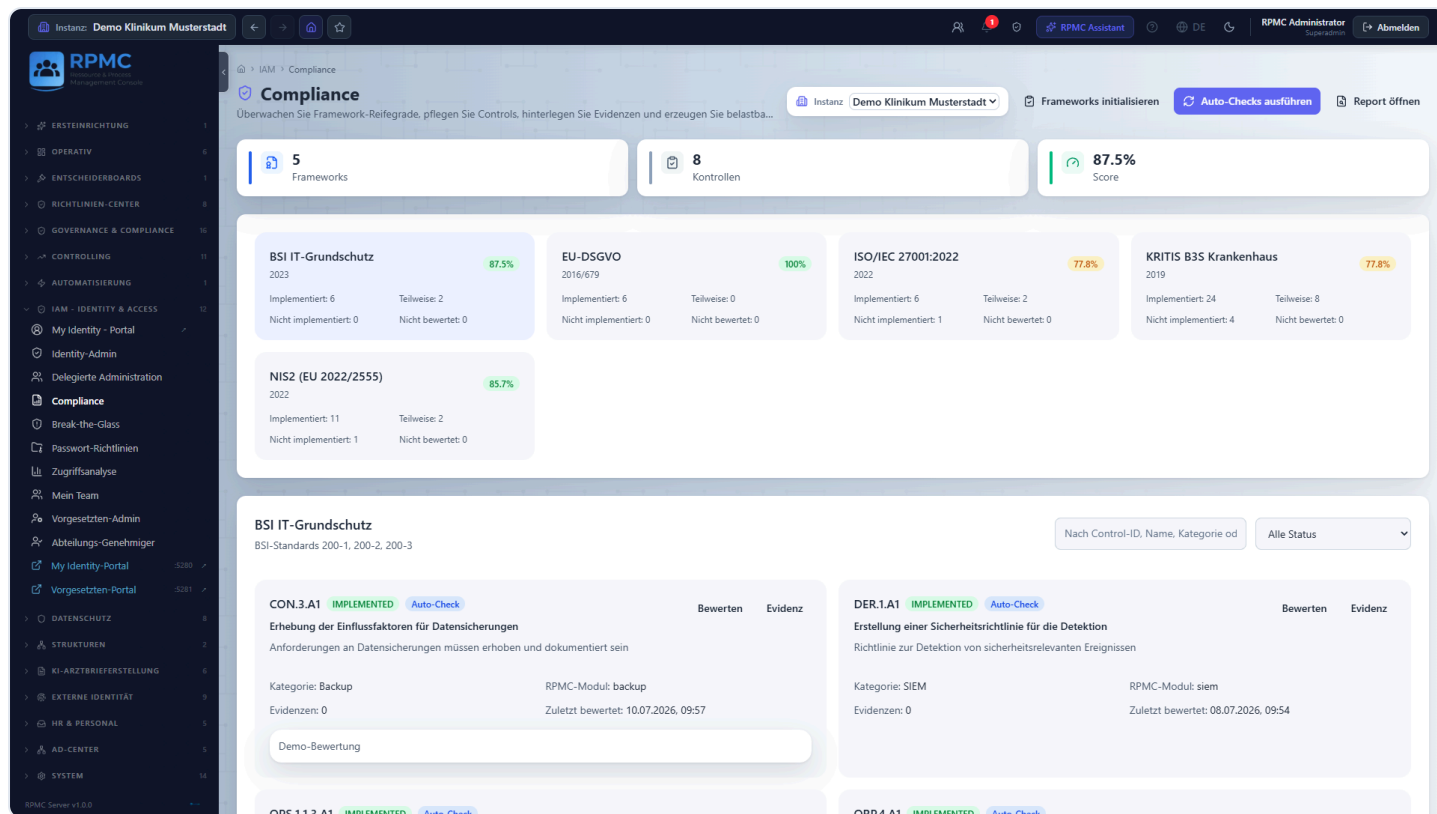


Compliance-Score — Ampel-Kacheln (Gut/Mittel/Kritisch), Durchschnitts-Ring und die Bottom-25-Liste der Mitarbeiter mit dem größten Handlungsbedarf. Der Score verdichtet Rechte-Hygiene, Rezertifizierungs-Stand und Anomalien zu einer steuerbaren Kennzahl.

Jeder Mitarbeiter erhält einen Compliance-Score; das Haus einen aggregierten Wert. Steigt oder fällt er, ist das die früheste Warnlampe vor dem nächsten Audit — und die Bottom-Liste zeigt sofort, *wo* anzusetzen ist. Ergänzend bewertet das **Risk-Scoring** (0–100, sechs gewichtete Faktoren) jeden Mitarbeiter nach Gefährdungspotenzial; Schwellwert-Überschreitungen lösen automatisch Prüf-Fälle aus.

BERICHTE UND EXPORTE

RPMC unterstützt die strukturierte Nachweisführung mit konfigurierbaren Auswertungen und Exporten. Ob diese für eine konkrete gesetzliche, vertragliche oder prüferische Anforderung genügen, ist im jeweiligen Einsatzkontext zu bewerten.



Framework-Compliance — fünf Regelwerke, acht Kontrollen, Gesamt-Score 87,5 %: Framework-Karten mit Reifegrad je Standard (BSI IT-Grundschutz 87,5 %, EU-DSGVO 100 %, ISO/IEC 27001:2022 77,8 %, KRITIS B3S 77,8 %, NIS2 85,7 %) und Kontroll-Liste mit Auto-Check, Bewertung und Evidenz-Ablage. Der Prüfungsstand des Hauses — jederzeit, nicht erst zur Prüfung.

12.2 Rezertifizierung & Rechte-Audit

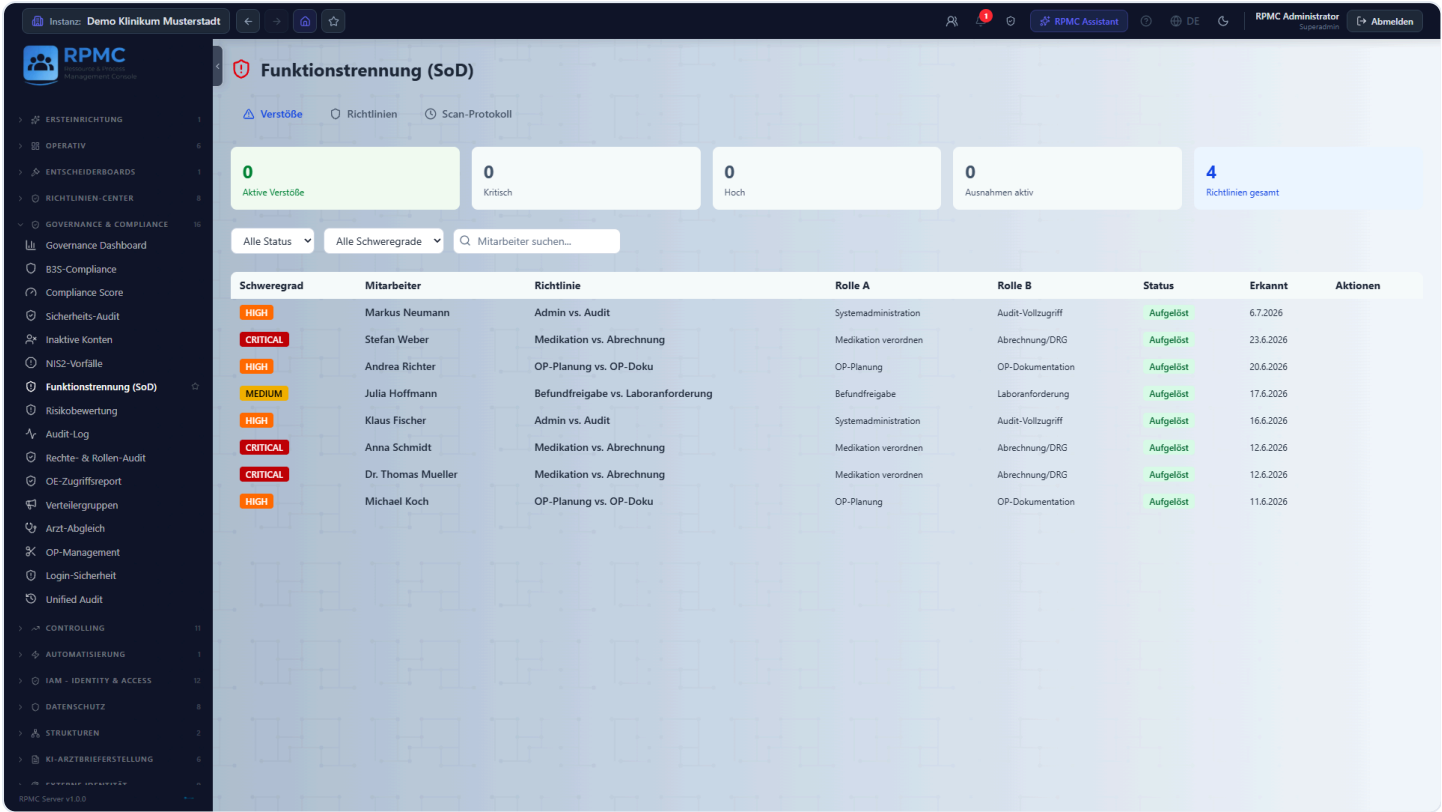
Zeitpunkt	Akteur	Aktion	Objekt	Details
9.7.2026, 18:06:44	demo-seed	role.assign	sync_job - 19	Demo-Audit: role.assign durch system
28.6.2026, 23:41:44	j.hoffmann	role.remove	sync_job - 79	Demo-Audit: role.remove durch j.hoffmann
26.6.2026, 10:57:44	m.schneider	role.assign	status_case - 125	Demo-Audit: role.assign durch m.schneider
26.6.2026, 05:10:44	t.wagner	role.assign	recert_campaign - 192	Demo-Audit: role.assign durch t.wagner
26.6.2026, 05:02:44	admin	role.remove	employee - 102	Demo-Audit: role.remove durch admin
24.6.2026, 02:02:44	t.wagner	role.assign	recert_campaign - 45	Demo-Audit: role.assign durch t.wagner
18.6.2026, 18:04:44	demo-seed	role.remove	role - 186	Demo-Audit: role.remove durch system
15.6.2026, 14:36:44	t.wagner	role.remove	status_case - 47	Demo-Audit: role.remove durch t.wagner
12.6.2026, 00:30:44	admin	role.assign	employee - 103	Demo-Audit: role.assign durch admin
10.6.2026, 22:59:44	t.wagner	role.remove	employee - 135	Demo-Audit: role.remove durch t.wagner
10.6.2026, 22:36:44	m.schneider	role.assign	sync_job - 192	Demo-Audit: role.assign durch m.schneider
9.6.2026, 20:43:44	admin	role.assign	employee - 54	Demo-Audit: role.assign durch admin
6.6.2026, 14:06:44	t.wagner	role.remove	employee - 94	Demo-Audit: role.remove durch t.wagner
31.5.2026, 23:29:44	t.wagner	role.remove	employee - 164	Demo-Audit: role.remove durch t.wagner
28.5.2026, 00:00:44	m.schneider	role.remove	user - 199	Demo-Audit: role.remove durch m.schneider
26.5.2026, 13:59:44	demo-seed	role.assign	user - 92	Demo-Audit: role.assign durch system
26.5.2026, 12:15:44	demo-seed	role.remove	settings - 66	Demo-Audit: role.remove durch system
20.5.2026, 00:26:44	demo-seed	role.remove	recert_campaign - 182	Demo-Audit: role.remove durch system
17.5.2026, 16:26:44	admin	role.assign	recert_campaign - 156	Demo-Audit: role.assign durch admin
15.5.2026, 09:36:44	t.wagner	role.assign	recert_campaign - 105	Demo-Audit: role.assign durch t.wagner
14.5.2026, 05:41:44	demo-seed	role.remove	user - 128	Demo-Audit: role.remove durch system
7.5.2026, 10:45:44	t.wagner	role.assign	settings - 13	Demo-Audit: role.assign durch t.wagner
6.5.2026, 15:04:44	j.hoffmann	role.remove	employee - 66	Demo-Audit: role.remove durch j.hoffmann

Rechte- & Rollen-Audit — chronologisches Protokoll aller Zuweisungen und Entzüge (role.assign / role.remove) mit Akteur, Objekt und Details, inklusive der Einträge laufender Rezertifizierungs-Kampagnen.

Rezertifizierungs-Kampagnen prüfen Berechtigungen periodisch: Scope definieren, Reviewer benachrichtigen, Rückmeldungen einsammeln, nicht bestätigte Rechte nach Frist automatisch entziehen (Auto-Revoke), Audit-Trail abschließen. Die

kontinuierliche Rezertifizierung ergänzt Kampagnen ereignisbasiert: Abteilungswechsel, Reaktivierung, kritische Rollen-Zuweisung oder ein Risk-Score-Sprung lösen sofort eine Mini-Prüfung aus, statt auf den Quartalstermin zu warten.

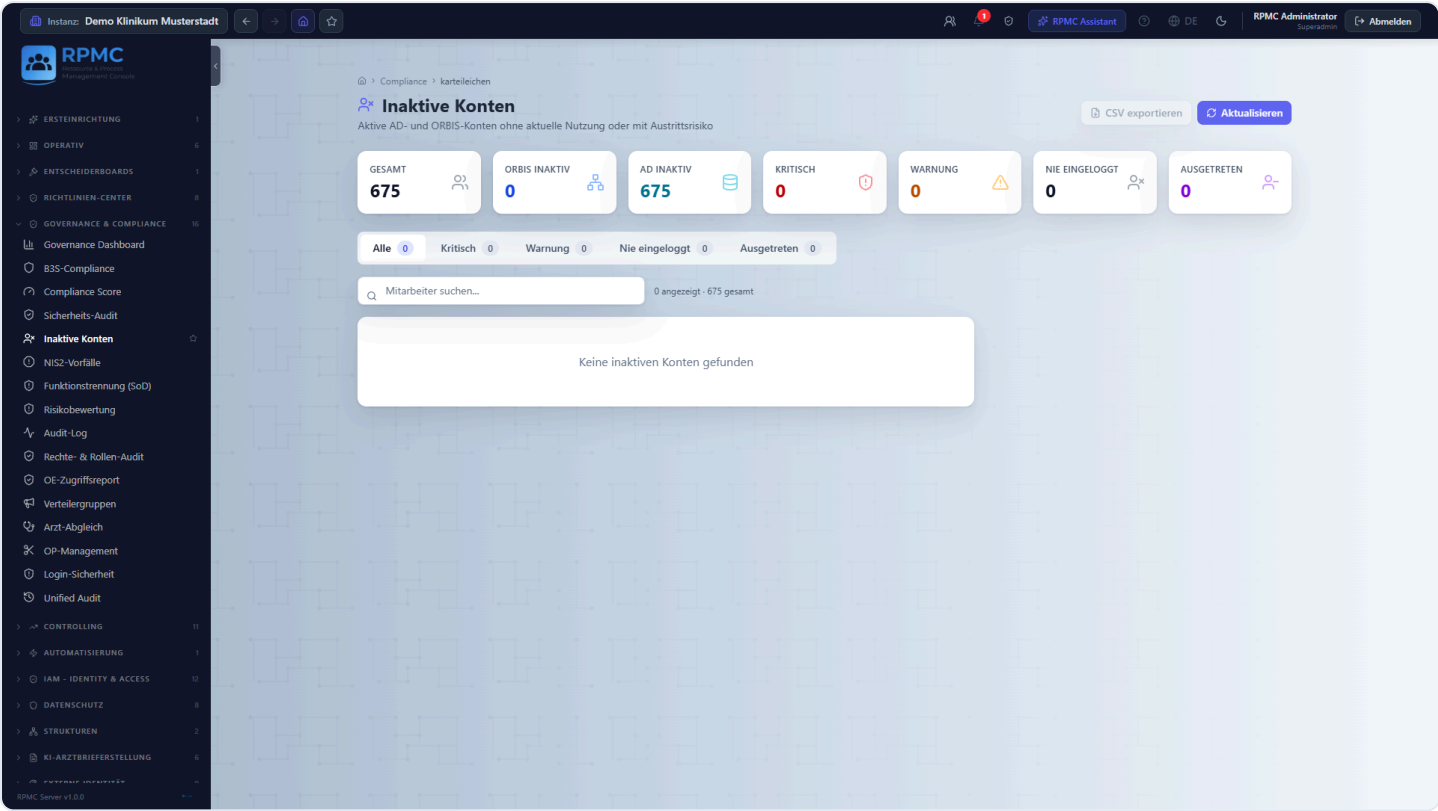
12.3 Funktionstrennung (SoD)



Funktionstrennung (SoD) — Konflikt-Regelwerk mit inkompatiblen Rollenpaaren und Prüfergebnissen je Mitarbeiter. Verstöße werden je nach Policy gewarnt oder blockiert; Ausnahmen laufen über einen begründeten, befristeten Genehmigungs-Workflow.

Inkompatible Rollenpaare (z. B. Anordnung und Freigabe) werden als Policies hinterlegt. Die Engine prüft jede Zuweisung in Echtzeit — WARN oder BLOCK — und überwacht den Bestand. Der Exception-Workflow dokumentiert bewusste, befristete Ausnahmen mit Genehmiger, statt sie im Graubereich zu dulden.

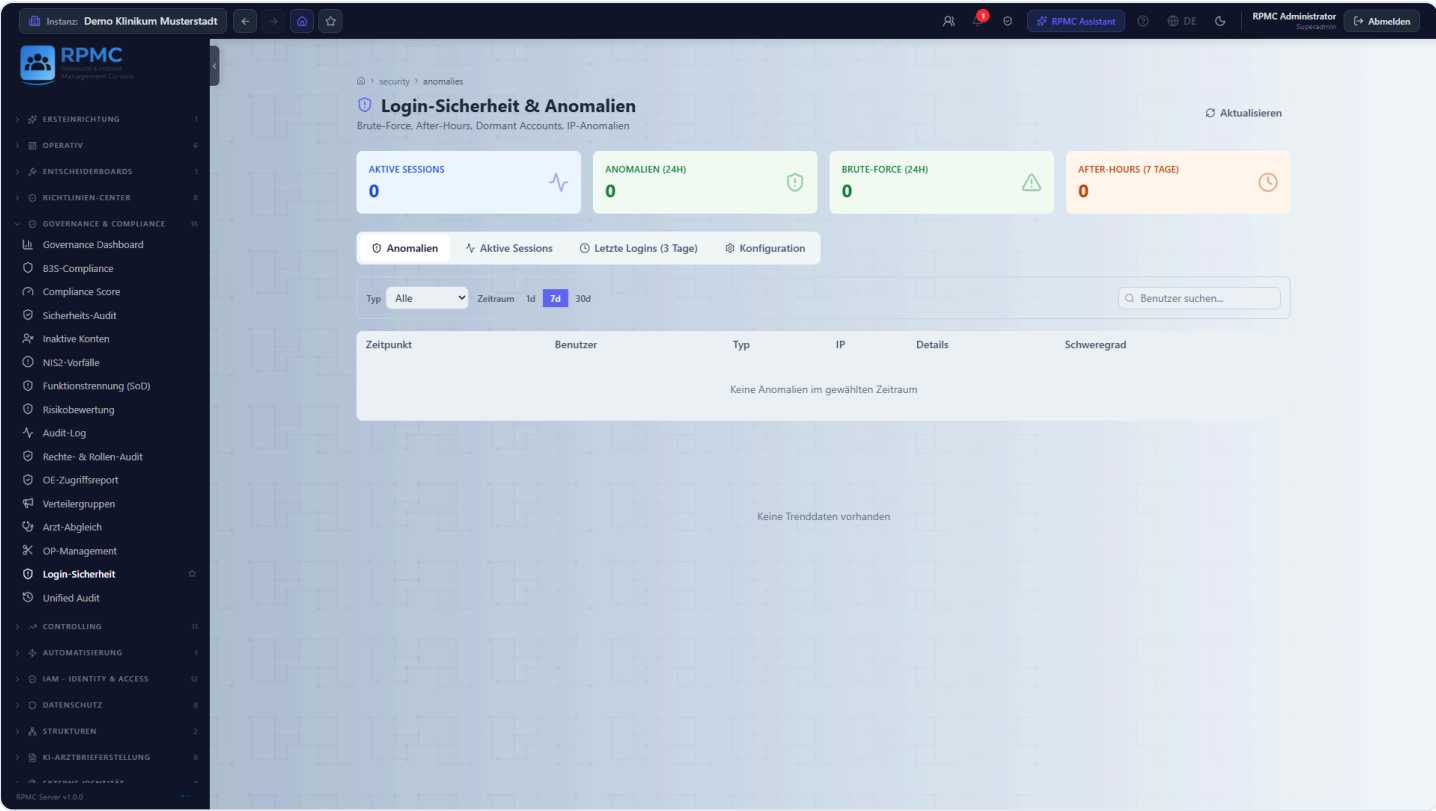
12.4 Inaktive Konten — die Karteileichen-Jagd



Inaktive Konten — aktive ORBIS-Konten ohne Anmeldung im gewählten Zeitraum, mit Recency-Filtern und Austritts-Abgleich. Der Klassiker unter den Audit-Befunden, hier als ständig aktuelle Arbeitsliste.

Aktive Konten ohne Nutzung sind das häufigste Prüfungs-Finding überhaupt. RPMC kombiniert ORBIS-Anmeldedaten, AD-Logins und HR-Austritte zu einer Liste, die kritische Fälle (ausgetreten, aber aktiv) von Warnfällen trennt — mit direktem Absprung in Deaktivierung oder Offboarding-Kette.

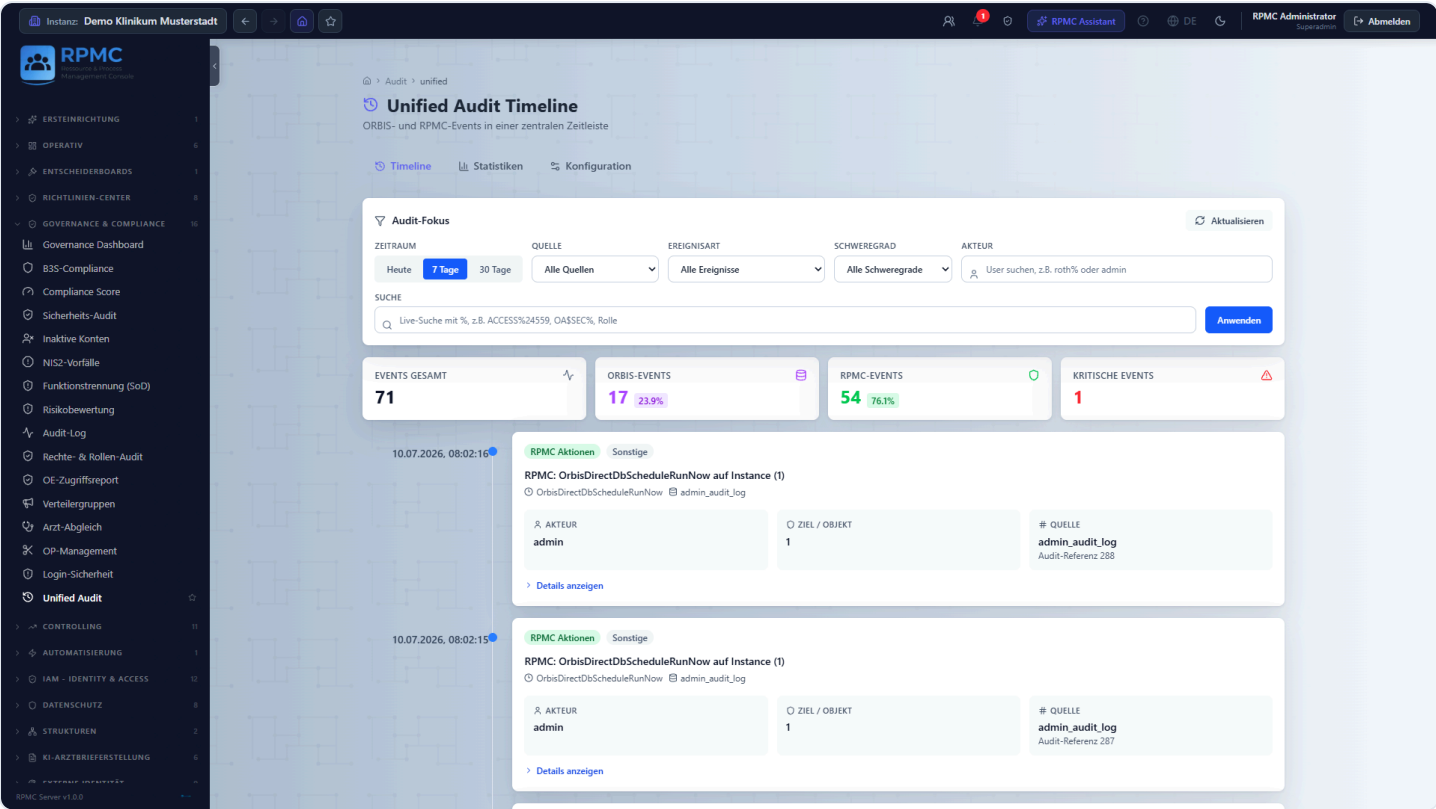
12.5 Login-Sicherheit & Anomalien



Login-Sicherheit & Anomalien — aktive Sessions, Anomalien der letzten 24 h, Brute-Force- und After-Hours-Erkennung. Die Anomalien-Tabelle der Demo ist leer — im Ernstfall stehen hier Konto, Muster und Zeitpunkt.

RPMC überwacht das Anmeldegeschehen: Brute-Force-Muster, Logins zu ungewöhnlichen Zeiten, ruhende Konten, die plötzlich erwachen, parallele Sessions. Auffälligkeiten erzeugen Ereignisse in der Audit-Kette und — bei angebundenem SIEM — Echtzeit-Alarme in der Sicherheits-Leitstelle. Die **Notfall-Login-Auswertung** dokumentiert zusätzlich jede Nutzung von ORBIS-Notfallzugängen mit Benutzer-Kontext — eine KRITIS-Pflicht, die kaum ein Haus manuell sauber erfüllt.

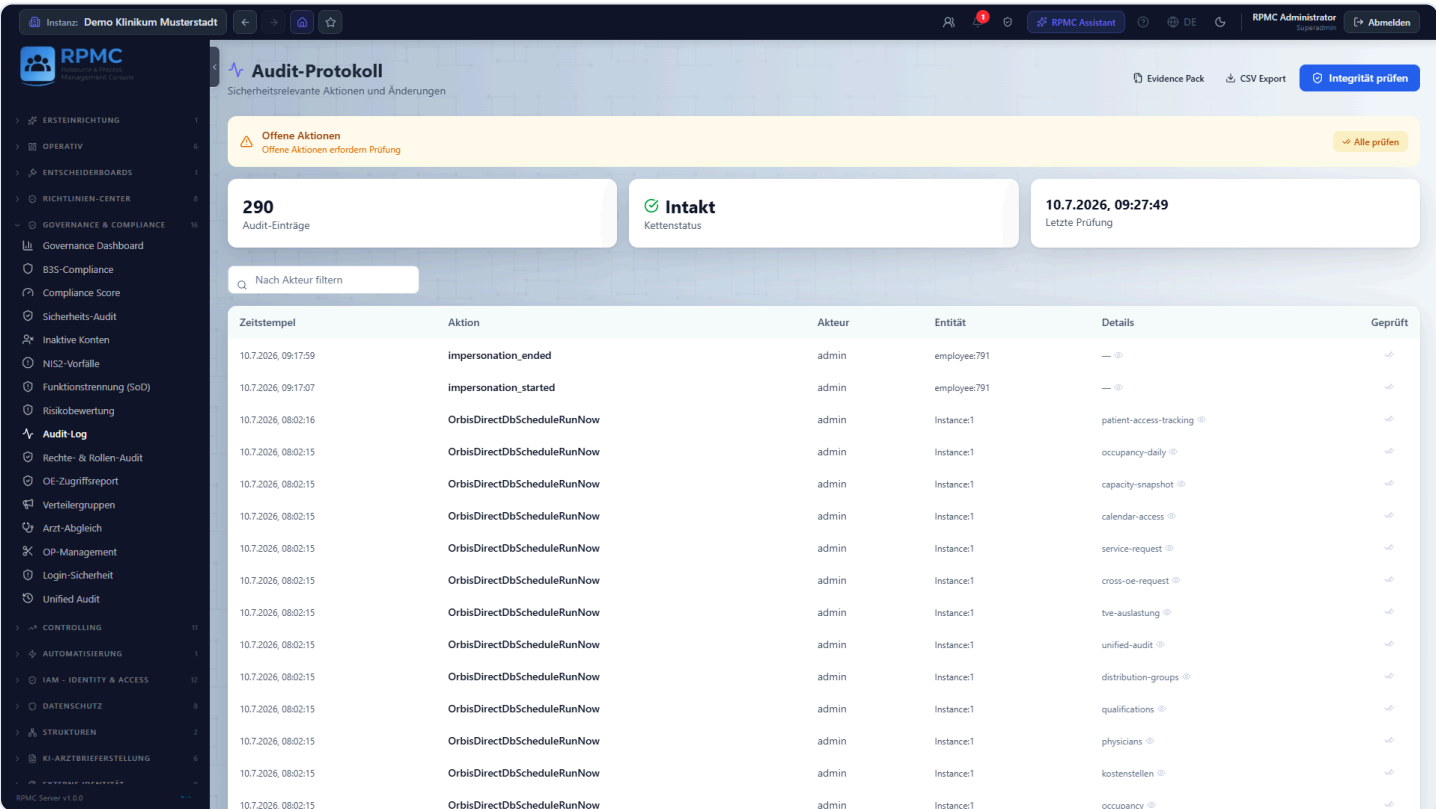
12.6 Unified Audit: zwei Welten, eine Zeitleiste



Unified Audit Timeline — ORBIS- und RPMC-Ereignisse in einem Strom (hier 71 Events: 17 ORBIS, 54 RPMC, 1 kritisch) mit Audit-Fokus-Filtern und Live-Suche. Prüffragen enden nicht mehr an der Systemgrenze.

Die Unified Audit Timeline führt die ORBIS-Änderungshistorie und die RPMC-Audit-Kette zusammen. Wer im KIS eine Rolle vergab und wer sie in RPMC rezertifizierte, steht in derselben chronologischen Sicht — filterbar, durchsuchbar, exportierbar.

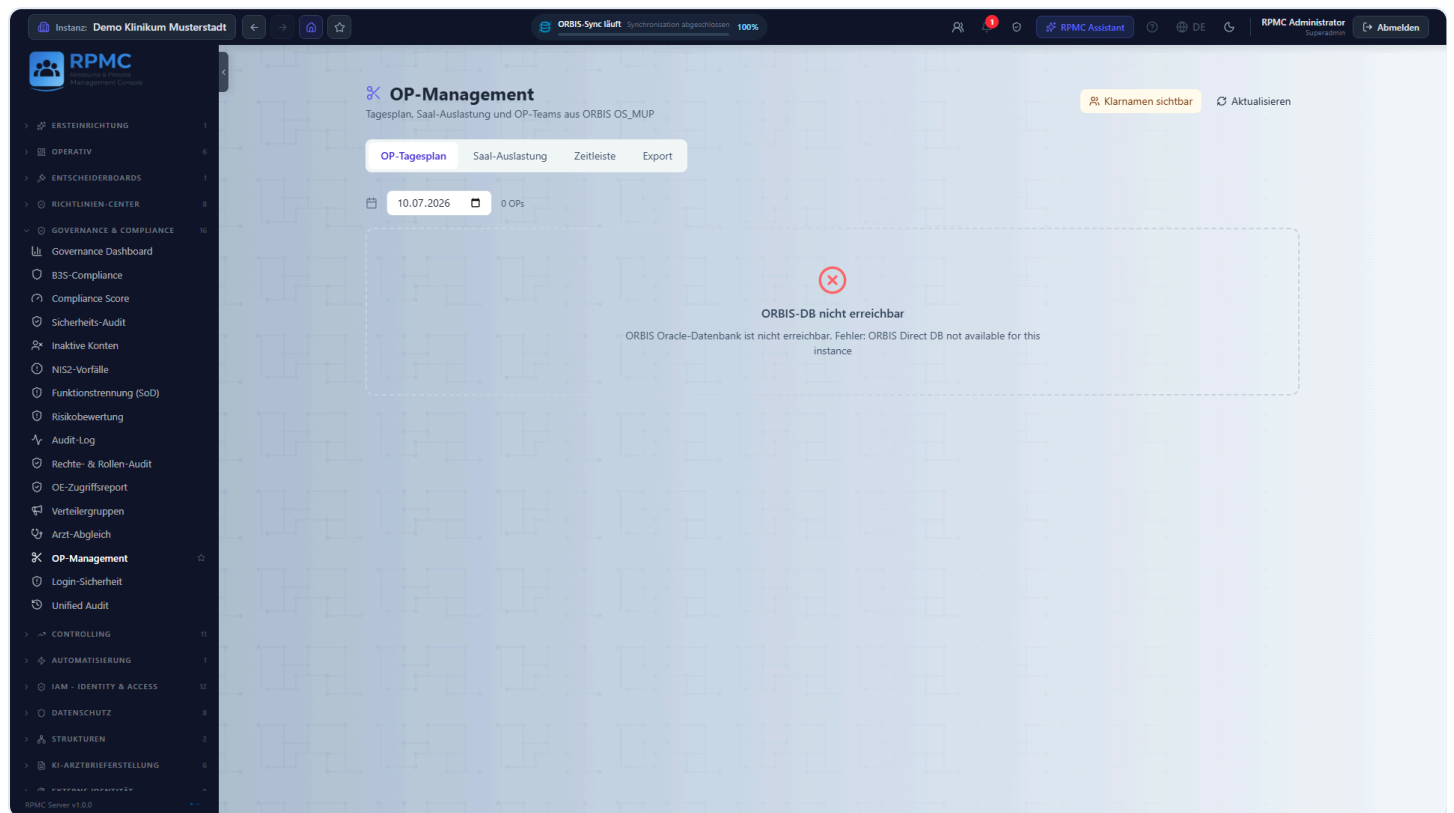
12.7 HMAC-verkettete, manipulationserkennende Auditspur



Audit-Protokoll — 290 Einträge, Ketten-Status „Intakt“: jeder Eintrag ist per HMAC-SHA256 mit seinem Vorgänger verkettet. Integritäts-Prüfung, Evidence-Pack- und CSV-Export direkt aus der Oberfläche.

Sicherheitsrelevante Aktionen werden HMAC-SHA256-verkettet und durch eine Append-only-Datenbankrolle geschützt. Änderungen an der Kette können durch die Verifikation erkannt werden. Ein Audit-of-Audit protokolliert zusätzlich, wer Audit-Einträge eingesehen hat.

12.8 OP-Management in Produktion



OP-Management — Tagesplan, Saal-Auslastung und OP-Teams direkt aus den ORBIS-OP-Daten. Live-ORBIS-Modul: auf der Demo-Instanz ohne Oracle-Verbindung bleibt die Ansicht bewusst leer statt Scheinwerte zu zeigen.

Das OP-Management wertet die ORBIS-OP-Planung live aus: Tagespläne, Saal-Auslastung, Teamzusammensetzungen, Wechselzeiten. Für das Prozess-Benchmarking exportiert RPMC die Auslastungs- und Plandaten in gängigen Formaten und bedient damit **Schnittstellen zu externen Benchmark-Anbietern wie Digma OPTeamizer** — das Haus nutzt seine ORBIS-Daten für den Anbietervergleich, ohne eine weitere Datenerfassung aufzubauen.

WAS KLASSISCHE IAM-SYSTEME HIER NICHT KÖNNEN

Compliance-Score, SoD und Rezertifizierung finden sich auch in großen IGA-Suiten. Aber: OP-Auslastung, Notfall-Login-Auswertung, ORBIS-vereinheitlichtes Audit und der Export an Klinik-Benchmark-Anbieter existieren dort schlicht nicht — RPMC verbindet IAM-Governance mit klinischer Betriebsrealität.

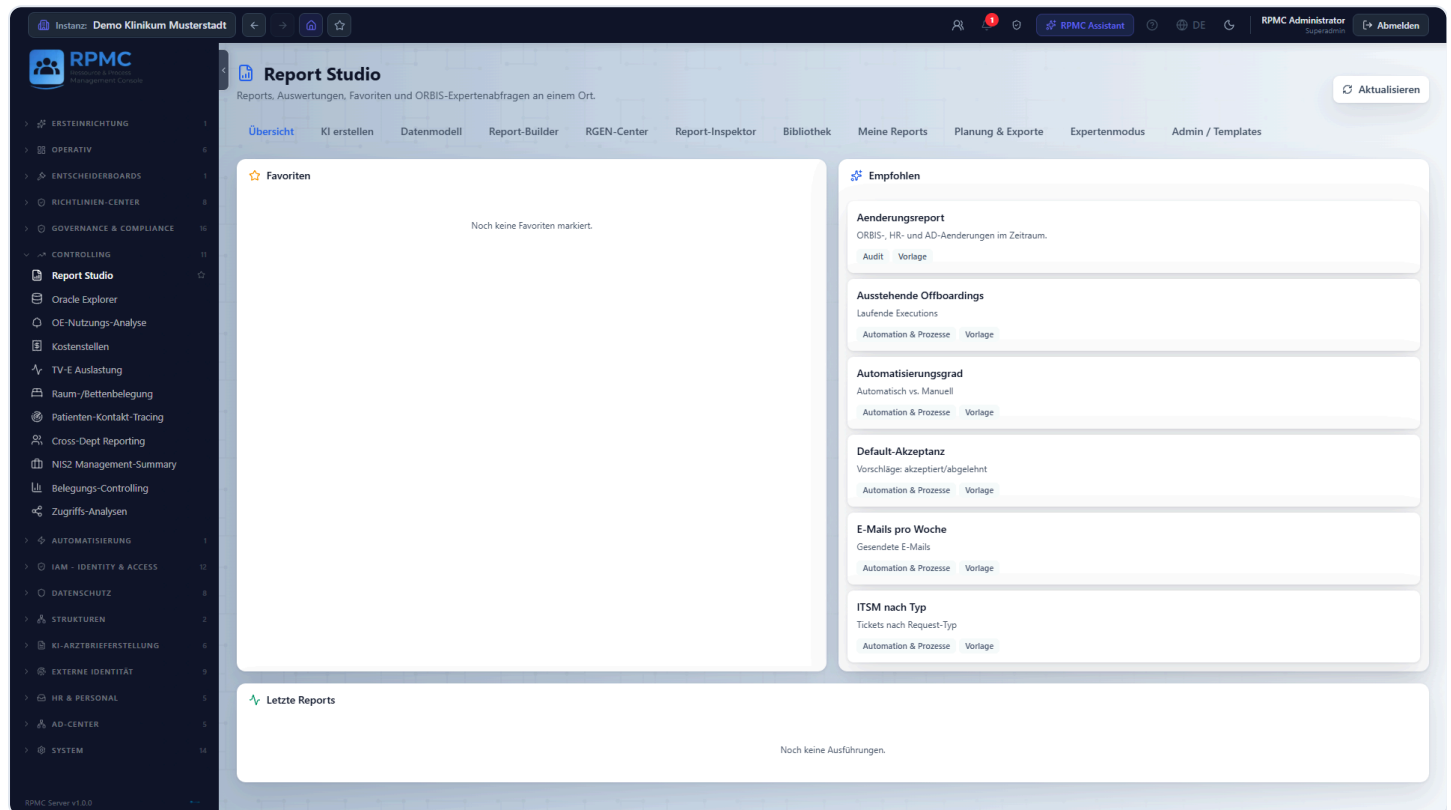
Controlling & Analysen

RELEASED

REPORT STUDIO: BETA

RPMC macht aus ORBIS-Rohdaten Steuerungswissen: Reports in Minuten statt IT-Tickets, Belegung bis auf das einzelne Bett, Pflegepersonal-Bemessung, Kostenstellen-Transparenz und forensische Zugriffs-Analysen — nahezu live und mit Sofort-Export für jede Auswertung.

13.1 Report Studio: mehrere Wege zum Report



Report Studio — Einstieg mit Favoriten und empfohlenen Vorlagen; die Reiter KI erstellen, Datenmodell, Report-Builder, RGEN-Center, Report-Inspektor und Bibliothek decken jeden Erstellungsweg ab.

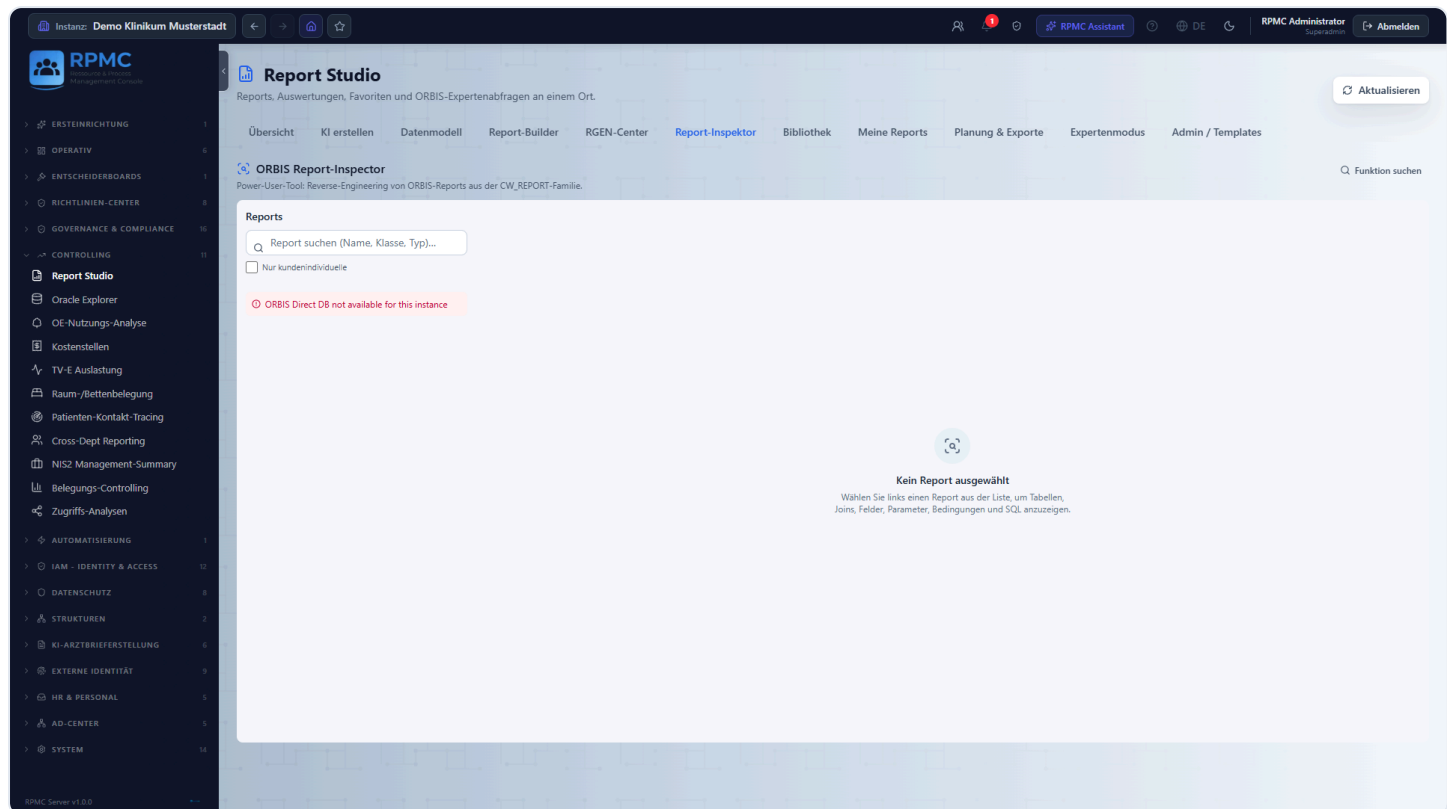
Kein Anwender gleicht dem anderen — deshalb führen im Report Studio mehrere Wege zum Ziel:

- **Bibliothek:** über 180 vorkonfigurierte Reports und Analysen (Audit, Compliance, Governance, Mitarbeiter, Rollen & Rechte, Trends) — Parameter setzen, Vorschau, Excel-Export. Favoriten und Zeitpläne inklusive.
- **Report-Builder:** eigene Reports per Drag-and-Drop auf dem visualisierten Datenmodell — für Power-User ohne SQL.
- **KI-Erstellung:** der Wunsch in natürlicher Sprache („Alle Mitarbeiter der Chirurgie mit Rollen, die seit über einem Jahr nicht rezertifiziert wurden“) wird zur wiederverwendbaren, garantiert lesenden Abfrage.
- **RGEN-Center & Datenmodell:** das durchsuchbare ORBIS-Schema-Wissensmodell — für Expertenhäuser, die eigene Auswertungstiefe wollen.

NAHEZU LIVE, SOFORT EXPORTIERT

Alle Auswertungen laufen gegen den aktuellen Datenbestand (je nach Anbindungsweg minutengenau) und besitzen einen Sofort-Export nach XLSX/CSV/PDF. Der klassische Weg — Anforderung ans Controlling, Wartezeit, Rückfragen, statischer Bericht — entfällt: Die Fachabteilung beantwortet ihre Frage selbst, in der Kaffeepause.

13.2 ORBIS-Report-Inspektor

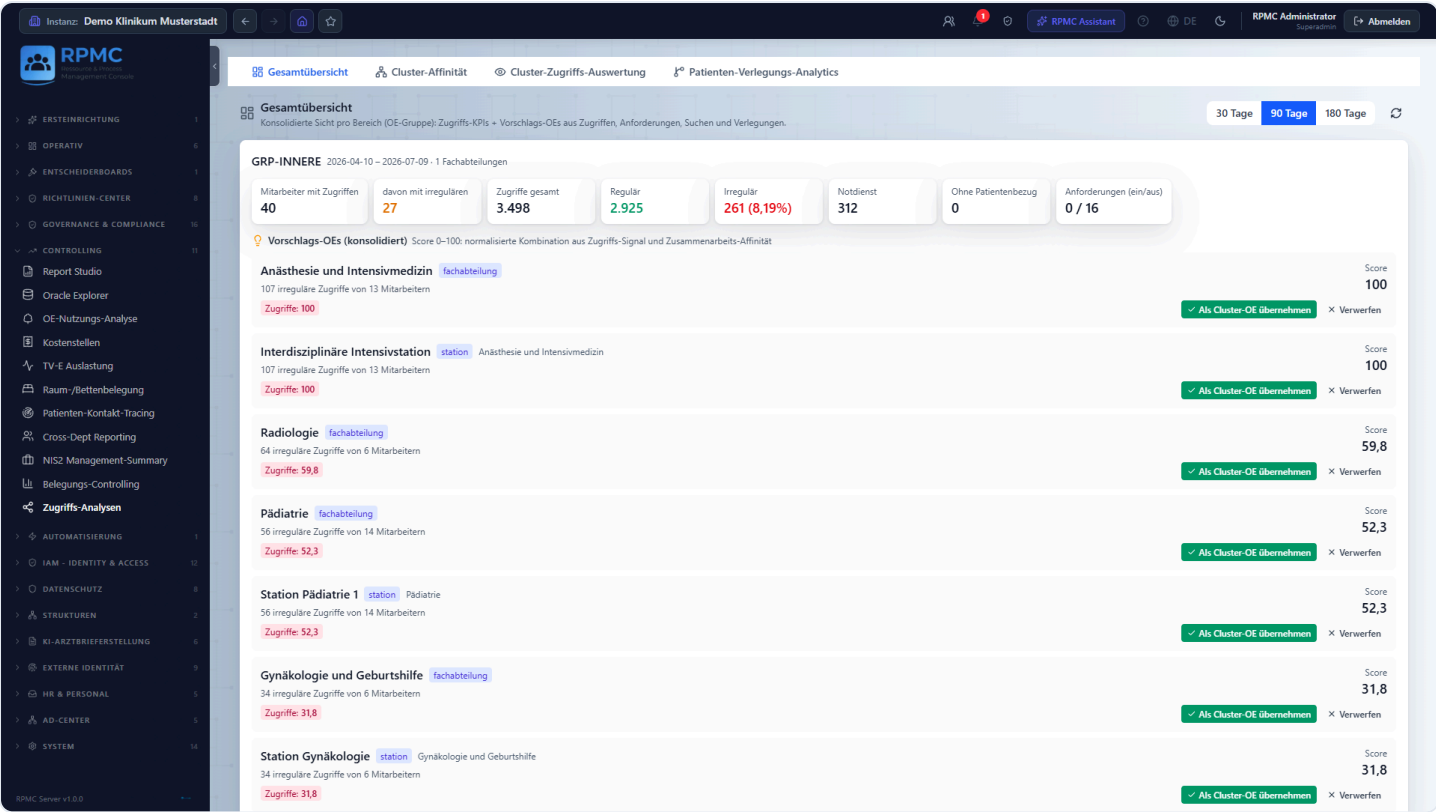


ORBIS-Report-Inspektor — Reverse-Engineering der hausinternen ORBIS-Report-Familie: Tabellen, Joins, Felder, Parameter und Bedingungen jedes Reports werden lesbar aufgeschlüsselt, kundenindividuelle Reports sind gezielt filterbar. (Live-ORBIS-Funktion; Demo ohne Oracle-Verbindung.)

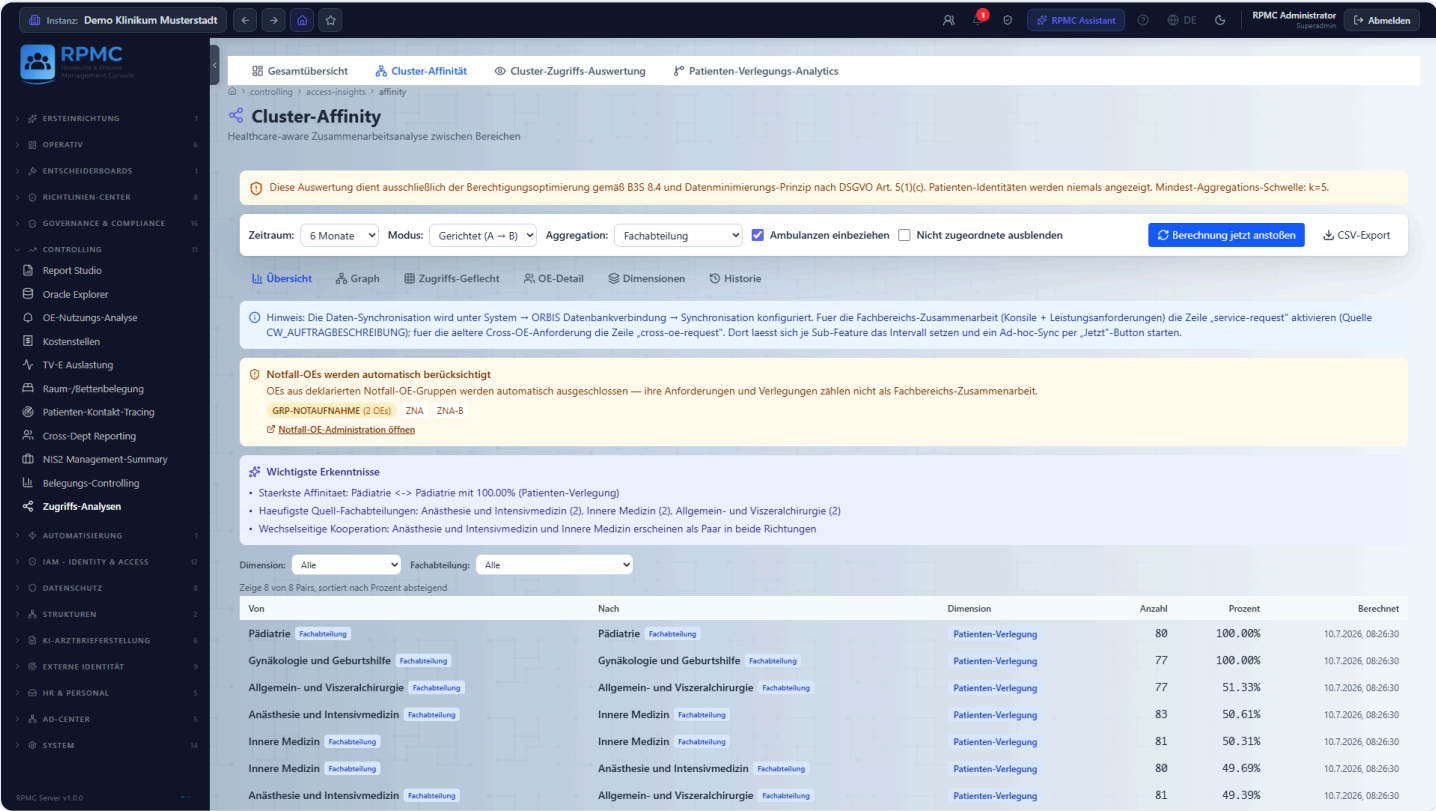
Über Jahre sammeln sich in jedem ORBIS Hunderte Reports an — niemand weiß mehr, was sie tun. Der Report-Inspektor öffnet die Blackbox: Er analysiert die ORBIS-Report-Definitionen inklusive kundenindividueller Designer-Reports und zeigt Struktur, Datenquellen und Bedingungen im Klartext. Für Konsolidierungen, Migrations-Vorbereitungen und die Frage „Können wir diesen Report abschalten?“ ein Werkzeug, das es so bislang nirgends gab.

13.3 Zugriffs-Analysen: das Röntgenbild der Zusammenarbeit

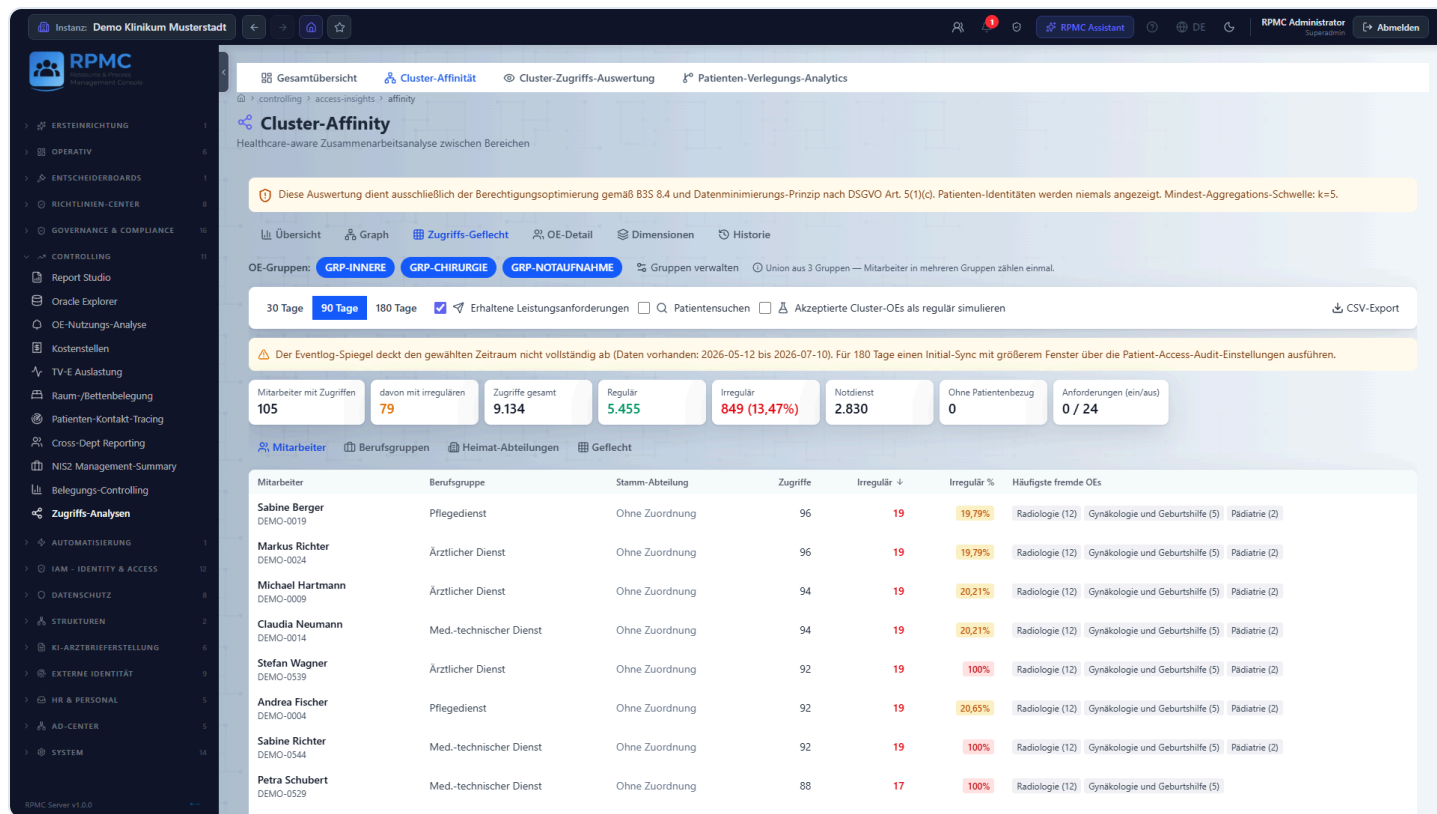
Die Zugriffs-Analysen beantworten die Governance-Kernfrage des § 393 SGB V: *Wer greift auf Patientendaten welcher Bereiche zu — und ist das plausibel?* Vier Sichten arbeiten dabei zusammen; alle respektieren die Notfall-OE-Automatik (Kapitel 17), damit Notaufnahme-Zugriffe die Statistik nicht verzerren.



Gesamtübersicht (neu) — konsolidierte Zugriffs-KPIs pro OE-Gruppe (hier GRP-INNERE: 3.498 Zugriffe, 8,19 % irregulär) mit score-bewerteten Vorschlägen, welche OEs fachlich zusammengehören. Alle Signale der Einzel-Analysen fließen zu einer 0–100-Bewertung zusammen.

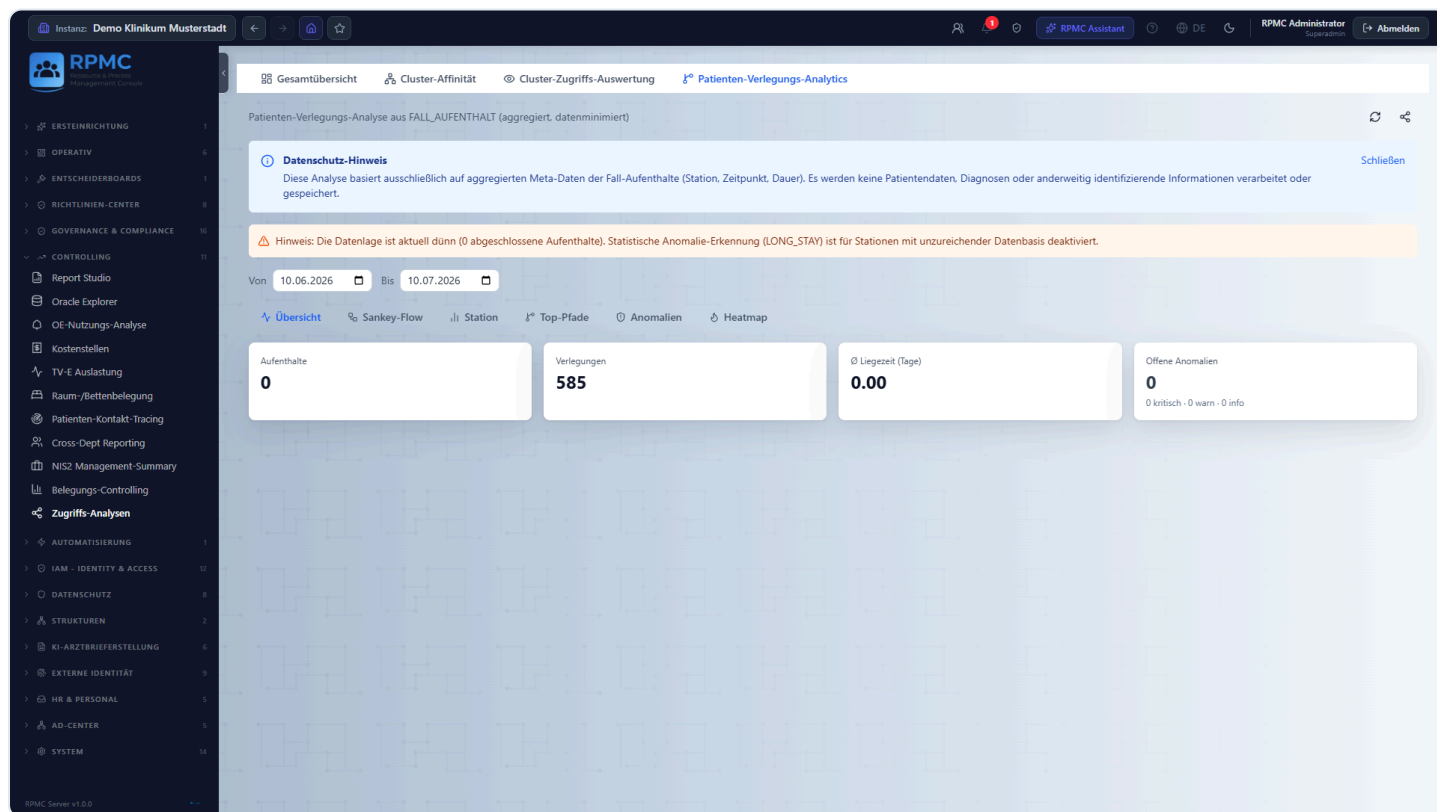


Cluster-Affinität — healthcare-bewusste Zusammenarbeitsanalyse (B3S 8.4) mit Notfall-OE-Ausschluss: Welche Bereiche arbeiten nachweislich zusammen? Die Affinitäts-Tabelle quantifiziert jede Achse in Prozent.



Zugriffs-Geflecht — Mehrfachauswahl von OE-Gruppen (hier Innere, Chirurgie, Notaufnahme kombiniert), KPI-Zeile (9.134 Zugriffe, 13,47 % irregulär) und Mitarbeiter-Tabelle mit individuellen Irregulär-Quoten: vom Bereichs-Muster bis zur Einzelperson.

Dynamische OE-Gruppen aus nachweisbarer Zusammenarbeit: Das Besondere an allen Cluster-Sichten — die Gruppen sind nicht organigramm-getrieben, sondern werden aus dem tatsächlichen, protokollierten Zugriffs- und Verlegungsgeschehen gebildet. RPMC schlägt vor: „Diese fünf Stationen bilden faktisch einen Versorgungs-Cluster.“ Berechtigungs-Zuschnitte folgen damit der gelebten Medizin statt dem Papier-Organigramm — und irreguläre Zugriffe heben sich umso schärfer ab.

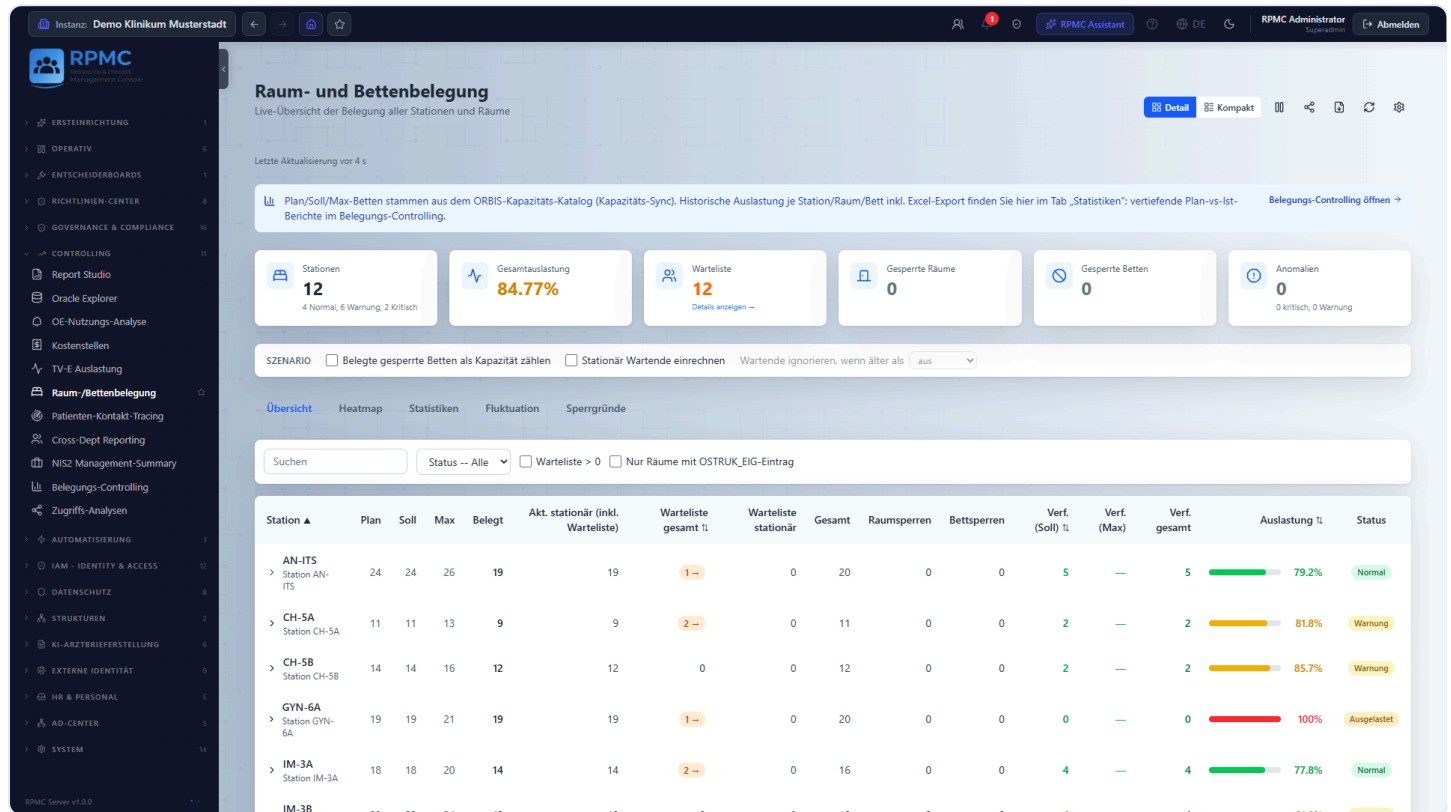


Patienten-Verlegungs-Analytics (neu) — Verlegungsströme zwischen Stationen als Sankey-Flow, Top-Pfade, Anomalien und Heatmap (hier 585 Verlegungen), mit Datenschutz-Hinweis. Verlegungsmuster ergänzen die Zugriffs-Sicht um die physische Patienten-Bewegung.

FALLBEISPIEL

Die Datenschutzbeauftragte prüft eine Beschwerde: Zugriffe einer Station auf fachfremde Akten. Das Zugriffs-Geflecht zeigt die Quote der Station im Vergleich, die Gesamtübersicht den Score, die Cluster-Affinität belegt: Mit der beklagten Fachabteilung besteht eine nachweisbare Konsil-Zusammenarbeit von 22 % — die Zugriffe sind plausibel. Aus einem diffusen Verdacht wird in zehn Minuten ein dokumentierter, datenbasierter Prüfvermerk.

13.4 Raum- und Bettenbelegung — bis auf das einzelne Bett

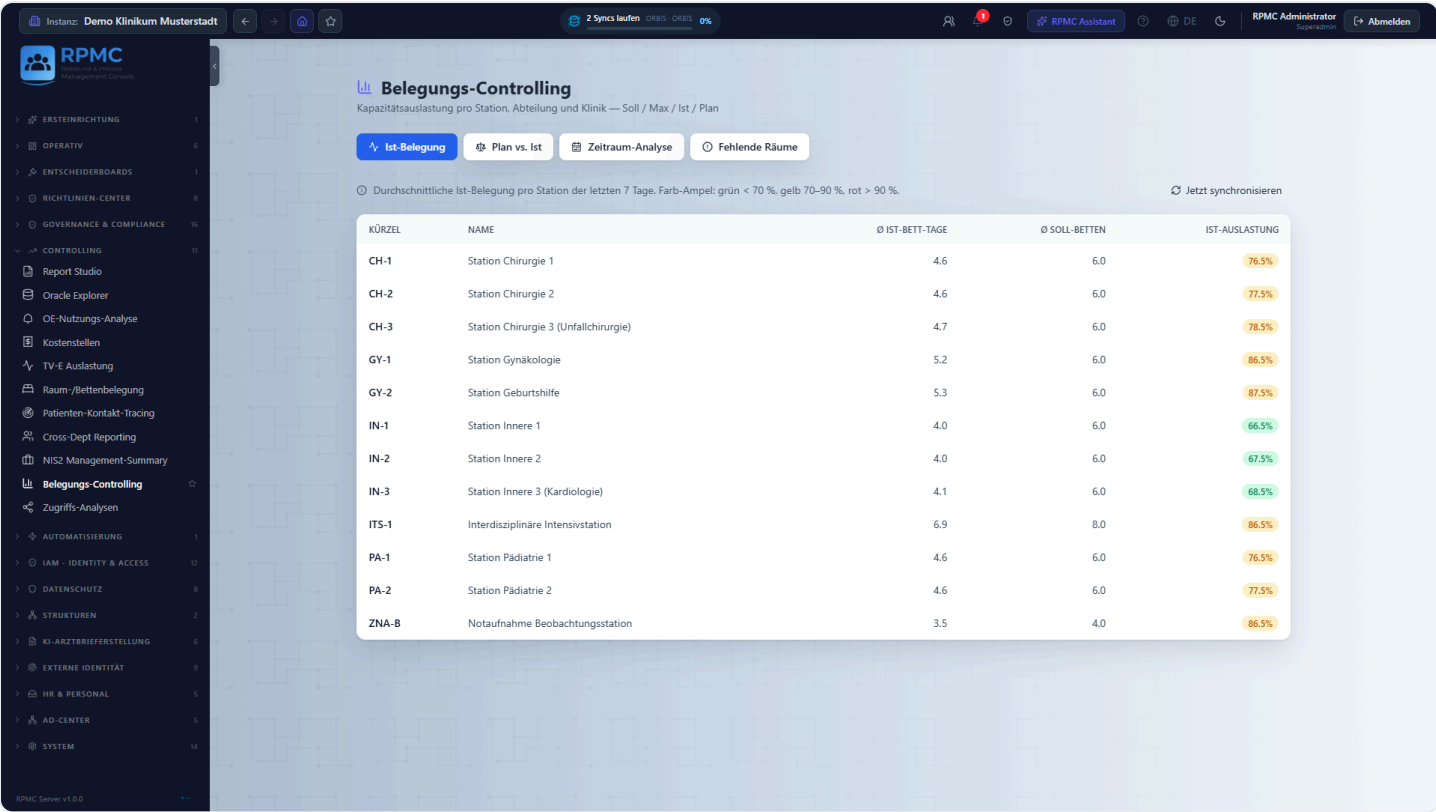


Raum-/Bettenbelegung — Live-Übersicht über 12 Stationen (84,77 % Gesamtauslastung, Warteliste 12) mit Auslastungs-Balken, Ampel-Status und Szenario-Schaltern je Station; Drilldown bis auf Raum- und Betten-Ebene.

RPMC liest Belegung, Räume und Betten direkt aus den ORBIS-Strukturen und zeigt den Zustand live: frei, belegt, gesperrt, in Reinigung — je Station, je Raum, je Bett. Ein Sonderthema verdient besondere Aufmerksamkeit:

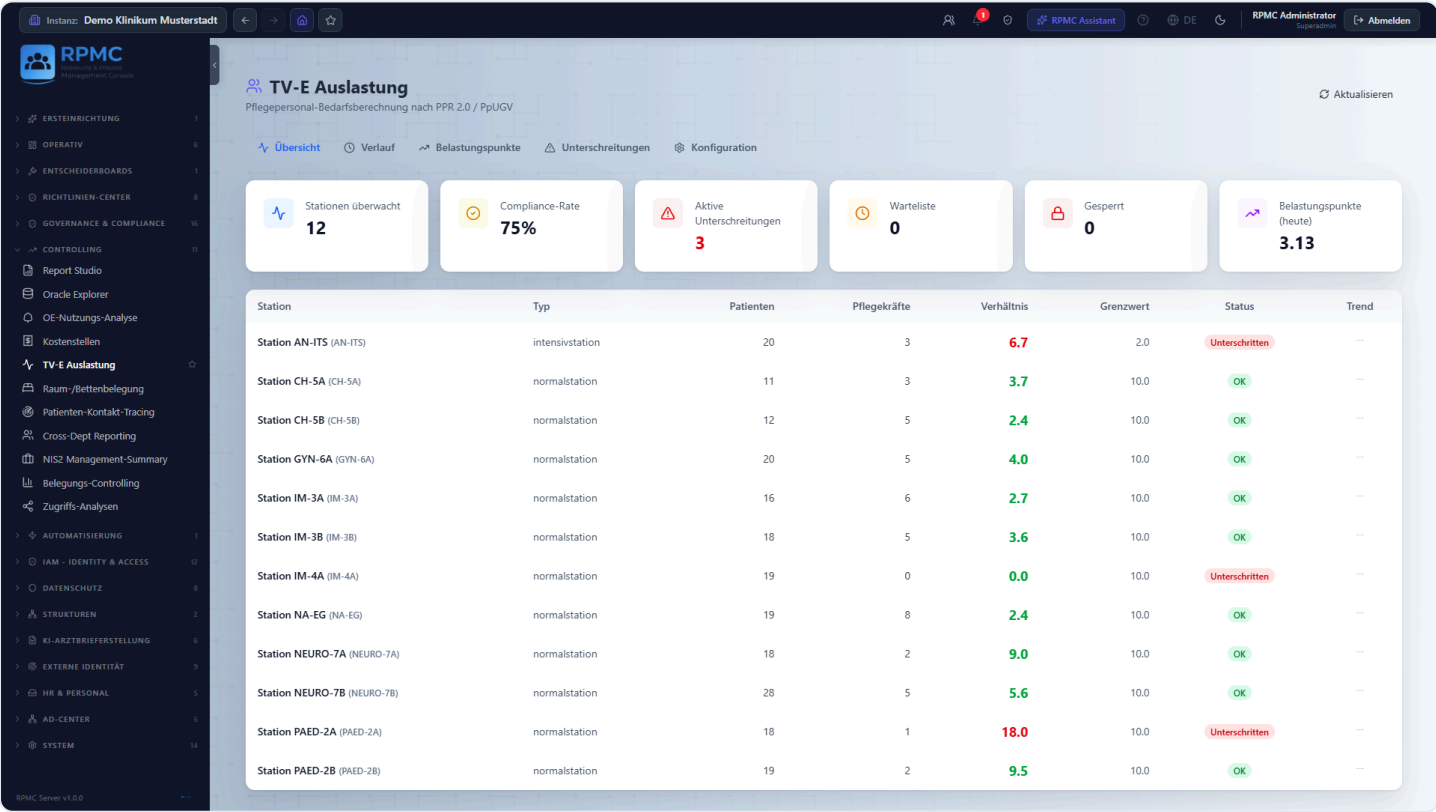
DAS BETTSPERREN-PROBLEM — UND WIE RPMC GEGENSTEUERT

In der Praxis werden Bettsperrern häufig zweckentfremdet: als Dauer-Reservierung, als „privates“ Pufferbett, als vergessene Sperre nach längst beendeter Sanierung. Die Folge sind Phantom-Engpässe — das Haus weist Patienten ab, während gesperrte Betten leer stehen, und die Auslastungs-Statistik wird systematisch verfälscht. RPMC macht jede Sperre sichtbar und prüfbar: Beginn, Ende, Grund und Dauer je Sperre, auffällig lange oder unbegründete Sperren werden markiert, Sperr-Statistiken je Station decken Muster auf. Das Controlling erkennt zweckentfremdete Sperren auf einen Blick — und gewinnt real verfügbare Betten zurück, ohne ein einziges neues Bett zu kaufen.



Belegungs-Controlling (Kapazitäts-Reporting) — Ist-Belegung pro Station gegen Soll-Bett-Tage mit Farb-Ampel; Reiter für Plan vs. Ist, Zeitraum-Analyse und fehlende Räume. Die Datengrundlage für Vorstandsberichte und Strukturentscheidungen.

13.5 TV-E-Auslastung & PPR 2.0



TV-E-Auslastung / PPR-2.0-Dashboard — Pflegepersonal-Bedarf je Station mit Compliance-Rate (hier 75 %), aktiven Unterschreitungen und Patienten-Pflegekräfte-Verhältnis. Personaluntergrenzen werden zur täglich gelebten Kennzahl statt zur Quartals-Überraschung.

Das Dashboard spiegelt die Personalbemessungs-Vorgaben gegen die tatsächliche Besetzung: Soll/Ist je Station und Schicht, Compliance-Rate, aktive Unterschreitungen mit Alarm. Pflegedienstleitung und Geschäftsführung sehen dasselbe Bild — Diskussionen über Zahlen weichen Diskussionen über Maßnahmen.

13.6 Kostenstellen

Instanz: Demo Klinikum Musterstadt

RPMC

Personale & Prozess Management Console

ERSTEINRICHTUNG

OPERATIV

ENTSCHEIDERBOARDS

RICHTLINIEN-CENTER

GOVERNANCE & COMPLIANCE

CONTROLLING

Report Studio

Oracle Explorer

OE-Nutzungs-Analyse

Kostenstellen

TV-E Auslastung

Raum-/Bettenbelegung

Patienten-Kontakt-Tracing

Cross-Dept Reporting

NIS2 Management-Summary

Belegungs-Controlling

Zugriffs-Analysen

AUTOMATISIERUNG

IAM - IDENTITY & ACCESS

DATENSCHUTZ

STRUKTUREN

KI-ARZTBRIEFERSTELLUNG

EXTERNE IDENTITÄT

HR & PERSONAL

AD-CENTER

SYSTEM

RPMC Server v1.0.0

Kostenstellen

Kostenstellen-Zuordnung für Mitarbeiter und Organisationseinheiten

20

Kostenstellen gesamt

0

Mitarbeiter zugeordnet

780

Mitarbeiter ohne Kostenstelle

Übersicht

Hierarchie

OEs & Kostenstellen

Nutzung / Abrechnung

TV-E Belastungspunkte

Suchen: KST-Nr., Bezeichnung, OE, Kostenart ...

Alle Einrichtungen

KST-NR.	BEZEICHNUNG	ART	MITARBEITER	OES
2301	KST Station Innere 1	K	0	1
2302	KST Station Innere 2	K	0	1
2303	KST Station Innere 3	K	0	1
2310	KST Innere Medizin Leitung	K	0	1
2401	KST Station Chirurgie 1	K	0	1
2402	KST Station Chirurgie 2	K	0	1
2403	KST Station Chirurgie 3	K	0	1
2410	KST Chirurgie Leitung	K	0	1
2501	KST Station Gynäkologie	K	0	1
2502	KST Station Geburtshilfe	K	0	1
2601	KST Station Pädiatrie 1	K	0	1
2602	KST Station Pädiatrie 2	K	0	1
2701	KST Intensivstation	K	0	1

Kostenstellen · Übersicht — 20 Kostenstellen mit KPI-Kacheln und übergreifender Suche (KST-Nummer, Bezeichnung, OE, Kostenart).

Instanz: Demo Klinikum Musterstadt

RPMC

Personale & Prozess Management Console

ERSTEINRICHTUNG

OPERATIV

ENTSCHEIDERBOARDS

RICHTLINIEN-CENTER

GOVERNANCE & COMPLIANCE

CONTROLLING

Report Studio

Oracle Explorer

OE-Nutzungs-Analyse

Kostenstellen

TV-E Auslastung

Raum-/Bettenbelegung

Patienten-Kontakt-Tracing

Cross-Dept Reporting

NIS2 Management-Summary

Belegungs-Controlling

Zugriffs-Analysen

AUTOMATISIERUNG

IAM - IDENTITY & ACCESS

DATENSCHUTZ

STRUKTUREN

KI-ARZTBRIEFERSTELLUNG

EXTERNE IDENTITÄT

HR & PERSONAL

AD-CENTER

SYSTEM

RPMC Server v1.0.0

Kostenstellen

Kostenstellen-Zuordnung für Mitarbeiter und Organisationseinheiten

20

Kostenstellen gesamt

0

Mitarbeiter zugeordnet

780

Mitarbeiter ohne Kostenstelle

Übersicht

Hierarchie

OEs & Kostenstellen

Nutzung / Abrechnung

TV-E Belastungspunkte

Suchen: KST-Nr., Bezeichnung, OE, Kostenart ...

Alle Einrichtungen

OE-KÜRZEL	OE-NAME	EINRICHTUNG	ZUGEORDNETE KOSTENSTELLEN
AMB-CH	Chirurgische Ambulanz	Demo Klinikum Musterstadt	Keine Kostenstelle zugeordnet
AMB-GY	Gynäkologische Ambulanz	Demo Klinikum Musterstadt	Keine Kostenstelle zugeordnet
AMB-IN	Internistische Ambulanz	Demo Klinikum Musterstadt	Keine Kostenstelle zugeordnet
ANE	Anästhesie und Intensivmedizin	Demo Klinikum Musterstadt	2702 KST Anästhesie Haupt
CH-1	Station Chirurgie 1	Demo Klinikum Musterstadt	2401 KST Station Chirurgie 1 Haupt
CH-1-Z1	Zimmer 1 (CH-1)	Demo Klinikum Musterstadt	Keine Kostenstelle zugeordnet
CH-1-Z1-B1	Bett 1	Demo Klinikum Musterstadt	Keine Kostenstelle zugeordnet
CH-1-Z1-B2	Bett 2	Demo Klinikum Musterstadt	Keine Kostenstelle zugeordnet
CH-1-Z2	Zimmer 2 (CH-1)	Demo Klinikum Musterstadt	Keine Kostenstelle zugeordnet
CH-1-Z2-B1	Bett 1	Demo Klinikum Musterstadt	Keine Kostenstelle zugeordnet
CH-1-Z2-B2	Bett 2	Demo Klinikum Musterstadt	Keine Kostenstelle zugeordnet
CH-1-Z3	Zimmer 3 (CH-1)	Demo Klinikum Musterstadt	Keine Kostenstelle zugeordnet
CH-1-Z3-B1	Bett 1	Demo Klinikum Musterstadt	Keine Kostenstelle zugeordnet
CH-1-Z3-B2	Bett 2	Demo Klinikum Musterstadt	Keine Kostenstelle zugeordnet

Kostenstellen · OEs & Kostenstellen (neu) — die Zuordnung von Organisationseinheiten zu Kostenstellen: Grundlage jeder verursachungsgerechten Personalkosten-Verteilung.

Instanz: Demo Klinikum Musterstadt

RPMC Management Console

ERSTEINRICHTUNG

OPERATIV

ENTSCHEIDERBOARDS

RICHTLINIEN-CENTER

GOVERNANCE & COMPLIANCE

CONTROLLING

Report Studio

Oracle Explorer

OE-Nutzungs-Analyse

Kostenstellen

TV-E Auslastung

Raum-/Bettenbelegung

Patienten-Kontakt-Tracing

Cross-Dept Reporting

NIS2 Management-Summary

Belegungs-Controlling

Zugriffs-Analysen

AUTOMATISIERUNG

IAM - IDENTITY & ACCESS

DATENSCHUTZ

STRUKTUREN

KI-ARZTBRIEFERSTELLUNG

EXTERNE IDENTITÄT

HR & PERSONAL

AD-CENTER

SYSTEM

RPMC Server v1.0.0

Kostenstellen

Kostenstellen-Zuordnung für Mitarbeiter und Organisationseinheiten

Export (XLSX)

20Kostenstellen gesamt

0Mitarbeiter zugeordnet

780Mitarbeiter ohne Kostenstelle

Übersicht

Hierarchie

OEs & Kostenstellen

Nutzung / Abrechnung

TV-E Belastungspunkte

Suchen: KST-Nr., Bezeichnung, OE, Kostenart ...

KST-NR.	BEZEICHNUNG	PERIODE	KOSTENART	BUCHUNGEN	FÄLLE	BETRAG
2301	KST Station Innere 1	2025-08	Medizinischer Sachbedarf	156	27	21.519,00
2301	KST Station Innere 1	2025-08	Personalkosten	143	24	21.118,00
2301	KST Station Innere 1	2025-09	Medizinischer Sachbedarf	149	22	20.602,00
2301	KST Station Innere 1	2025-09	Personalkosten	136	19	20.201,00
2301	KST Station Innere 1	2025-10	Medizinischer Sachbedarf	142	17	19.685,00
2301	KST Station Innere 1	2025-10	Personalkosten	129	14	19.284,00
2301	KST Station Innere 1	2025-11	Medizinischer Sachbedarf	135	12	18.768,00
2301	KST Station Innere 1	2025-11	Personalkosten	122	9	18.367,00
2301	KST Station Innere 1	2025-12	Medizinischer Sachbedarf	128	67	17.851,00
2301	KST Station Innere 1	2025-12	Personalkosten	115	64	17.450,00
2301	KST Station Innere 1	2026-01	Medizinischer Sachbedarf	121	62	16.934,00
2301	KST Station Innere 1	2026-01	Personalkosten	108	59	16.533,00
2301	KST Station Innere 1	2026-02	Medizinischer Sachbedarf	114	57	16.017,00
2301	KST Station Innere 1	2026-02	Personalkosten	101	54	15.616,00
2301	KST Station Innere 1	2026-03	Medizinischer Sachbedarf	107	52	15.100,00

Kostenstellen · Nutzung / Abrechnung — Perioden-Daten mit Buchungen, Fällen und Beträgen je Kostenart (z. B. Medizinischer Sachbedarf, Personalkosten) direkt aus den ORBIS-Buchungsdaten.

Die Kostenstellen-Sicht verbindet Organisationsstruktur, Personal und Buchungsdaten: Welche OE bucht auf welche Kostenstelle, welche Mitarbeiter sind zugeordnet, wie entwickeln sich Beträge je Kostenart? Exporte fließen direkt in die Controlling-Werkzeuge des Hauses.

13.7 Patienten-Kontakt-Tracing

Instanz: Demo Klinikum Musterstadt

RPMC Management Console

ERSTEINRICHTUNG

OPERATIV

ENTSCHEIDERBOARDS

RICHTLINIEN-CENTER

GOVERNANCE & COMPLIANCE

CONTROLLING

Report Studio

Oracle Explorer

OE-Nutzungs-Analyse

Kostenstellen

TV-E Auslastung

Raum-/Bettenbelegung

Patienten-Kontakt-Tracing

Cross-Dept Reporting

NIS2 Management-Summary

Belegungs-Controlling

Zugriffs-Analysen

AUTOMATISIERUNG

IAM - IDENTITY & ACCESS

DATENSCHUTZ

STRUKTUREN

KI-ARZTBRIEFERSTELLUNG

EXTERNE IDENTITÄT

HR & PERSONAL

AD-CENTER

SYSTEM

RPMC Server v1.0.0

Patienten-Kontakt-Tracing

Infektions-Kontaktketten zwischen Patienten analysieren

DSGVO Art. 9 — Besondere Kategorien personenbezogener Daten

Die hier angezeigten Daten sind Gesundheitsdaten im Sinne von Art. 9 DSGVO. Der Zugriff ist auf berechtigte Nutzer (Hygiene, Infektionsschutz) beschränkt und wird im Audit-Log protokolliert.

Les- und Suchzugriffe auf Patientendaten werden im Audit-Log erfasst (wer, wann, welche Fallnummer). Fallnummern werden im Klartext angezeigt, damit fachlich gearbeitet werden kann (BUG-290).

ORBIS Direct DB nicht verfügbar

Die ORBIS Direct DB ist konfiguriert, aber aktuell nicht erreichbar. Bitte Verbindung und Zugangsdaten unter System prüfen.

Patienten-Tracing ist deaktiviert. Ein Administrator kann das Modul in den Einstellungen aktivieren.

In Einstellungen aktivieren --

Noch nie berechnet - Lookback: 90 Tage - Aufbewahrung: 730 Tage

Patient suchen

Patient-Timeline

Stations-Kontakte

Patient per Fallnummer suchen

ORBIS Direct DB ist für diese Instanz nicht verfügbar. Es werden keine Live-Patientendaten geladen.

Fallnummer

z.B. 2024-12345

Suchen

Kürzlich aufgenommene Patienten

ORBIS Direct DB ist für diese Instanz nicht verfügbar. Es werden keine Live-Patientendaten geladen.

Exposure-Radar — Kontakt-Tracing für Hygiene-Teams mit Patienten-Timeline und Stations-Kontakten, ausdrücklich mit DSGVO-Art.-9-Hinweis und Pseudonymisierung. (Live-ORBIS-Modul; auf der Demo deaktiviert.)

Patienten-Kontakt-Tracing
Infektions-Kontaktketten zwischen Patienten analysieren

DSGVO Art. 9 — Besondere Kategorien personenbezogener Daten
Die hier angezeigten Daten sind Gesundheitsdaten im Sinne von Art. 9 DSGVO. Der Zugriff ist auf berechtigte Nutzer (Hygiene, Infektionsschutz) beschränkt und wird im Audit-Log protokolliert.

Lese- und Suchzugriffe auf Patientendaten werden im Audit-Log erfasst (wer, wann, welche Fallnummer). Fallnummern werden im Klartext angezeigt, damit fachlich gearbeitet werden kann (BUG-290).

ORBIS Direct DB nicht verfügbar
Die ORBIS Direct DB ist konfiguriert, aber aktuell nicht erreichbar. Bitte Verbindung und Zugangsdaten unter System prüfen.

Patienten-Tracing ist deaktiviert. Ein Administrator kann das Modul in den Einstellungen aktivieren.
[In Einstellungen aktivieren](#)

Noch nie berechnet - Lookback: 90 Tage - Aufbewahrung: 730 Tage

Q Patient suchen Patient-Timeline Stations-Kontakte

Kontakt-Ketten auf einer Station

Station Von Bis

ITS-1 03.07.2026 11:12 10.07.2026 11:12 [Laden](#)

Sortieren nach: Überlappungsdauer Risiko Beginn

Patient 1	Patient 2	Station	Datum	Überlappungsdauer	Risiko
demoed92_0739	demo352d_7251	ITS-1	05.07.2026, 01:59 → 05.07.2026, 10:59	9.0 h Überlappung	Hoch
demoec6e_8adC	demoFF33_53ba	ITS-1	08.07.2026, 09:59 → 08.07.2026, 14:59	5.0 h Überlappung	Niedrig

Stations-Kontakte (Kontakt-Ketten) — pseudonymisierte Patienten-Paare der Intensivstation ITS-1 mit Überlappungszeitraum (z. B. 9,0 h gemeinsamer Aufenthalt) und Risiko-Badges (Hoch/Niedrig): Aus Bewegungsdaten wird eine priorisierte Arbeitsliste für das Hygiene-Team.

Bei Keimausbruch oder meldepflichtiger Infektion zählt jede Stunde: Das Exposure-Radar rekonstruiert aus den ORBIS-Bewegungsdaten, welche Patienten und Bereiche mit einem Index-Patienten in Kontakt kamen — pseudonymisiert, hygienetauglich, dokumentiert. Was Hygiene-Teams sonst aus Kurven und Verlegungslisten von Hand rekonstruieren, liefert RPMC in Minuten.

WAS KLASSISCHE IAM-SYSTEME HIER NICHT KÖNNEN

Nichts davon. Belegungs-Controlling, Bettsperren-Forensik, PPR-Bemessung, OP-Benchmark-Export und Kontakt-Tracing liegen komplett außerhalb des Horizonts generischer IAM-Produkte — in RPMC sind sie derselbe Datenbestand, dieselbe Oberfläche, dieselbe Lizenz.

ITSM-Anbindung

RELEASED

RPMC ersetzt kein Ticketsystem — es füttert es richtig. Die ITSM-Anbindung verbindet IAM-Ereignisse mit den Service-Prozessen des Hauses, kryptografisch abgesichert.

- **Webhook-Integration:** definierte Ereignisse (Onboarding abgeschlossen, Offboarding fällig, SoD-Verstoß, Gremien-Beschluss ...) lösen Webhooks an das ITSM aus — mit HMAC-Signatur, Zeitstempel und Nonce-Replay-Schutz, damit kein Dritter Tickets fälschen oder wiederholen kann.
- **Board-Kopplung:** Entscheiderboard-Vorgänge können Ticket-seitig gespiegelt werden — das Gremium arbeitet in RPMC, der Service-Desk behält seine gewohnte Sicht.
- **Fall-Übergaben:** Status-Center-Fälle, die IT-Arbeit erfordern, wandern als strukturierte Tickets ins ITSM statt als formlose Mails.
- **Generisch statt proprietär:** Die Webhook-Schnittstelle ist bewusst systemneutral — gängige ITSM-Werkzeuge werden über ihre Standard-Eingänge angebunden, ohne Vendor-Lock-in.

NUTZEN

IAM-Vorgänge werden im bestehenden Service-Prozess sichtbar und messbar (Durchlaufzeiten, SLA), ohne Doppelpflege. Die Signatur-Absicherung macht die Strecke auditfest — auch die Schnittstelle selbst besteht die Prüfung.

MyIdentity-Portal — Self-Service mit Leitplanken RELEASED

Das MyIdentity-Portal löst den ältesten Zielkonflikt der Krankenhaus-IT: maximale Freiheit für Anwender und IT — bei gleichzeitig strikter Auditierbarkeit. Mitarbeiter verwalten ihre Identität selbst und beantragen Rechte eigenständig; RPMC sorgt dafür, dass dabei nichts unkontrolliert bleibt.

15.1 Das eigene Profil — konsolidiert und transparent



MP
Mein Profil

Benutzername

☐ Benutzername merken

Passwort

Anmelden

Eigenständiges Portal — MyIdentity läuft als eigenes, im Design des Hauses gebrandetes Portal mit eigener Anmeldung (eigener Port, eigene Optik) — bewusst getrennt von der Admin-Konsole.

Sie agieren als **Wagner, Daniel** (Kürzel: DWAGNER, Abt: Chirurgie) — Impersonation aktiv

Beenden

My Identity

Mein ProfilMein TeamMitarbeiter wechselnWagner, Daniel

Daniel Wagner

Facharzt — Chirurgie

Kürzel: DWAGNER

Profil

Meine Zugriffe

Einsatzplan

Meine Berechtigungen

Stammdaten

Nachname
Wagner

Vorname
Daniel

Titel
Dr. med.

Personalnummer
P10011

ORBIS-Kürzel
DWAGNER

Geburtsdatum
Nicht hinterlegt

Beschäftigungsstatus
Nicht hinterlegt

Vertragsart
Nicht hinterlegt

Eintrittsdatum
Nicht hinterlegt

Kontakt

E-Mail
d.wagner@uniklinik.de

Telefon
Nicht hinterlegt

Mobiletelefon
Nicht hinterlegt

Meine Anträge

Keine offenen Anträge. Klicken Sie auf das Stift-Symbol neben einem Feld um eine Änderung zu beantragen.

Organisation

Abteilung (offiziell)
Chirurgie

Einrichtung
Universitätsklinikum Eppendorf Hamburg

Funktionen & Qualifikationen

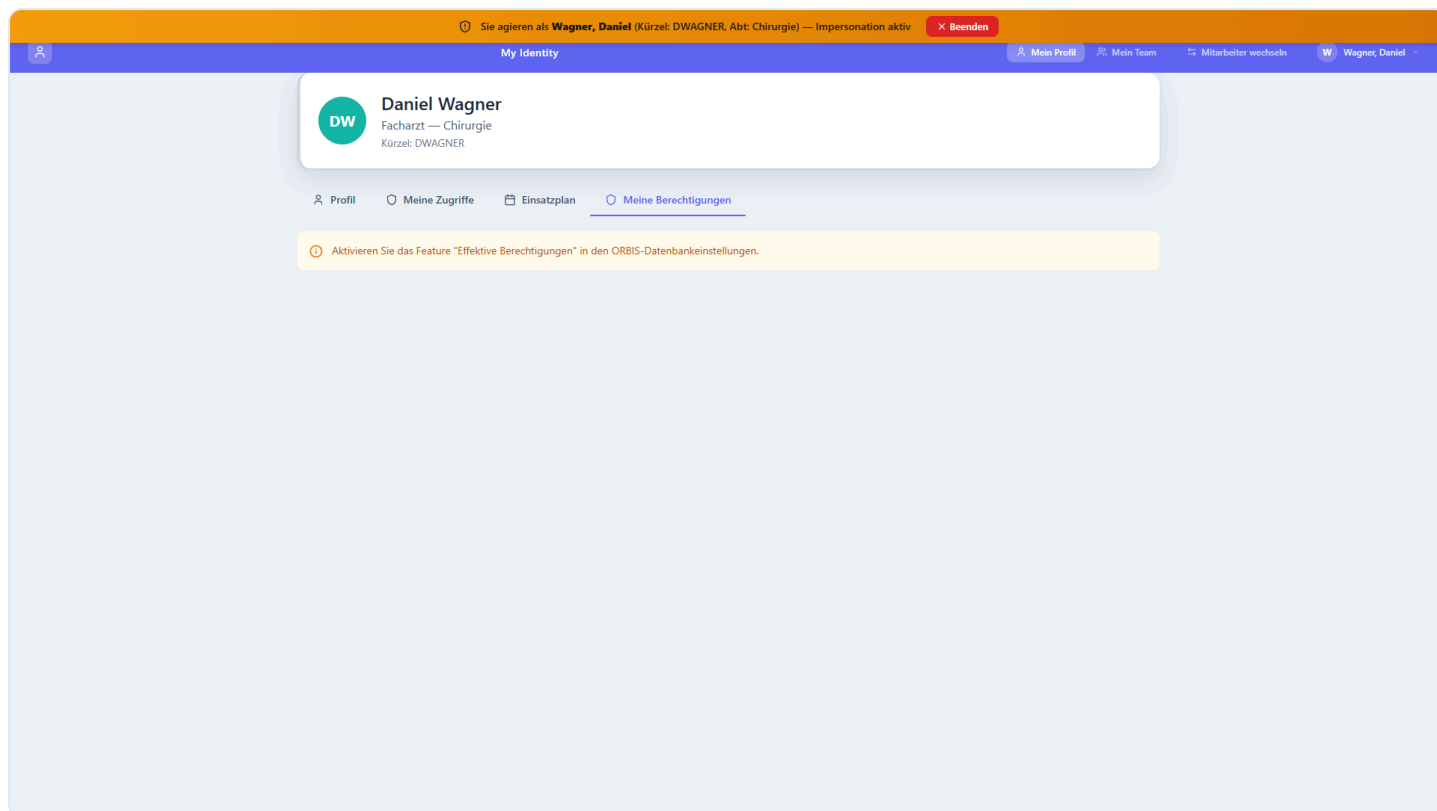
Berufsbezeichnung
Nicht hinterlegt

Funktion (offiziell)
Facharzt

Profilseite — Stammdaten, Kontakt, Organisation und laufende Anträge eines Mitarbeiters (hier der Demo-Arzt Dr. Daniel Wagner, angezeigt über die auditierte Superadmin-Funktion „Mitarbeiter wechseln“, erkennbar am orangen Banner). „Änderung beantragen“-Buttons machen jede Korrektur zum dokumentierten Antrag.

Jeder Mitarbeiter sieht seine konsolidierten **HR-Datensätze** und Organisationsdaten, seinen eigenen **Rotationsplan** (Kapitel 8) und seine laufenden Anträge. Fehler im Profil — veraltete Telefonnummer, falsche Funktionsbezeichnung — meldet er direkt aus der Seite heraus; ein Review-Workflow prüft die Änderung, bevor sie in die Systeme fließt. Die konfigurierbare Profil-Zuordnung verknüpft das Portal-Login zuverlässig mit dem richtigen Mitarbeiter-Datensatz — auf Wunsch mit Doppelprüfung gegen AD und ORBIS.

15.2 Rechte selbst beantragen — sofort oder über den Vorgesetzten



Meine Berechtigungen — die Selbstauskunft: jeder Mitarbeiter sieht jederzeit seine zugewiesenen Rollen und Rechte. Transparenz ist die Voraussetzung für Eigenverantwortung — und nebenbei ein Stück gelebtes DSGVO-Auskunftsrecht.

Aus dem kuratierten Katalog beantragt der Mitarbeiter zusätzliche Berechtigungen selbst. Je nach Eintrag gilt: **Sofort-Vergabe** (für unkritische Rechte — die IT wird komplett entlastet), **Vorgesetzten-Genehmigung**, Vier-Augen-Modus oder vorläufige Vergabe mit nachgelagerter Prüfung. Begründungspflicht, Datenschutzhinweis, Gültigkeitsbegrenzung und Sperrfrist nach Ablehnung sind eingebaut.

15.3 Die Leitplanken: Freiheit, die sich selbst kontrolliert

DAS PRINZIP

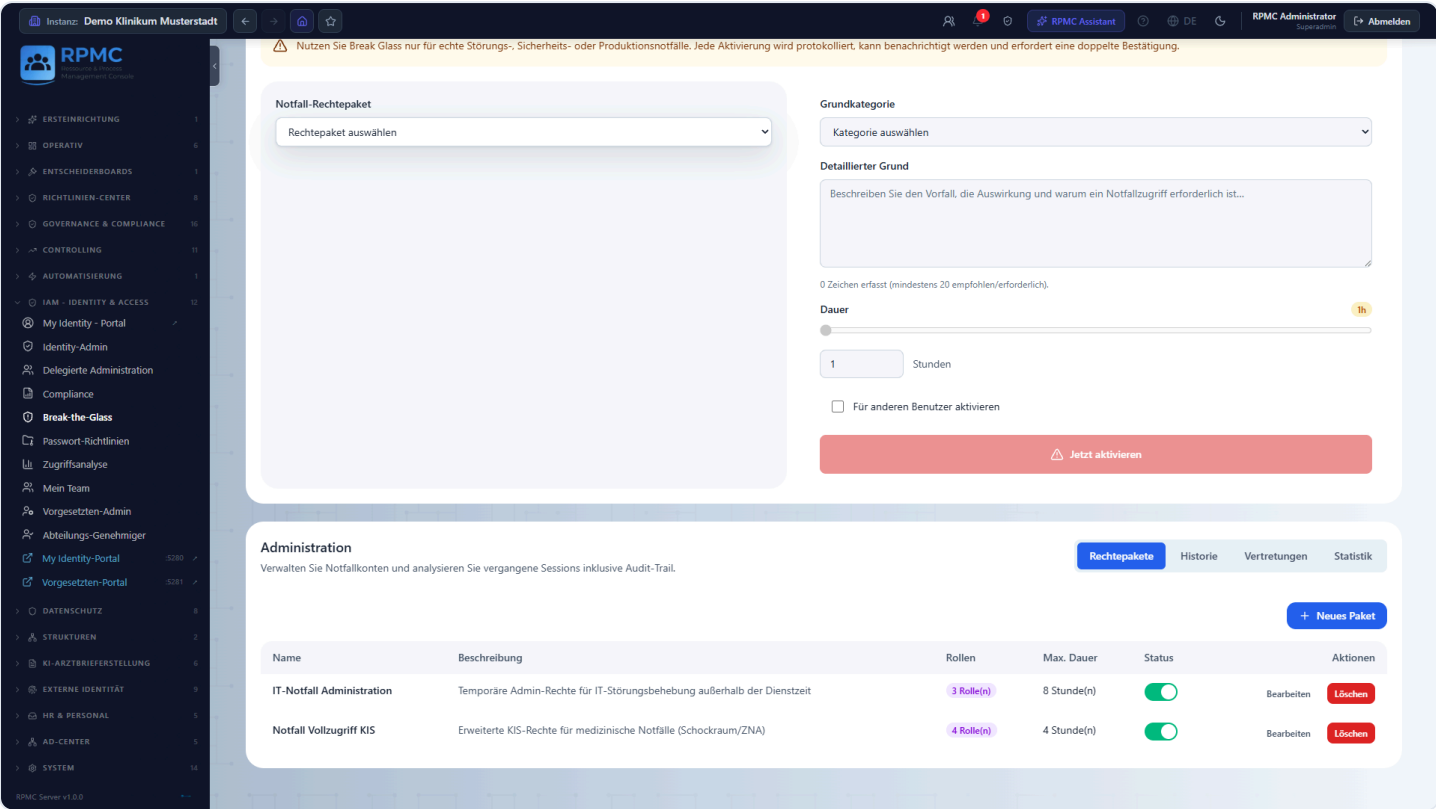
Maximale Freiheit für IT und Anwender — trotzdem strikt auditierbar. Möglich machen es drei Mechanismen, die jede Selbst-Vergabe automatisch wieder einfangen:

- **Zusatzrechte werden immer rezertifiziert:** Jedes selbst beantragte Recht landet automatisch im Rezertifizierungs-Zyklus. Der Mitarbeiter (oder sein Vorgesetzter) muss den fortbestehenden Bedarf periodisch bestätigen.
- **Automatischer Entzug bei Nichtmeldung:** Bleibt die Bestätigung aus und liegt das Recht außerhalb der Norm — die Norm sind die SETs des Richtlinien-Centers (Kapitel 11) —, wird es automatisch entzogen. Selbst vergebene Rechte können also niemals dauerhaft „hängenbleiben“.
- **Lückenlose Attribution:** Zu jedem Recht ist jederzeit sichtbar: *wer* es hat, *was* es umfasst, *wieso* es vergeben wurde (Begründung) und *durch wen* (Genehmiger oder Sofort-Vergabe-Regel) — für Mitarbeiter, Vorgesetzte, IT und Prüfer gleichermaßen.

FALLBEISPIEL

Eine MTA beantragt für ein Forschungsprojekt lesenden Zugriff auf ein Zusatzmodul — Sofort-Vergabe, null IT-Aufwand. Sechs Monate später endet das Projekt; die Rezertifizierungs-Anfrage bleibt unbeantwortet. Da das Recht außerhalb ihres Pflege-SETs liegt, entzieht RPMC es automatisch und dokumentiert den Vorgang. Ergebnis: volle Flexibilität im Projekt, keine Berechtigungs-Leiche danach — und niemand musste daran denken.

15.4 Break-the-Glass: der kontrollierte Notfallzugriff



Break-Glass — Notfall-Rechteerweiterung — das Aktivierungs-Formular (Rechtepaket, Grundkategorie, Grund, Dauer) und die Administration mit zwei konfigurierten Rechtepaketen: „IT-Notfall Administration“ (3 Rollen, max. 8 h) und „Notfall Vollzugriff KIS“ (4 Rollen, max. 4 h) — jeweils mit Status-Schaltern, Historie und Vertretungsregeln.

Im medizinischen Notfall zählt Geschwindigkeit: Break-the-Glass erhebt Rechte zeitlich begrenzt per Selbstaktivierung — mit Pflicht-Begründung und Doppelbestätigung. Gleichzeitig feuern SIEM-Ereignis hoher Dringlichkeit und E-Mail-Alarm; ein Ablauf-Worker entzieht die Rechte automatisch. Hybrid-Provisioning sorgt dafür, dass der Zugriff auch bei vorübergehend nicht erreichbarem ORBIS funktioniert. Am Folgetag prüft die IT-Sicherheit jede Session: wer, wann, warum, welche Rechte, wann entzogen.

15.5 Delegated Admin & Flow Analytics

- **Delegated Admin:** Abteilungs- und Stationsleitungen verwalten ausschließlich ihren eigenen Bereich — Anträge genehmigen, Team einsehen, Rezertifizierungen bearbeiten — ohne globale Admin-Rechte. Mandantentrennung bis auf OE-Ebene.
- **Flow Analytics:** Antragswege werden messbar — Durchlaufzeiten, Genehmigungsquoten, Engpässe je Schritt. Der Self-Service optimiert sich datenbasiert weiter, statt auf Zuruf.

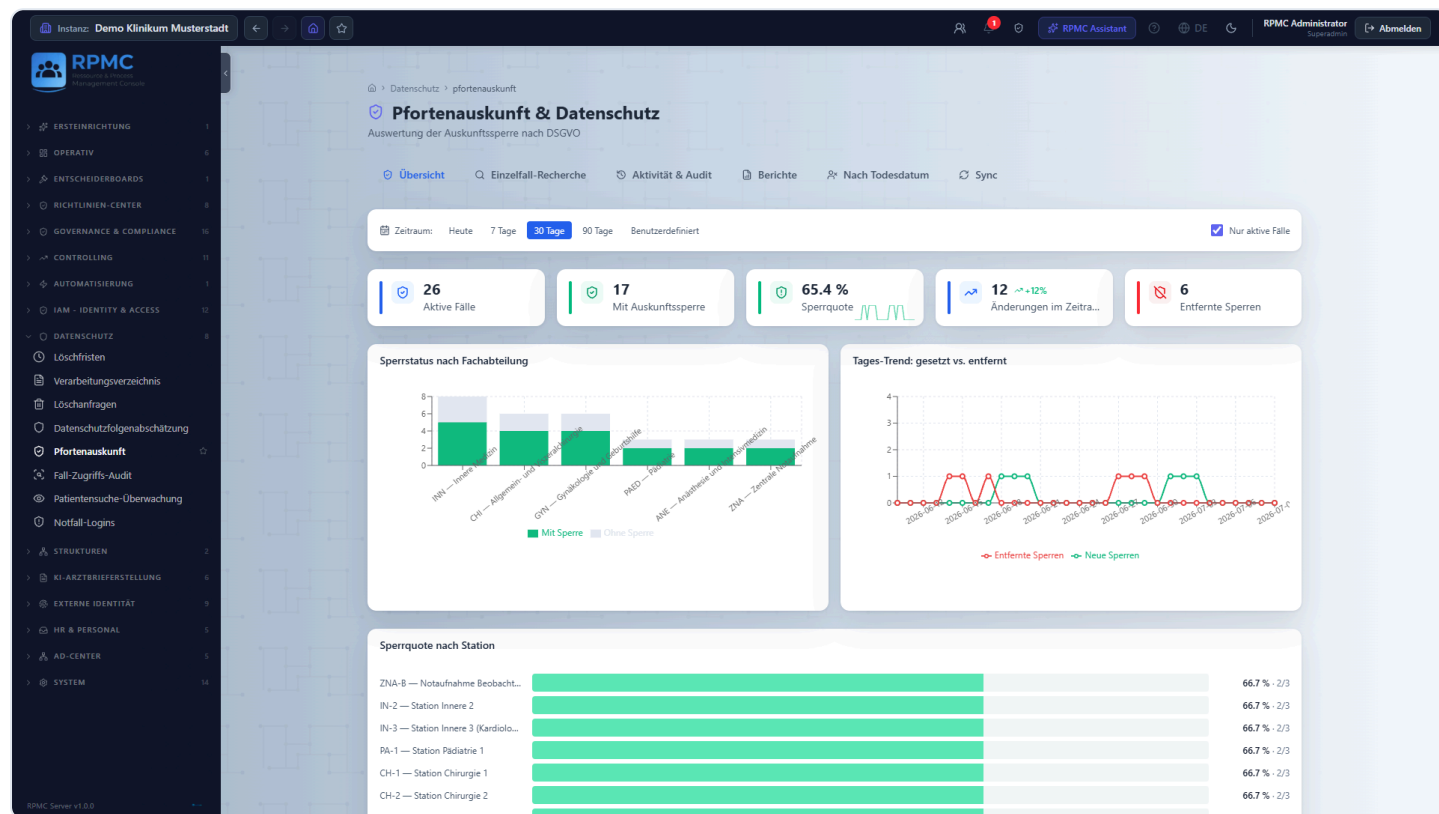
RETURN ON INVEST

Jeder Rechte-Antrag, der nicht als Ticket bei der IT landet, spart im Schnitt 15–30 Minuten Bearbeitungszeit. Bei einem Haus mit 2.000 Mitarbeitern und üblichen Antragsvolumina entlastet der Self-Service die IT um mehrere Personentage pro Monat — bei gleichzeitig besserer, nicht schlechterer Audit-Lage. Genau diese Kombination können klassische IAM-Systeme nicht: Dort bedeutet Self-Service fast immer Kontrollverlust oder Workflow-Bürokratie.

Datenschutz-Suite — jedes Werkzeug im Detail RELEASED

Der Datenschutz-Bereich ist die Werkbank des Datenschutzbeauftragten: sechs eigenständige Werkzeuge, die reale DSGVO-Pflichten nicht dokumentieren, sondern erledigen. Jedes Werkzeug hier einzeln — mit Beispiel und Nutzen.

16.1 Pfortenauskunft & Auskunftssperre

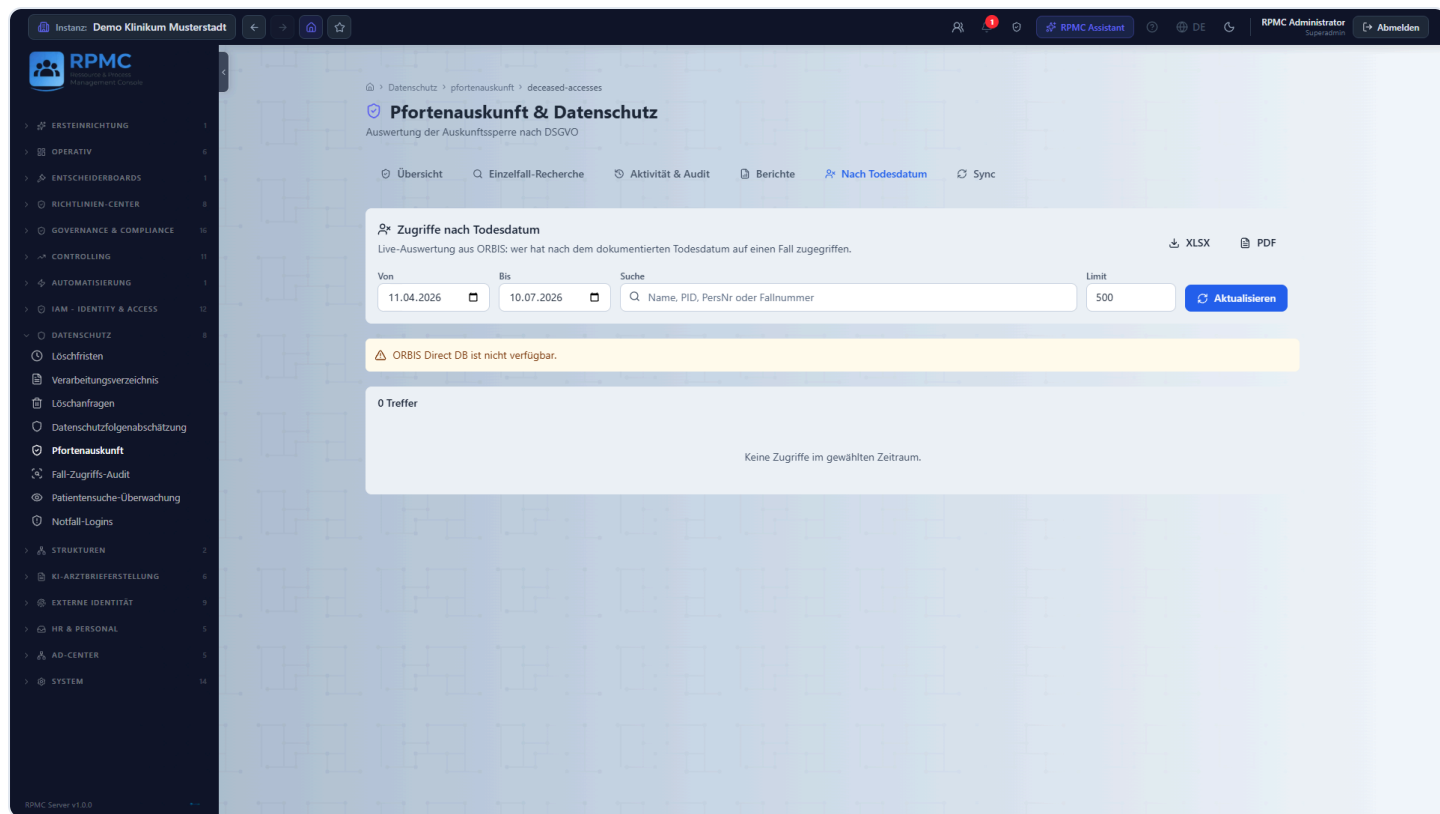


Pfortenauskunft-Dashboard — KPI-Zeile (26 aktive Fälle, 17 mit Auskunftssperre, 65,4 % Sperrquote), Sperrstatus nach Fachabteilung, Tages-Trend und Sperrquote je Station als Heatmap.

Patienten haben das Recht, dass ihre Anwesenheit im Haus nicht preisgegeben wird (Auskunftssperre). Die Pforte muss das zuverlässig wissen — in der Praxis eine ständige Fehlerquelle. RPMC spiegelt die Sperr- und Fallinformationen aus ORBIS, überwacht Quoten je Station und Fachabteilung und macht Ausreißer sichtbar (eine Station mit auffällig niedriger Sperrquote deutet auf Erfassungslücken hin).

Beispiel: Ein Prominenter wird stationär aufgenommen. Das Dashboard zeigt: Sperre aktiv, Pforten-Sicht korrekt. Zwei Tage später ruft eine „besorgte Angehörige“ an — die Pforte gibt korrekt keine Auskunft; der Datenschutz kann die durchgängige Sperre lückenlos belegen.

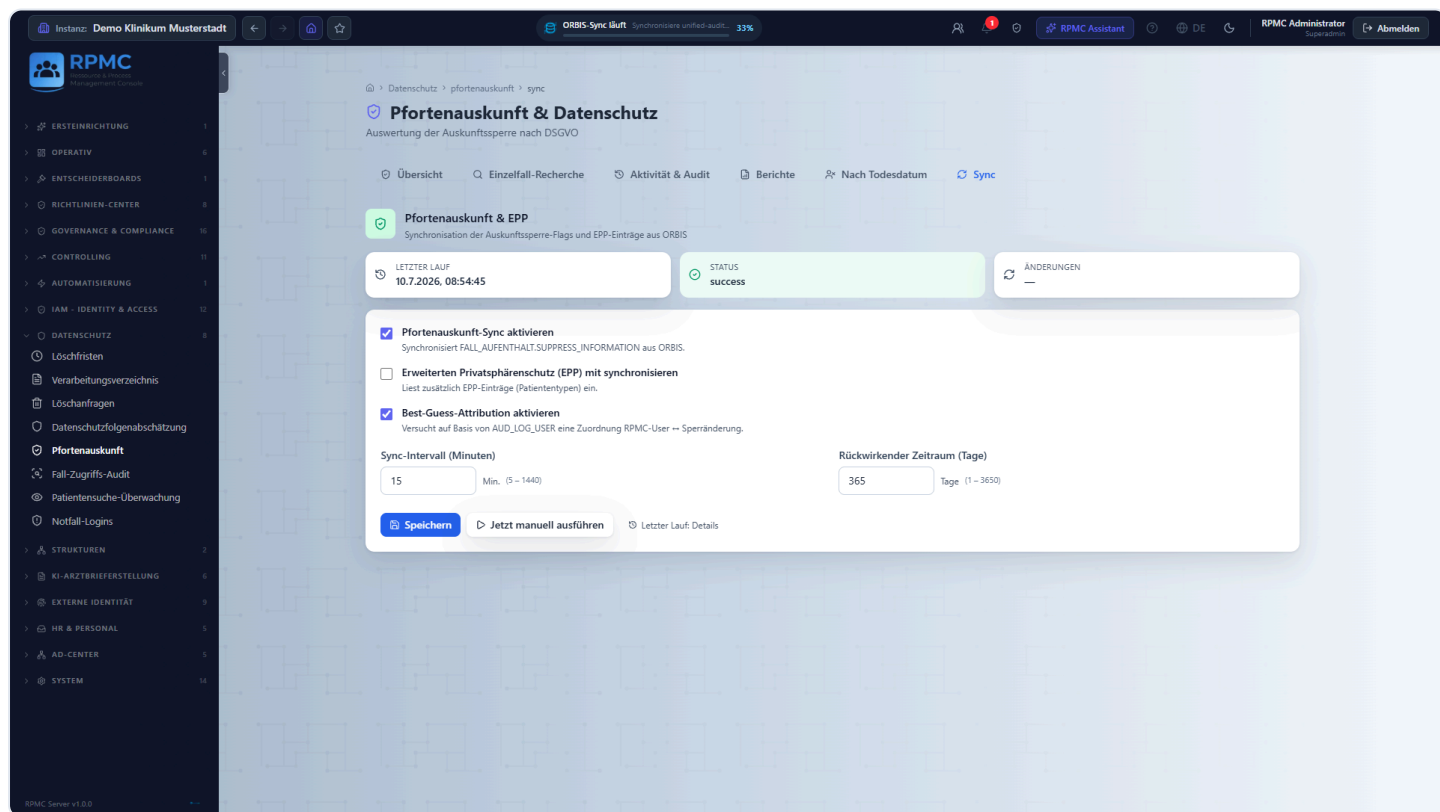
Nutzen: Die Auskunftssperre wird vom Zufallsprodukt zur überwachten Kennzahl — und der DSB bekommt erstmals ein Echtzeit-Bild statt Stichproben.



Reiter „Nach Todesdatum“ — Auswertung der Sperren und Fälle nach Todesdatum: Auch postmortale Persönlichkeitsrechte und Presse-Anfragen zu Verstorbenen werden kontrolliert behandelt.

Beispiel: Nach dem Tod eines Patienten fragt eine Lokalredaktion an. Die Nach-Todesdatum-Sicht zeigt: Sperre bestand und besteht fort — die Auskunftsverweigerung ist dokumentiert rechtssicher.

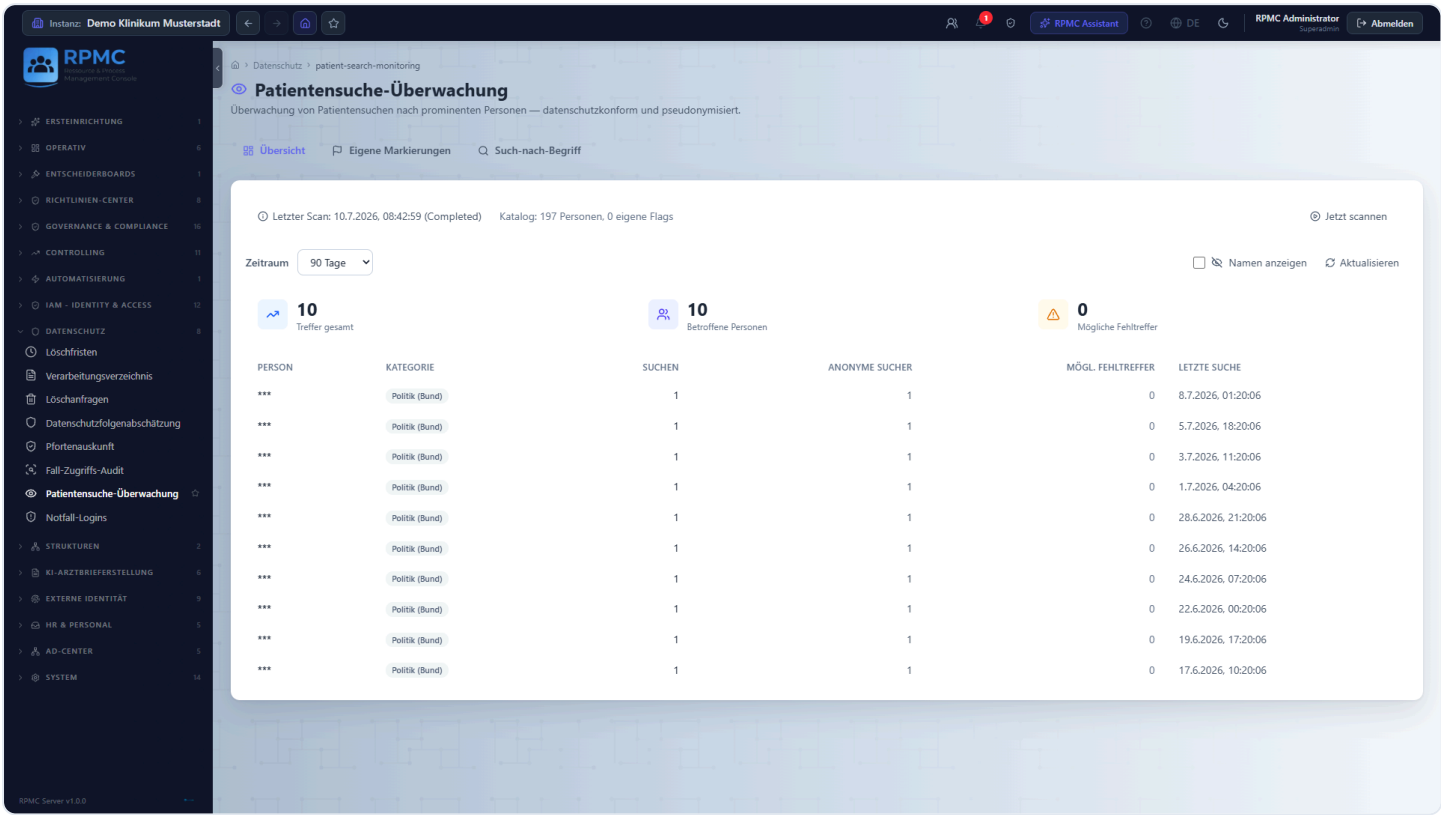
Nutzen: Ein regelmäßig übersehener Graubereich (Sperren Verstorbener) wird systematisch verwaltet statt fallweise improvisiert.



Reiter „Sync“ — Synchronisation der Sperr-Flags aus ORBIS mit letztem Lauf, Intervall, Attributions-Logik und manuellem Sofort-Lauf. Der DSB sieht nicht nur die Daten, sondern auch deren Frische.

Beispiel: Vor dem Wochenende stößt der DSB manuell einen Sync an und verifiziert: letzter Lauf erfolgreich, Datenstand aktuell.
Nutzen: Vertrauen in die Datengrundlage ist selbst prüfbar — ein oft übersehener Baustein der Rechenschaftspflicht (Art. 5 Abs. 2 DSGVO).

16.2 Patientensuche-Überwachung (VIP-/Personenschutz)



Patientensuche-Überwachung — Status-Panel mit letztem Scan (Completed, Katalog: 197 Personen), „Jetzt scannen“-Button und pseudonymisierter Treffer-Tabelle (10 Treffer, Kategorie Politik).

Der Strict-Match kann Vornamen und Geburtsdatum einbeziehen, um gleichnamige Personen besser zu unterscheiden. Das Scan-Panel zeigt Katalogstand und letzten Lauf; Treffer können pseudonymisiert weiterbearbeitet werden.

Beispiel: Ein Landespolitiker liegt auf der Inneren. Der Nacht-Scan meldet drei Suchanfragen aus Abteilungen ohne Behandlungsbezug. Der DSB deckt die pseudonymisierten Treffer nach dokumentierter Begründung auf und leitet ein Klärungsverfahren ein.
Nutzen: Neugier-Zugriffe — das häufigste reale Datenschutz-Delikt im Krankenhaus — werden systematisch erkannt, und zwar datenschutzkonform: pseudonymisiert, begründungspflichtig, auditiert.

16.3 Fall-Zugriffs-Audit (Forensik)

Instanz: Demo Klinikum Musterstadt

RPMC Administrator

Fallnummer Patienten-ID Mitarbeiter

Fallnummer: z. B. 1234567 Von (Datum): tt.mm.jjjj Bis (Datum): tt.mm.jjjj Limit (optional): Server-Defau

Zeitraum: 30 Tage 92 Tage 180 Tage 365 Tage

Laden

Fallnummer eingeben

Geben Sie eine Fallnummer ein und klicken Sie auf „Laden“, um das forensische Zugriffsprotokoll anzuzeigen.

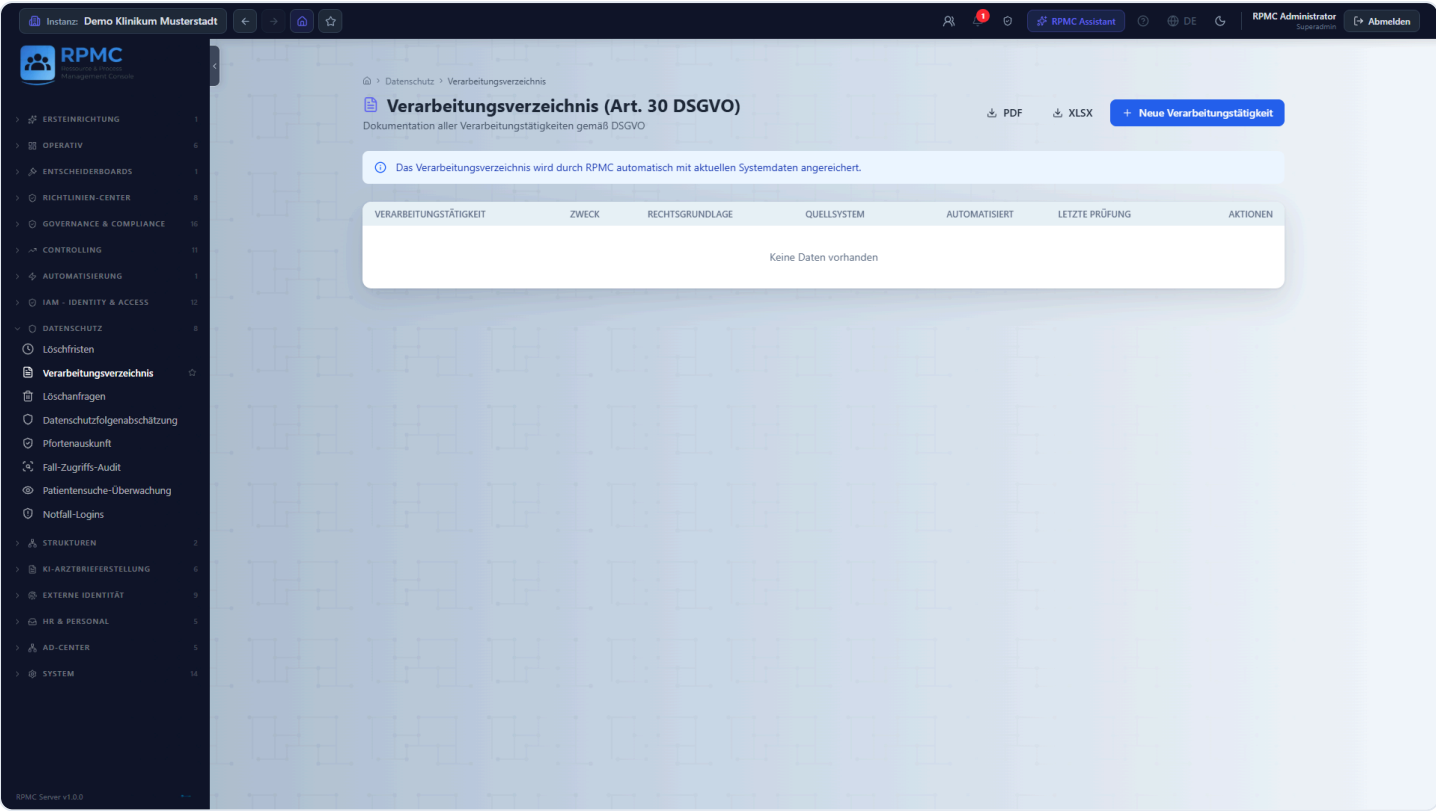
Fall-Zugriffs-Audit — forensische Suchmaske nach Fallnummer, Patienten-ID oder Mitarbeiter mit Zeitfenster-Presets. Das Zugriffsprotokoll wird live aus ORBIS gelesen — konzeptbedingt zeigt die Maske ohne Fallnummer keine Daten.

Bei Beschwerde oder Verdacht rekonstruiert das Fall-Zugriffs-Audit lückenlos, wer wann auf einen konkreten Fall zugegriffen hat — inklusive Kontext (reguläre Behandlung, Konsil, Notfallzugriff). Die Auswertung läuft live gegen die ORBIS-Protokolle; nichts wird auf Vorrat kopiert.

Beispiel: Eine Patientin beschwert sich, ihr Ex-Partner (Klinik-Mitarbeiter) habe ihre Akte gelesen. Fallnummer eingeben, Zeitraum wählen: Der Zugriff ist belegt, samt Datum, Arbeitsplatz und fehlendem Behandlungsbezug — die Grundlage für das arbeitsrechtliche Verfahren steht in fünf Minuten.

Nutzen: § 393 SGB V verlangt genau diese Auswertbarkeit; RPMC liefert sie als Werkzeug statt als SQL-Projekt. Vorhalte-Aufwand: null.

16.4 Verarbeitungsverzeichnis (VVT)

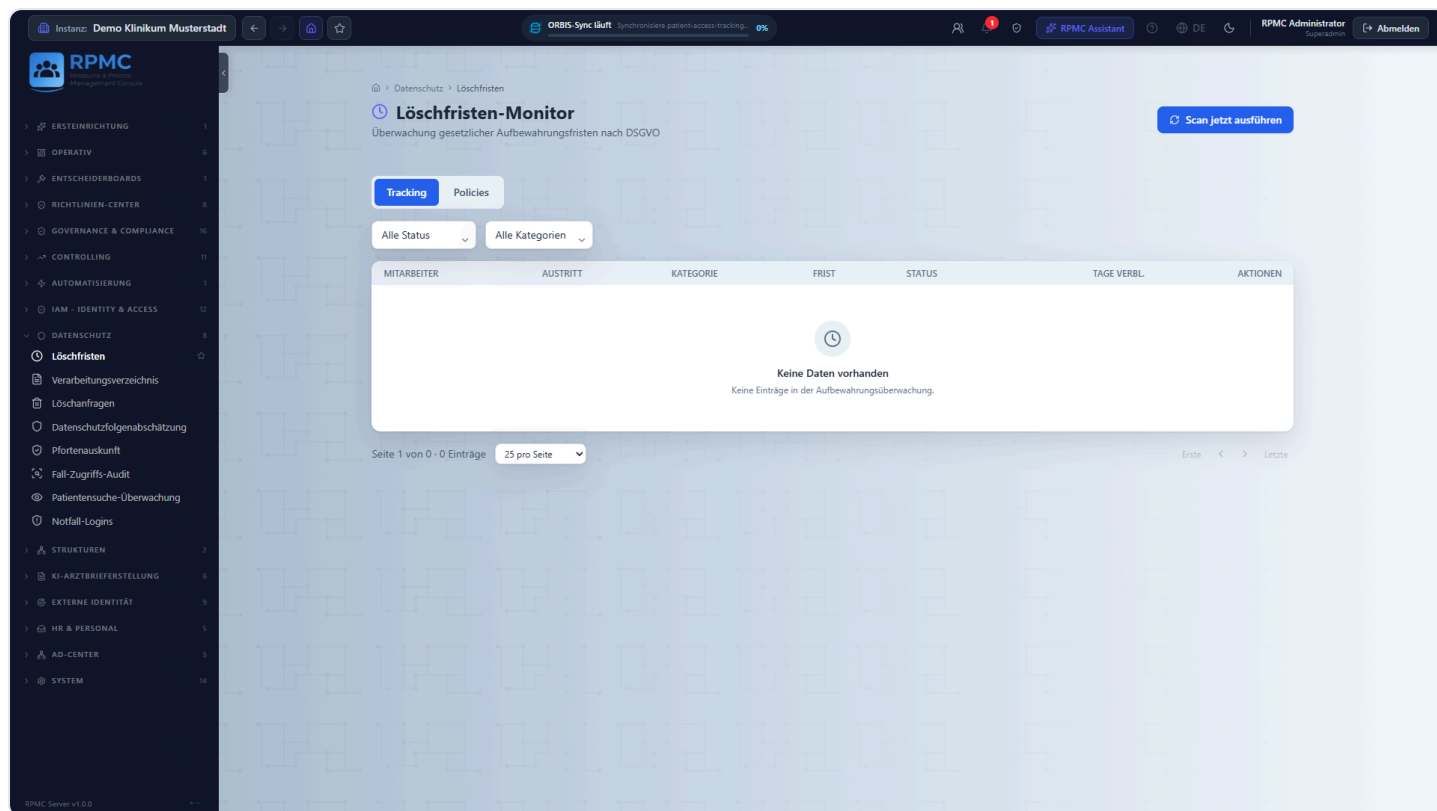


Verarbeitungsverzeichnis — die Verarbeitungstätigkeiten nach DSGVO Art. 30, direkt in RPMC gepflegt: Zweck, Kategorien, Empfänger, Fristen — versioniert und exportierbar.

Beispiel: Die Aufsichtsbehörde bittet um das aktuelle VVT. Statt eine verstreute Word-Sammlung zu konsolidieren, exportiert der DSB das gepflegte Verzeichnis — aktueller Stand, ein Dokument, fünf Minuten.

Nutzen: Das VVT lebt dort, wo die Verarbeitungen tatsächlich stattfinden — nahe an Modulen und Datenflüssen statt im Dateisystem-Nirwana.

16.5 Löschfristen-Verwaltung



Löschfristen — Aufbewahrungs- und Löschregeln je Datenkategorie: Frist, Rechtsgrundlage, Status. Speicherbegrenzung (Art. 5 Abs. 1 lit. e DSGVO) wird planbar statt anlassgetrieben.

Beispiel: Bewerberdaten sind nach sechs Monaten zu löschen, Behandlungsdaten nach 30 Jahren, Audit-Ereignisse je nach Kategorie unterschiedlich. Die Löschfristen-Verwaltung hinterlegt jede Kategorie mit Frist und Rechtsgrundlage und macht fällige Bestände sichtbar.

Nutzen: Die Frage „Warum existieren diese Daten noch?“ bekommt eine dokumentierte Antwort — bevor die Behörde sie stellt.

16.6 Patientenzugriffs-Audit (laufende Überwachung)

Ergänzend zur fallbezogenen Forensik wertet das Patientenzugriffs-Audit die ORBIS-Zugriffsprotokolle **täglich flächig** aus: Zugriffszahlen je Mitarbeiter und OE, Ausreißer-Erkennung, Zubringer für die Zugriffs-Analysen (Kapitel 13.3) und den Compliance-Score. So entsteht Prävention statt bloßer Aufarbeitung.

Beispiel: Ein Mitarbeiter der Verwaltung ruft binnen einer Woche 40 Akten ohne OE-Bezug auf. Der tägliche Lauf markiert das Muster, ein Prüf-Fall entsteht automatisch — Wochen bevor eine Beschwerde es ans Licht gebracht hätte.

Nutzen: Aus der gesetzlichen Protokollierungspflicht wird ein aktives Frühwarnsystem.

WAS KLASSISCHE IAM-SYSTEME HIER NICHT KÖNNEN

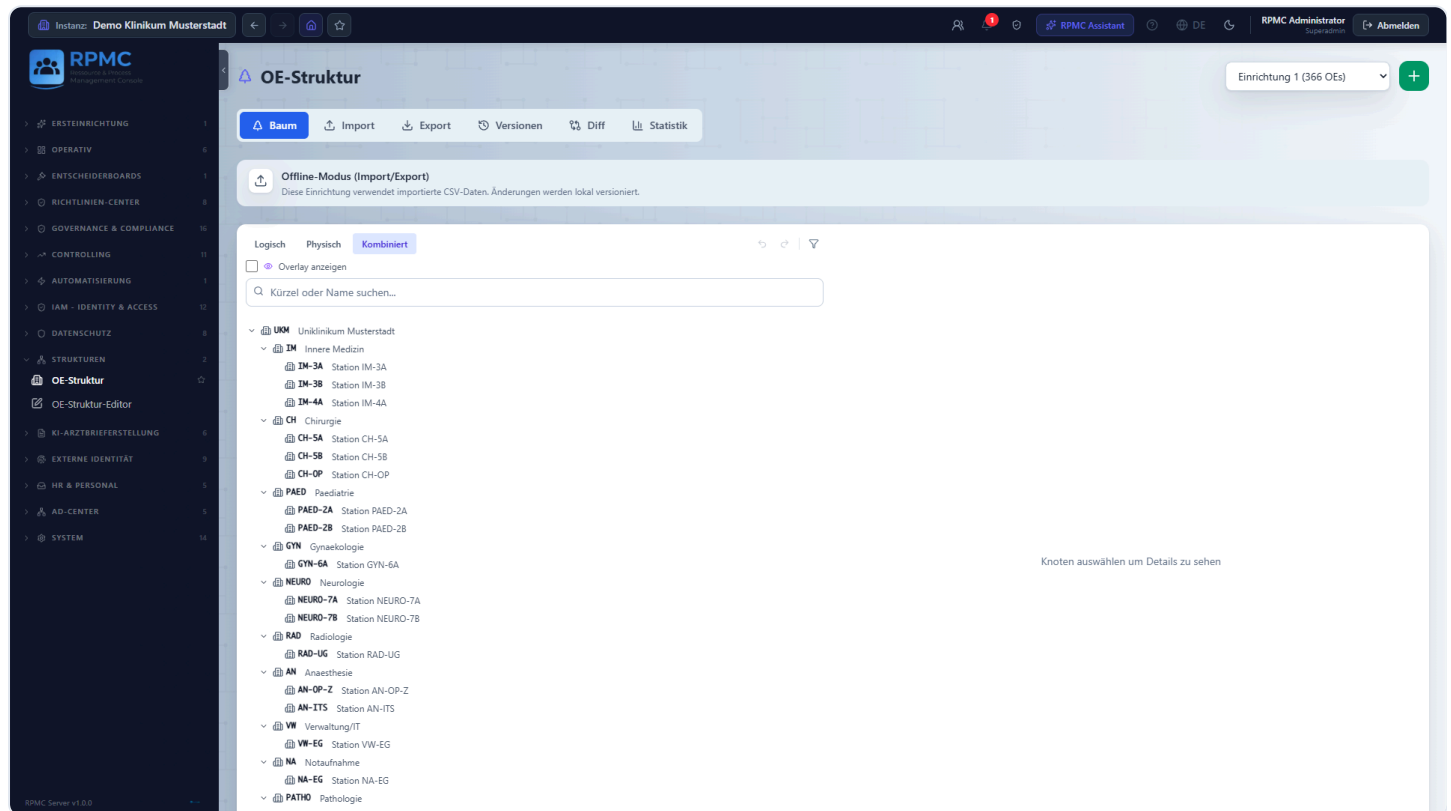
Auskunftssperren-Überwachung, VIP-Suchschutz, fallbezogene KIS-Forensik und tägliche Patientenzugriffs-Auswertung setzen tiefes ORBIS-Verständnis voraus — Tabellen, Ereignistypen, Notfall-Semantik. Generische Werkzeuge besitzen dieses Wissen nicht; RPMC liefert es als fertige, vom DSB selbst bedienbare Suite.

Strukturen — OE-Baum, Editor, Notfall-OE-Automatik

RELEASED

Die Organisationsstruktur ist das Rückgrat jeder Berechtigungs-Entscheidung. RPMC bildet sie originalgetreu ab — als lebendes Modell mit Editor, Versionierung und einer Automatik, die Notfallbereiche selbstständig erkennt.

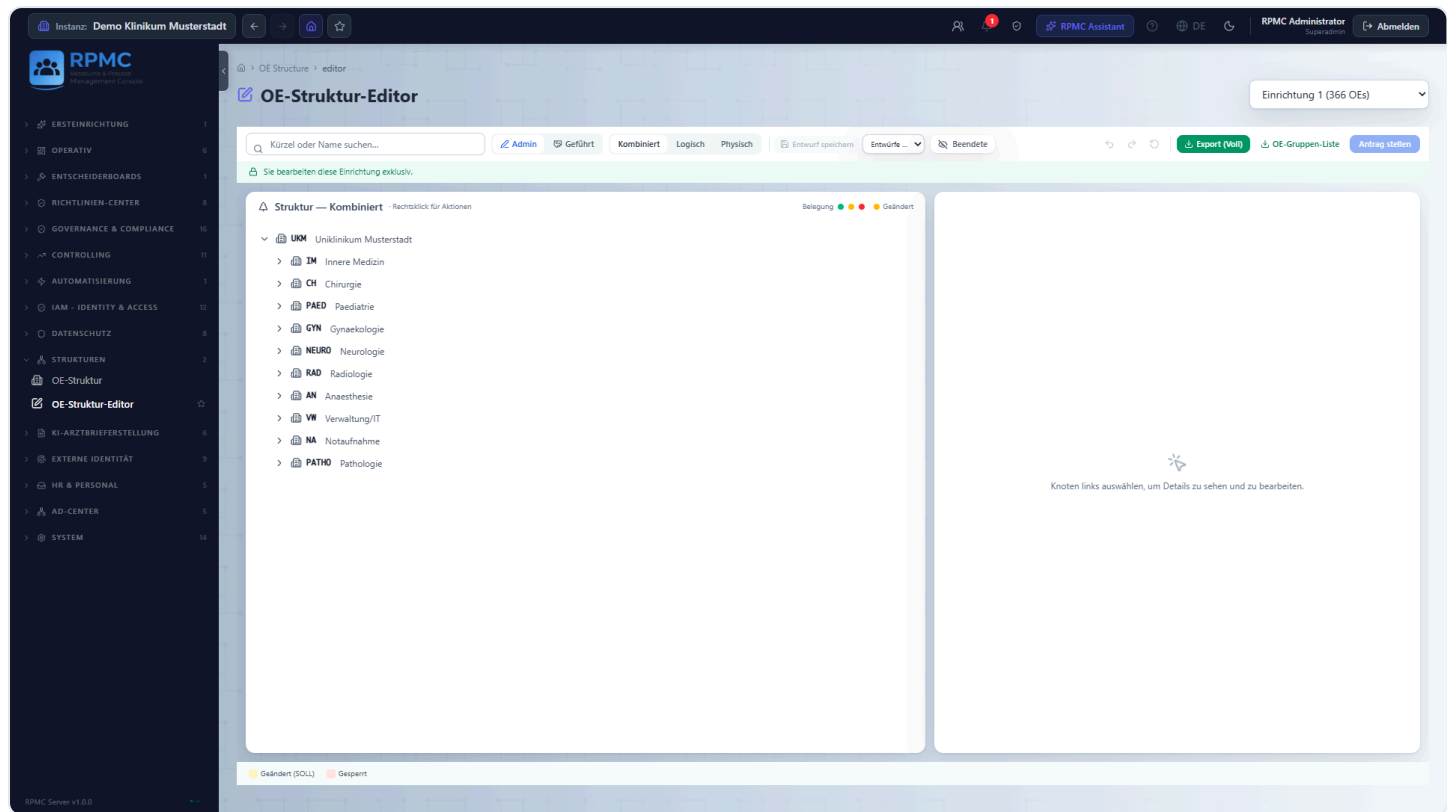
17.1 Der Live-OE-Baum



OE-Struktur (Live-Baum) — das Klinikum mit Fachabteilungen und Stationen (366 OEs), umschaltbar zwischen logischer, physischer und kombinierter Sicht; Import, Export, Versionen, Diff und Statistik direkt am Baum.

Der Live-Baum zeigt die ORBIS-Organisationsstruktur mit allen Krankenhaus-Typen (Klinik, Fachabteilung, Station, Funktionsbereich, OP, ICU, Gebäude, Etage, Raum ...) — logisch und physisch. Versionierung und Diff machen jede Strukturänderung vergleichbar: Was hat sich zwischen Januar und Juli geändert? Ein Klick.

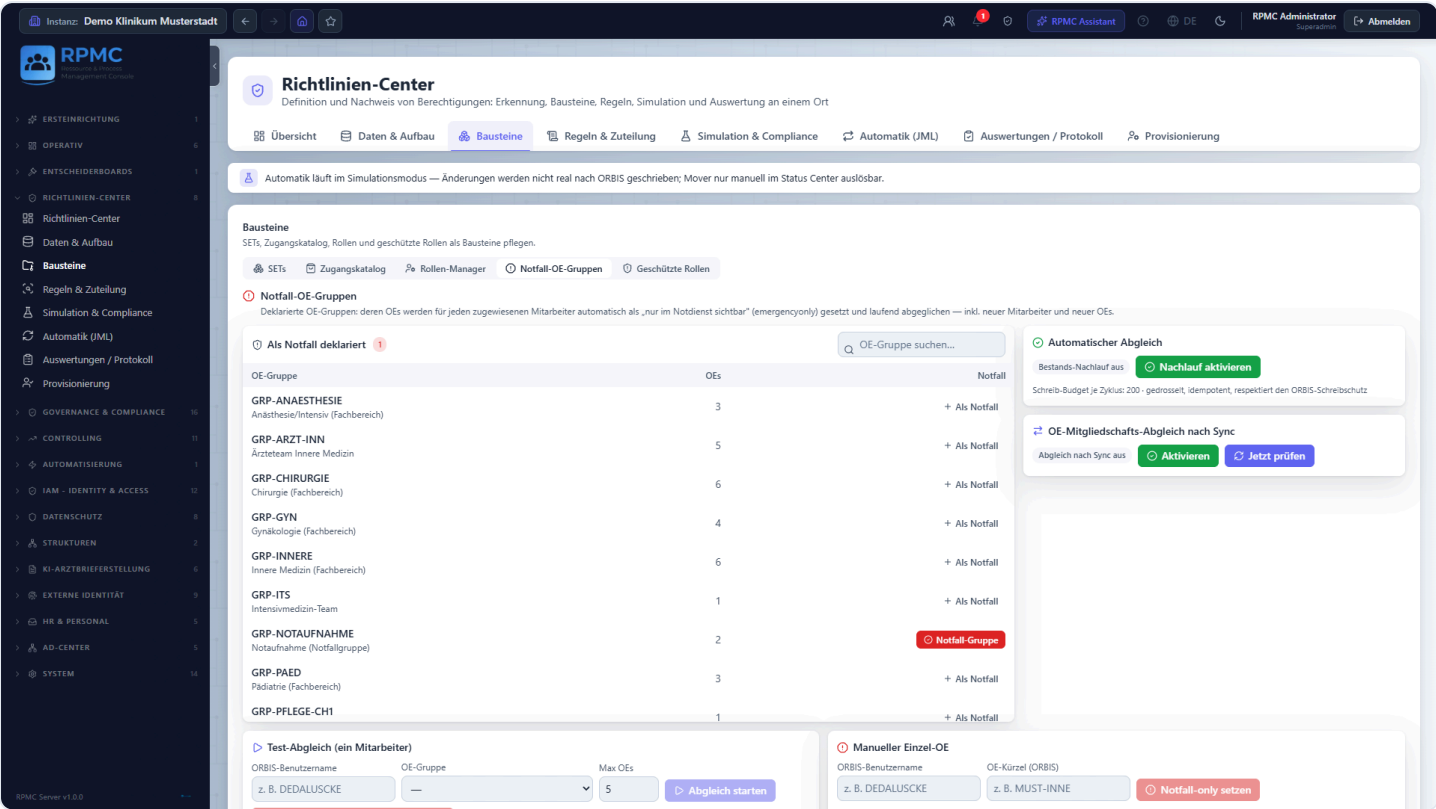
17.2 Der OE-Struktur-Editor



OE-Struktur-Editor — exklusive Bearbeitungssperre (kein gegenseitiges Überschreiben), Admin- und geführter Modus, Entwurfs-Verwaltung, Voll-Export und OE-Gruppen-Liste mit Details-Panel.

Strukturänderungen entstehen als **Entwürfe**: Der Editor sperrt exklusiv, führt wahlweise im Admin- oder im geführten Modus (für Antragsteller ohne Strukturwissen — die Basis des OE-Entscheidungsboards, Kapitel 10) und exportiert fertige Strukturen für die ORBIS-Pflege und die Dokumentation. Soll-Ist-Abgleiche zeigen, wo die gelebte ORBIS-Struktur vom beschlossenen Modell abweicht.

17.3 Notfall-OE-Automatik



Notfall-OE-Gruppen — definierte Gruppen werden mit dem fachlichen Notfallstatus auf OE-Ebene abgeglichen. Test- und kontrollierter Produktivabgleich machen Abweichungen vor der Übernahme sichtbar.

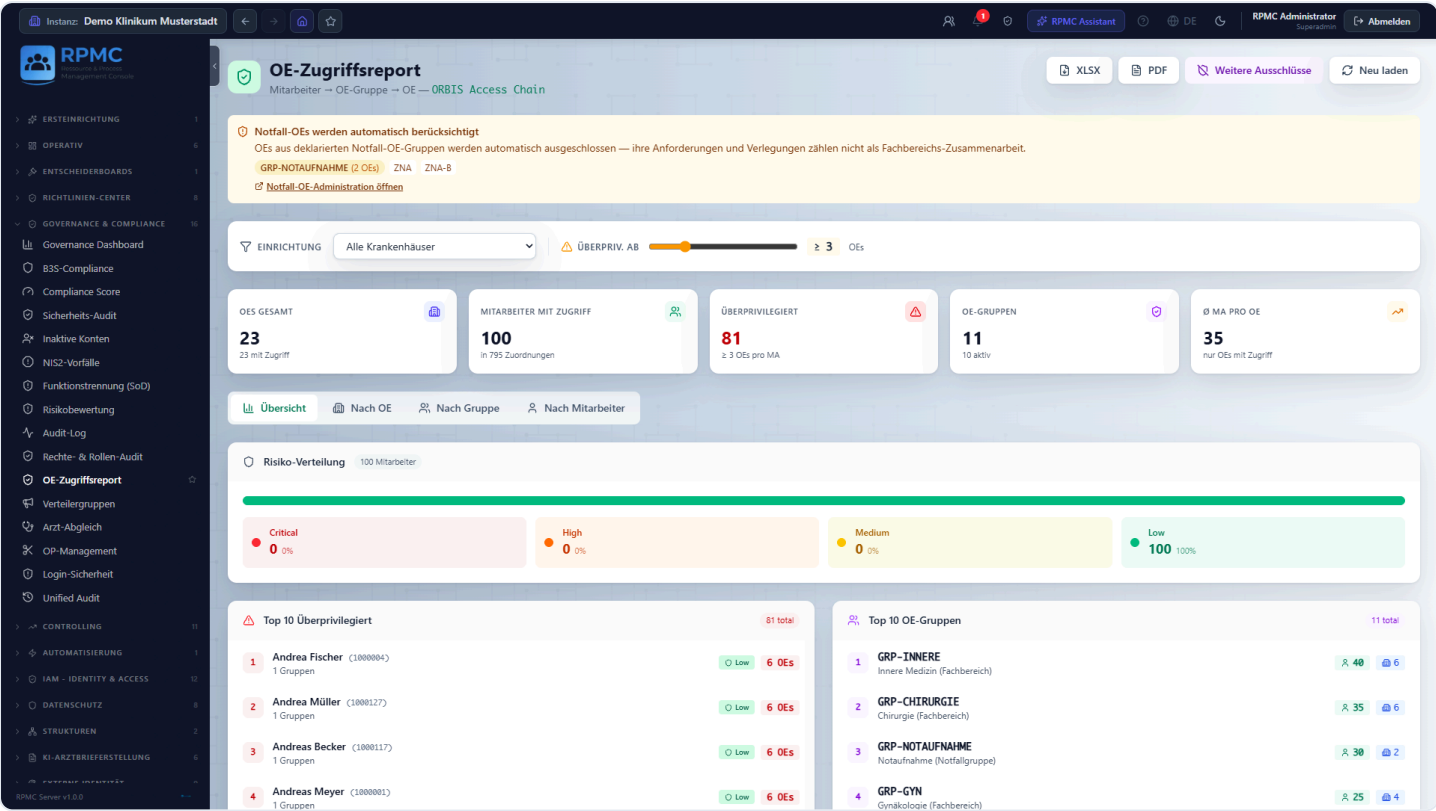
Die reine Mitgliedschaft einer OE in einer Notfall-OE-Gruppe setzt in angebundenen Verwaltungswegen nicht zwingend zugleich den fachlichen Notfallstatus auf OE-Ebene. Dadurch können OEs trotz Gruppenzuordnung weiterhin als normale OEs hinterlegt bleiben.

RPMC verwaltet den Notfallstatus auf OE-Ebene und gleicht ihn automatisch mit definierten Notfall-OE-Gruppen ab. Wird in ORBIS eine neue OE zu einer solchen Gruppe hinzugefügt und die Kennzeichnung vergessen, erkennt RPMC die Abweichung und kann den vorgesehenen Notfallstatus im kontrollierten Abgleich nachziehen.

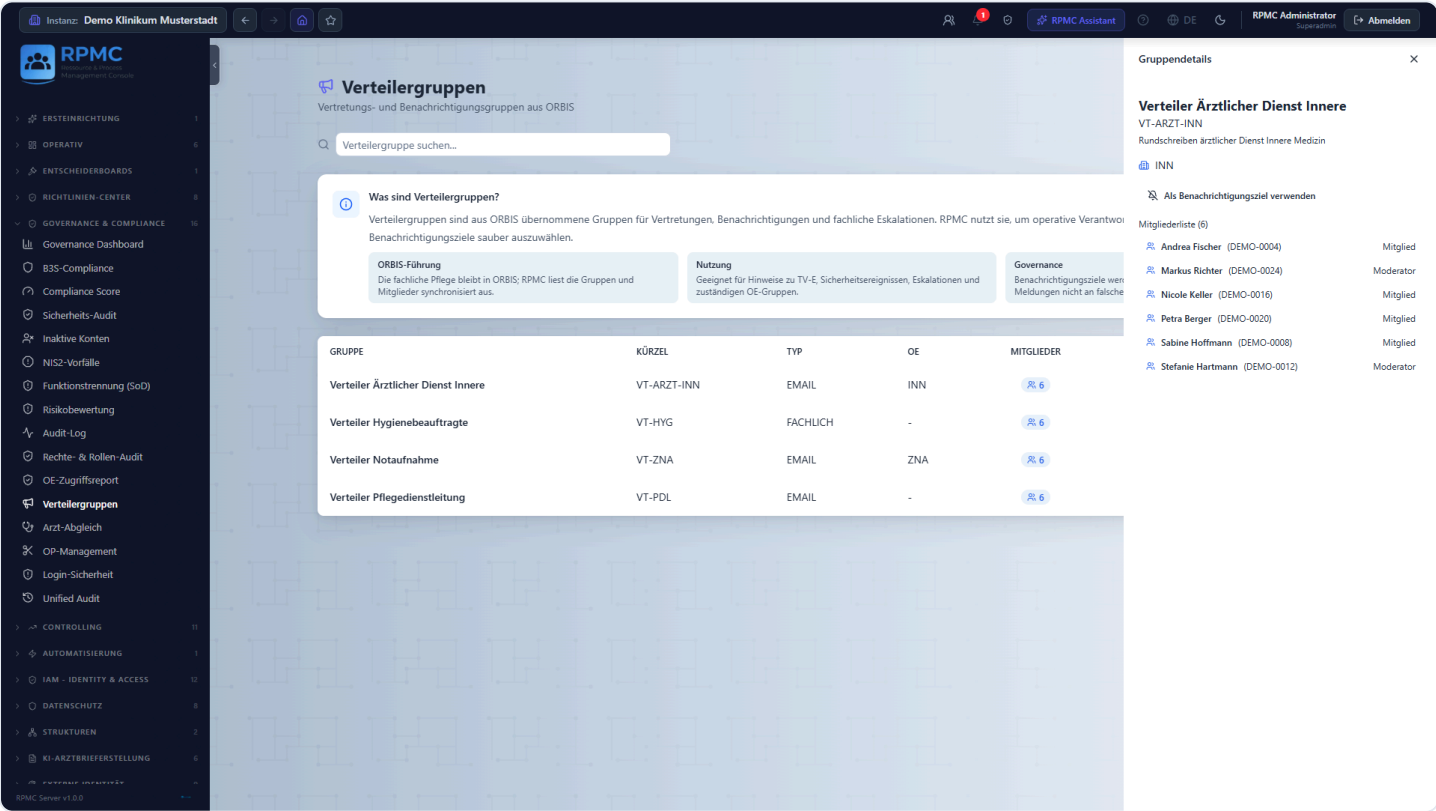
NUTZEN

Neue Gruppenmitgliedschaften werden nicht nur als normale OE-Zuordnung übernommen; die fachliche Notfallkennzeichnung bleibt konsistent und für nachgelagerte Auswertungen verfügbar.

17.4 OE-Zugriffsreport & Verteilergruppen



OE-Zugriffsreport — „Wer hat Zugriff auf was“: Mitarbeiter-Zugriffe je OE und Station, als Bericht für Leitungen und Prüfer.



Verteilergruppen — vier in ORBIS geführte Gruppen (u. a. Ärztlicher Dienst Innere, Hygiene, ZNA, PDL mit je 6 Mitgliedern); das geöffnete Detail-Panel zeigt die Mitgliederliste inklusive Rollen (Mitglied/Moderator). Verteilerpflege wird sichtbar und auditierbar statt ORBIS-Geheimwissen.

Arzt-Abgleich mit LANR-Konsolidierung RELEASED

Fehlerhafte Arztnummern kosten bares Geld: Ohne korrekte LANR (lebenslange Arztnummer) scheitern Abrechnungen, Arztbriefe tragen falsche Signaturen, KV-Meldungen laufen ins Leere. Der Arzt-Abgleich macht ORBIS- und HR-Arztdata deckungsgleich.

Instanz: Demo Klinikum Musterstadt

RPMC Administrator

Abmelden

RPMC

Management Console

ERSTENRICHTUNG

OPERATIV

ENTSCHEIDERBOARDS

RICHTLINIEN-CENTER

GOVERNANCE & COMPLIANCE

Governance Dashboard

B3S-Compliance

Compliance Score

Sicherheits-Audit

Inaktive Konten

NIS2-Vorfälle

Funktionstrennung (SoD)

Risikobewertung

Audit-Log

Rechte- & Rollen-Audit

OE-Zugriffsreport

Verteilerguppen

Arzt-Abgleich

OP-Management

Login-Sicherheit

Unified Audit

CONTROLLING

AUTOMATISIERUNG

IAM - IDENTITY & ACCESS

DATENSCHUTZ

STRUKTUREN

KI-ARZTBRIEFERSTELLUNG

Arzt-Abgleich

LANR, KH-Arztnummer, Fachgruppe, Anschrift, Stempel und HR-Abgleich

14

Ärzte gesamt

0

Teams

6

Fachrichtungen

Ärzte

Ärzte Prüfliste

Teams

Read-only-Abgleich der LANR aller Ärzte gegen den Fachgruppencode-Katalog. Es wird nichts nach ORBIS geschrieben — Korrekturen erfolgen gezielt in ORBIS. Gruppierung nach ORBIS-Einrichtung; der HR-Import ist das führende System für die LANR.

Alle Einrichtungen

Name, Kürzel oder LANR...

HR-Spalten

ORBIS-Pflege

Export (CSV)

Alle

Verifiziert

ORBIS abweichend

Fehlt in ORBIS

Fehlt im HR

HR nicht konsolidierbar

LANR fehlt

LANR ungültig

Fachgruppe ungültig

Adressmaske fehlt

ADREMA fehlt

14 Ärzte - 14 mit Auffälligkeit

NAME	TYP	LANR ORBIS	LANR (HR)	KHANR (HR)	FACHGRUPPE (HR)	KONSOLIDIERTE LANR	ABGLEICH	STATUS
Demo Klinikum Musterstadt 14 Ärzte 14 Auffälligkeiten								
Brandt, Oliver OBRANDT	Assistenzarzt	421234512	—	—	—	fehlt in HR	fehlt im HR	OK
König, Wolfgang WKOENIG	Chefarzt	421234502	—	—	—	fehlt in HR	fehlt im HR	OK
Lange, Andreas ALANGE	Assistenzarzt	fehlt in ORBIS	—	—	—	fehlt in HR	beidseitig fehlend	LANR fehlt
Meier, Thomas TMEIER	Assistenzarzt	421234510	—	—	—	fehlt in HR	fehlt im HR	OK
Meyer, Andreas DEMO-0001	Stationsarzt	421234513	—	—	—	fehlt in HR	fehlt im HR	OK
Müller, Markus MMUELLER	Facharzt	421234505	—	—	—	fehlt in HR	fehlt im HR	OK
Neumann, Jürgen JNEUMANN	Facharzt	421234509	—	—	—	fehlt in HR	fehlt im HR	OK
Schmidt, Sabine SSCHMIDT	Oberarzt	fehlt in ORBIS	—	—	—	fehlt in HR	beidseitig fehlend	LANR fehlt
Schröder, Frank FSCHROEDER	Chefarzt	421234501	—	—	—	fehlt in HR	fehlt im HR	OK
Stein, Vera VSTEIN	Facharzt	421234508	—	—	—	fehlt in HR	fehlt im HR	OK
Wagner, Daniel DWAGNER	Facharzt	fehlt in ORBIS	—	—	—	fehlt in HR	beidseitig fehlend	LANR fehlt

Ärzte-Prüfliste — der lesende LANR-Abgleich ORBIS vs. HR mit Ampel-Chips („fehlt in ORBIS“, „fehlt im HR“, „LANR fehlt“), Filter-Chips und Gruppierung nach Einrichtung (hier 14 Ärzte, 14 Auffälligkeiten im Demo-Bestand).

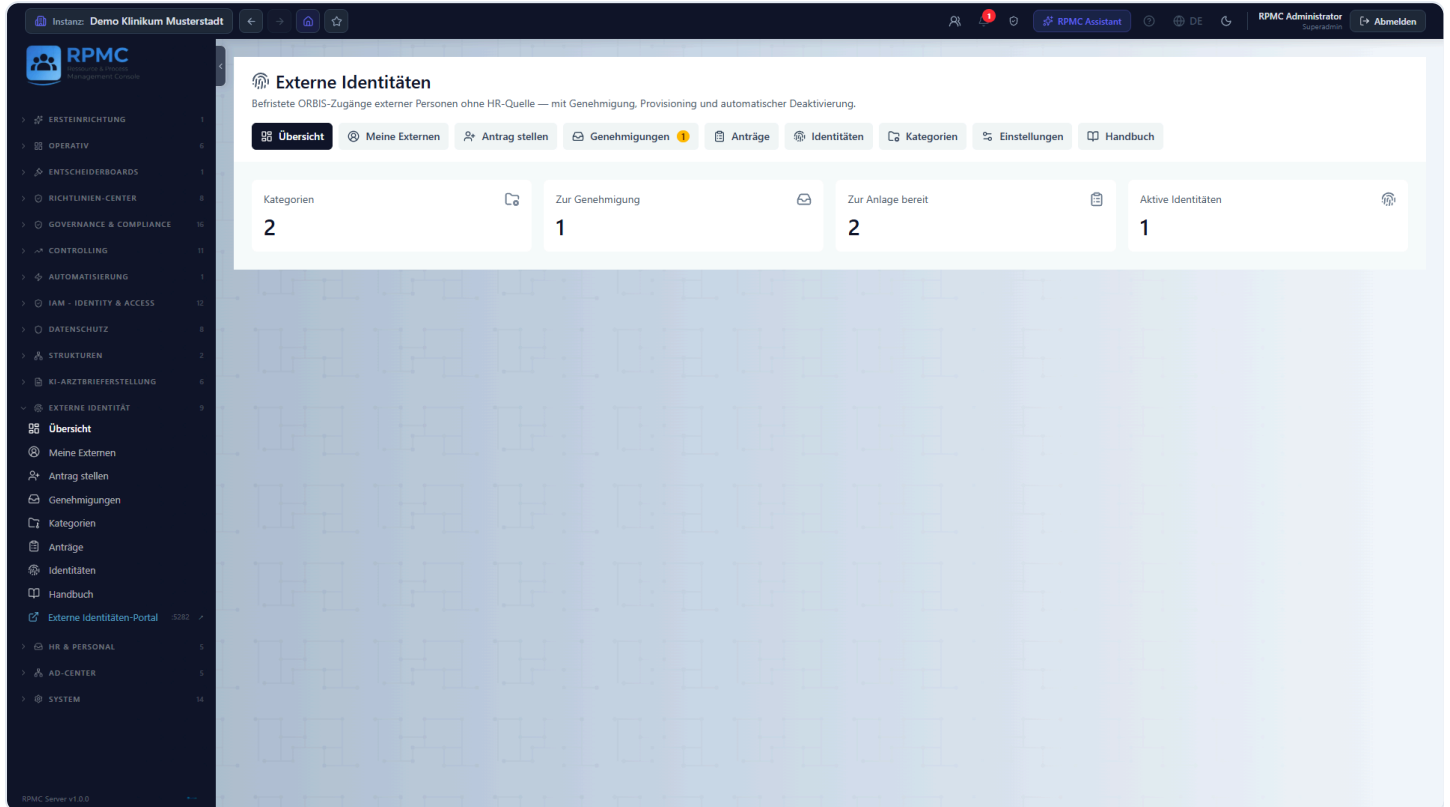
- LANR-Konsolidierung:** RPMC führt die Arztnummern aus beiden Welten zusammen — auch dort, wo ORBIS Krankenhausarzt-Nummer und Fachgruppe getrennt führt — und bildet daraus die konsolidierte LANR inklusive **KBV-Prüfziffern-Validierung**: Zahlendreher fallen sofort auf.
- HR als Master:** Die Ampel bewertet Abweichungen mit klarer Richtung — das HR-System gilt als führend; ORBIS-Abweichler werden als Korrekturbedarf markiert.
- Gruppierung je Einrichtung:** Verbünde sehen den Abgleich je Haus; die Prüfliste ist bewusst read-only — Korrekturen erfolgen kontrolliert im führenden System.

FALLBEISPIEL

Beim Quartalsabschluss moniert die KV zurückgewiesene Leistungen. Die Prüfliste zeigt: Zwei Fachärzte tragen in ORBIS eine LANR mit ungültiger Prüfziffer, ein dritter fehlt im HR-Stamm. Drei gezielte Korrekturen statt tagelanger Fehlersuche in Abrechnungsprotokollen — der Abgleich hat sich in einem einzigen Quartal bezahlt gemacht.

Externe Identitäten RELEASED

Honorarärzte, Werkstudenten, Medizintechnik-Dienstleister, Prüfer: Externe brauchen ORBIS-Zugang — aber befristet, begründet und mit garantiertem Ende. Externe Identitäten verwalten genau diesen Lebenszyklus.



Übersicht — befristete ORBIS-Zugänge externer Personen mit KPI-Kacheln: 2 Kategorien, 1 zur Genehmigung, 2 zur Anlage bereit, 1 aktive Identität — der Lebenszyklus auf einen Blick.

Instanz: Demo Klinikum Musterstadt

RPMC Management Console

Ersterne Identitäten

Befristete ORBIS-Zugänge externer Personen ohne HR-Quelle — mit Genehmigung, Provisioning und automatischer Deaktivierung.

Übersicht Meine Externen Anträge Genehmigungen Anträge Identitäten Kategorien Einstellungen Handbuch

CSV PDF

EXT-SCHLÜSSEL	ORBIS-BENUTZER	GÜLTIG BIS	STATUS
EXT_0001	EXT_KALTENBACH	2026-10-08	Aktiv
EXT_0002	-	2026-09-08	Wird angelegt
EXT_0004	EXT_OSTERMANN	2026-06-05	Abgelaufen

RPMC Server v1.0.0

Identitäten-Verwaltung — drei externe Zugänge mit sprechender EXT_-Kennung in unterschiedlichen Lebensphasen (aktiv, wird angelegt, abgelaufen) inklusive CSV-/PDF-Export für den Prüfer.

Instanz: Demo Klinikum Musterstadt

RPMC Management Console

Ersterne Identitäten

Befristete ORBIS-Zugänge externer Personen ohne HR-Quelle — mit Genehmigung, Provisioning und automatischer Deaktivierung.

Übersicht Meine Externen Anträge Genehmigungen Anträge Identitäten Kategorien Einstellungen Handbuch

PERSON	FIRMA	RISIKO	GÜLTIG BIS	STATUS
Jens Kaltenbach	MedTech Service GmbH	Mittel	2026-10-08	Genehmigt
Dr. Vera Sommerfeld	Praxis Dr. Sommerfeld	Hoch	2026-09-08	Genehmigt
Marco Weidner	CleanIT Systemhaus AG	Mittel	2026-11-07	In Genehmigung
Anja Ostermann	HygCert Prüfdienst	Mittel	2026-08-16	Entwurf

RPMC Server v1.0.0

Antrags-Workflow — vier Anträge externer Personen (MedTech-Techniker, Praxis-Ärztin, Reinigungs-Dienstleister, Hygiene-Auditorin) mit Status (genehmigt, in Genehmigung, Entwurf), Risiko-Badges und „Gültig bis“-Datum: kein Externen-Zugang ohne dokumentierten Weg.

- **Kategorien mit Vorgaben:** je Externe-Kategorie (Honorararzt, Dienstleister, Hospitant ...) sind Standard-Rechteumfang, maximale Laufzeit und Genehmigungsweg hinterlegt.
- **Workflow statt Zuruf:** Antrag → Genehmigung → Anlage (erkennbar an eigener Kennzeichnung im Konto-Namen) → automatisches Ablaufdatum. Verlängerung nur per erneuter Genehmigung.
- **Garantiertes Ende:** Ablauf-Worker deaktivieren fällige Zugänge automatisch — der Klassiker „der Techniker-Account von 2019 lebt noch“ ist konstruktiv ausgeschlossen.

- **Getrennte Sicht:** Externe verschmutzen nicht den Mitarbeiter-Bestand; Audits über Externe sind eine eigene, saubere Auswertung.

NUTZEN

Externe Konten sind bei Prüfungen ein Standard-Befund und real das beliebteste Einfallstor. Ein erzwungener Lebenszyklus mit Auto-Ablauf senkt dieses Risiko strukturell — nicht durch Disziplin, sondern durch Systemdesign.

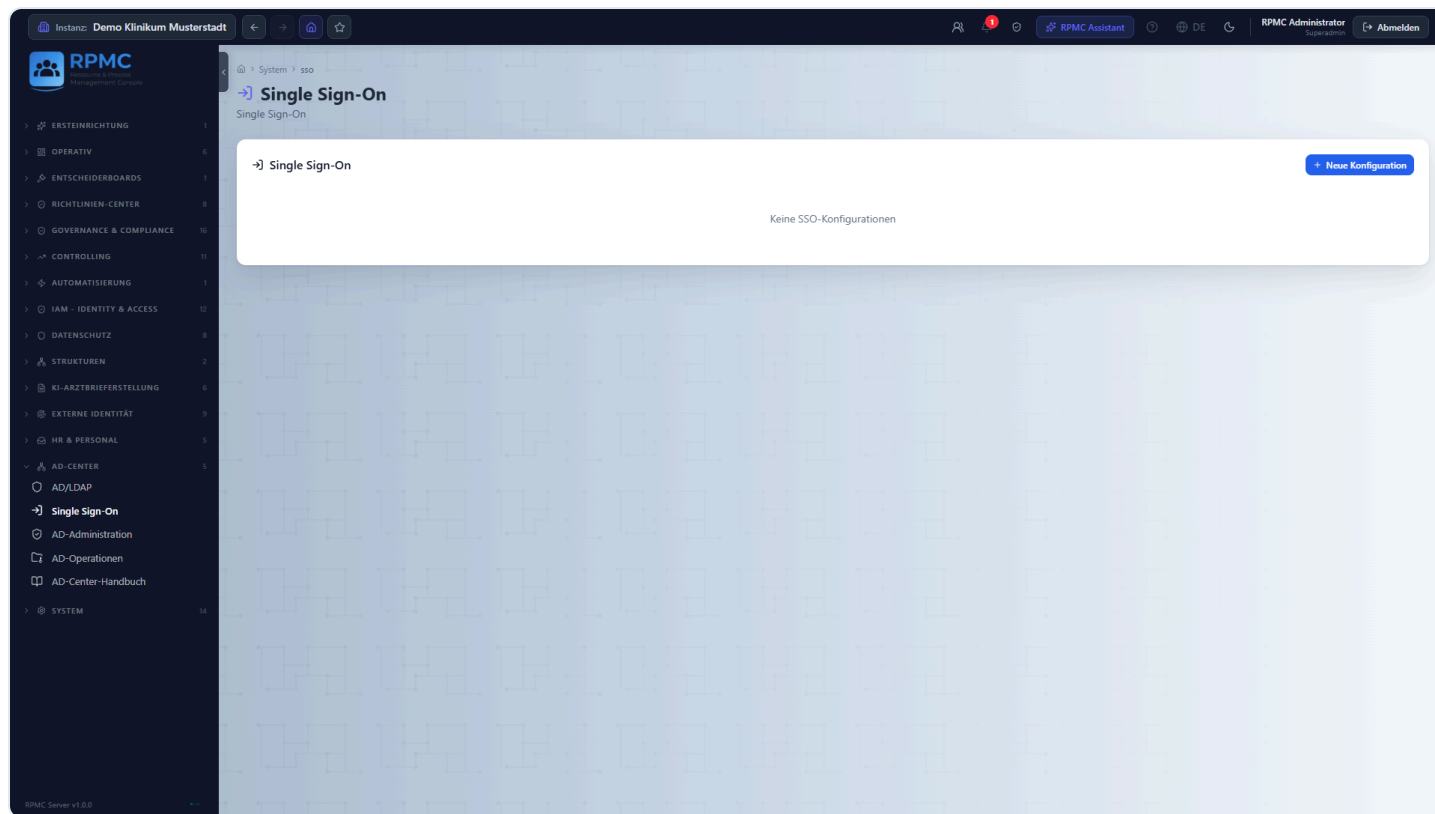
AD Center

IN ENTWICKLUNG

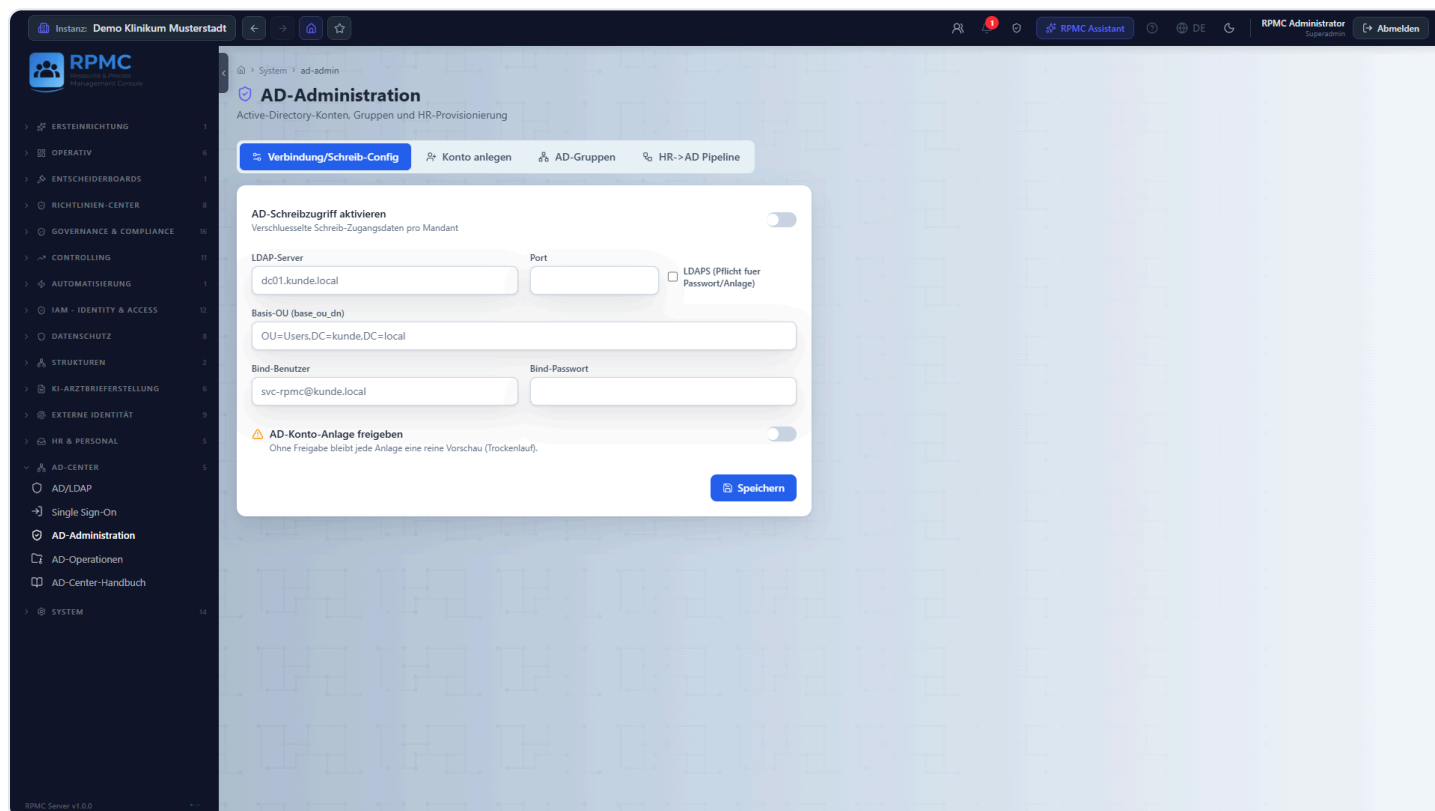
Das AD Center bündelt alles rund um Active Directory, LDAP und Single Sign-On in einem eigenen Bereich — von der Verbindungs-Konfiguration bis zur administrativen AD-Pflege direkt aus RPMC. Der Bereich ist produktiv nutzbar und wird aktuell aktiv ausgebaut — deshalb kennzeichnen wir ihn ehrlich als „in Entwicklung“.

The screenshot displays the RPMC (Rechtliche Prozessmanagement Center) interface, specifically the AD/LDAP configuration page. The top navigation bar shows the instance name "Demo Klinikum Musterstadt" and the user "RPMC Administrator". The left sidebar lists various RPMC modules, with "AD-CENTER" and "AD/LDAP" highlighted. The main content area is titled "AD/LDAP" and "Active Directory". It contains several sections: "Active Directory" with a toggle for "AD-Authentifizierung aktivieren", "Domain" (example.local), "LDAP Server (optional)" (dc01.example.local), "LDAP Port" (389), "Bind User (Service Account)" (CN=svc_rpmc,OU=Service,DC=example,DC=local), "User Base DN" (OU=Users,DC=example,DC=local), "Auto-Provisionierung" with a toggle for "Benutzer automatisch bei AD-Login anlegen", "Verbindungs-Timeout" (5), and "LDAP-SSO" with a toggle for "Single Sign-On über LDAP aktivieren". A "Verbindung testen" button is at the bottom left. A "Speichern" button is at the bottom right. Below the main configuration area, there is a section for "Single Sign-On (SSO)" with a toggle for "SSO-Federation via OpenID Connect oder SAML 2.0 (Azure AD, ADFS, Keycloak etc.)" and a link to "SSO-Einstellungen öffnen".

AD/LDAP — Anbindung mit Domain, LDAP-Server, Port und SSL, Bind-Benutzer, Auto-Provisionierung und LDAP-SSO inklusive „Verbindung testen“.



Single Sign-On — SSO-Federation über OpenID Connect und SAML 2.0 (Entra ID/Azure AD, ADFS, Keycloak u. a.) zentral konfiguriert.



AD-Administration — administrative AD-Operationen (Benutzer- und Gruppen-Verwaltung) aus RPMC heraus: der Ausbau-Schwerpunkt des AD Centers.

- **Heute produktiv:** LDAP-Sync in beide Richtungen (inkl. Write-Back), LDAP-Login-Fallback, SSO-Federation, AD-Konto-Anlage aus dem Benutzer-Management mit Live-Suche im Verzeichnis.
- **Im Ausbau:** erweiterte AD-Administration (Gruppen-Management, Massen-Operationen im Verzeichnis, tiefere Provisionierungs-Automatik) — Auslieferung schrittweise über reguläre Updates.

TRANSPARENZ

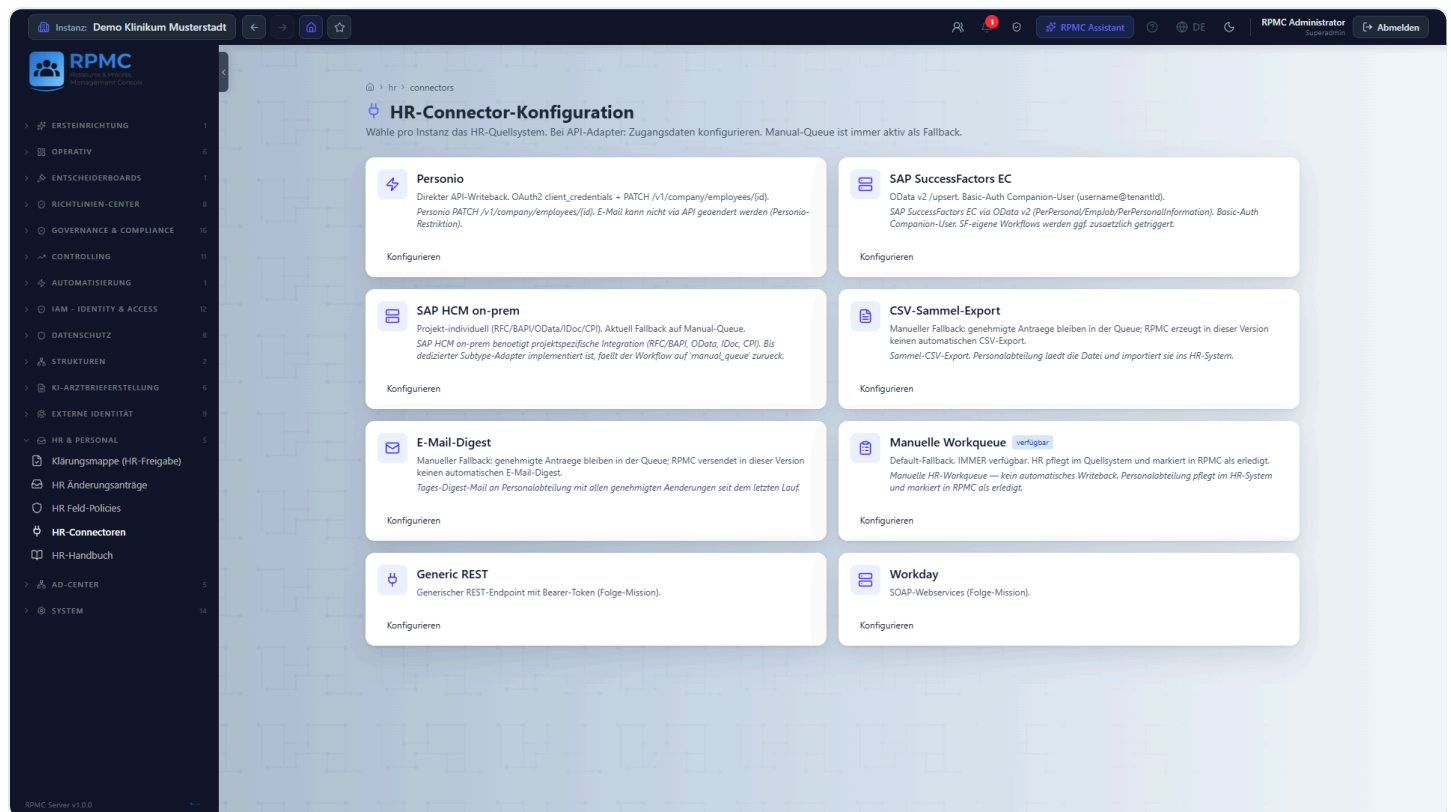
Wir kennzeichnen Module erst dann als „released“, wenn sie unseren eigenen Ansprüchen an Robustheit und Audit-Tiefe genügen. Das AD Center erfüllt seine Kernaufgaben bereits heute zuverlässig; der volle Administrations-Umfang folgt in den kommenden Releases — für Bestandskunden ohne Aufpreis.

HR & Personal — Anbindungen und Klärungsmappe

RELEASED

HR-Daten sind der Taktgeber jedes IAM-Prozesses — und zugleich die heterogenste Quelle im Haus. RPMC bindet praktisch jedes HR-System an, verkraftet mehrere Quellen parallel und gibt der Personalabteilung mit der Klärungsmappe ein eigenes Arbeitswerkzeug.

21.1 HR-System-Anbindungen



HR-Connector-Konfiguration — Adapter-Karten für Personio, SAP SuccessFactors EC, SAP HCM on-premise, CSV-Sammel-Export, E-Mail-Digest, manuelle Workqueue, Generic REST und Workday.

Acht Anbindungswege decken vom Cloud-HR bis zum Fax-Zeitalter alles ab: direkte Konnektoren (Personio, SAP SuccessFactors, SAP HCM, Workday), generische REST-Schnittstelle, CSV/XLSX-Dateien per Upload, SFTP oder **Watchfolder** (überwachtes Verzeichnis mit automatischem Import), E-Mail-Digest und die manuelle Workqueue für Häuser ganz ohne Export-Möglichkeit. Jede Quelle wird mit eigenem Zeitplan, eigener Feld-Zuordnung und eigener Import-Historie geführt.

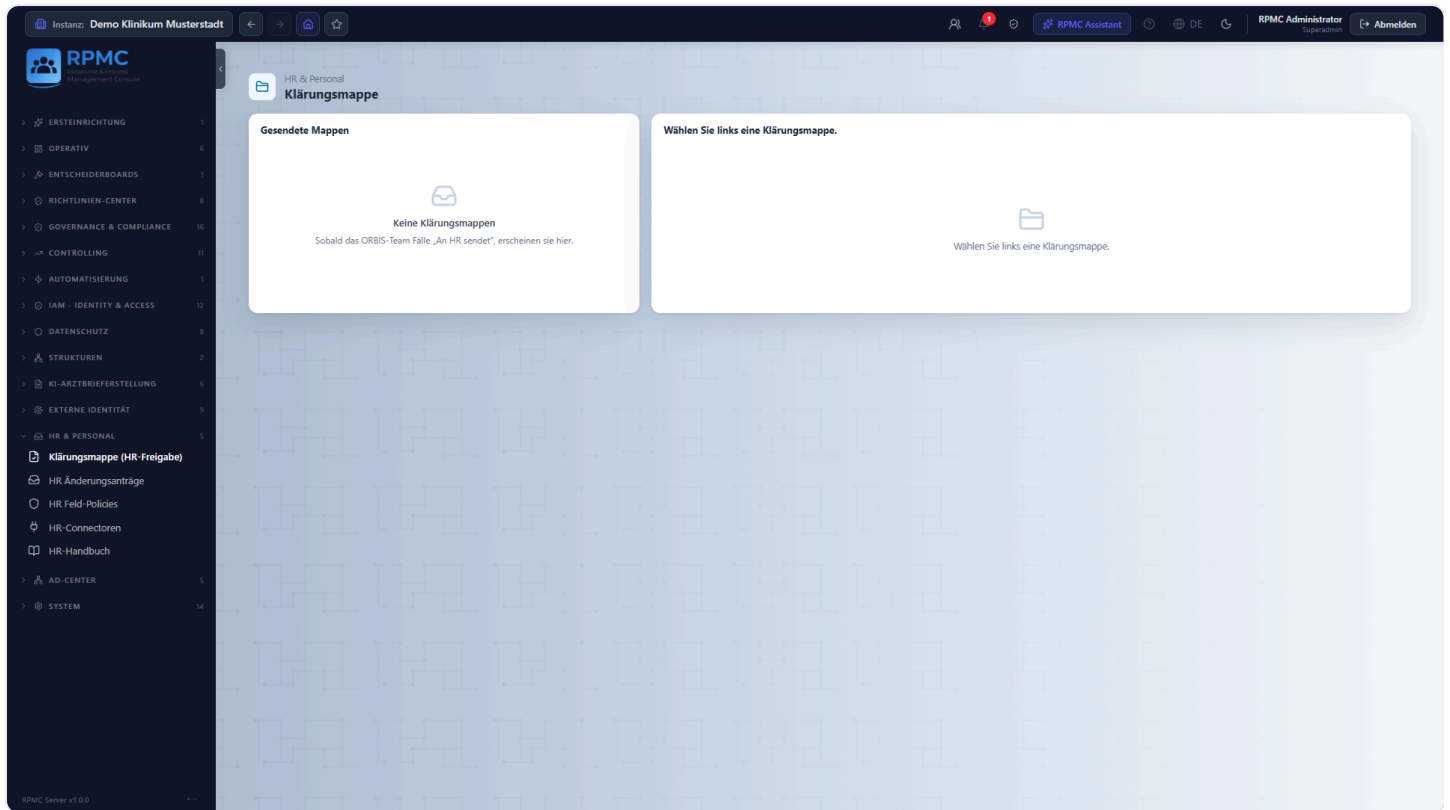
21.2 Multi-Source-Merge: mehrere HR-Wahrheiten, ein Bestand

The screenshot displays the RPMC Match Center interface. The top navigation bar includes the RPMC logo, a sidebar menu with categories like 'ERSTENRICHTUNG', 'OPERATIV', 'ENTSCHEIDERBOARDS', and 'SYSTEM', and a top right area with user information and a login button. The main content area is titled 'Match Center' and shows a 'Quellsystem-Abgleich und Verknüpfungen' section. Below this, there's a 'Aktive Quelle' section with a message 'Keine Quelle vorhanden'. A tab bar at the bottom of the main content area includes 'HR Gateway', 'Erkannte Spalten', 'Zuordnungen', 'Verlauf', 'Import-Historie', 'Datenquellen', 'Match-Konfiguration', and 'Einstellungen'. The 'Import-Läufe' section is active, showing a table with one entry: 'demo-seed' with a status of 'completed' and '712/712 Zeilen'. A green banner above the table states 'Aktive HR-Quellen: 1' and 'Gemeigte Datensätze: 712', with a note explaining that multiple import sources can be active simultaneously and that duplicates are handled by row hashes.

HR-Gateway (Match-/Merge-Center) — Import-Läufe mit Ergebnis (712/712 Zeilen), aktive HR-Quellen mit Merge-Logik sowie die Reiter Erkannte Spalten, Zuordnungen und Match-Konfiguration.

Viele Häuser haben nicht *ein* HR-System: Stammpersonal in SAP, Ärzte in einer Zusatzlösung, Tochtergesellschaften mit Personio. RPMC führt bis zu vier parallele HR-Quellen (Slots) mit definierter Vorrang-Logik zusammen; Duplikate werden über Zeilen-Hashes erkannt, erkannte Spalten automatisch zugeordnet, und die Schema-Selbstreparatur verkraftet es, wenn die Personalabteilung die Spaltenreihenfolge im Export ändert — der Montagsimport bricht deswegen nicht mehr.

21.3 Die HR-Klärungsmappe



HR-Klärungsmappe — der Posteingang der Personalabteilung für gemeldete Klärungsfälle mit Status-Workflow: jede Rückfrage dokumentiert, jede Antwort nachvollziehbar.

Aus Status Center und Mitarbeiter-Verwaltung wandern unklare Fälle per Klick zur HR-Klärung (Kapitel 6.3): widersprüchliche Stammdaten, fragliche Austritte, Doubletten. Die Personalabteilung arbeitet ihren Posteingang im eigenen Bereich ab — mit Detail-Sicht je Fall, Status-Workflow und dokumentierter Rückmeldung, die automatisch zum auslösenden Fall zurückfließt.

FALLBEISPIEL

Der HR-Import meldet für eine Pflegekraft ein Austrittsdatum, ORBIS zeigt sie weiter im Dienst. Statt Telefon-Pingpong: Fall an die Klärungsmappe. HR antwortet dokumentiert „Vertragswechsel Tochtergesellschaft, kein Austritt“ — der Fall schließt sich, die Antwort bleibt als Wissensbaustein am Mitarbeiter hängen. Beim Audit ein Jahr später ist der Vorgang in 30 Sekunden rekonstruiert.

NUTZEN

Die Klärungsschleife IT ↔ Personalabteilung ist in den meisten Häusern der langsamste IAM-Prozess überhaupt. Ein strukturierter Posteingang mit Fristen und Historie halbiert die Durchlaufzeiten erfahrungsgemäß — und beendet den Beweisnotstand („wir hatten das doch gemeldet ...“) auf beiden Seiten.

KI-Arztbrief-Pipeline

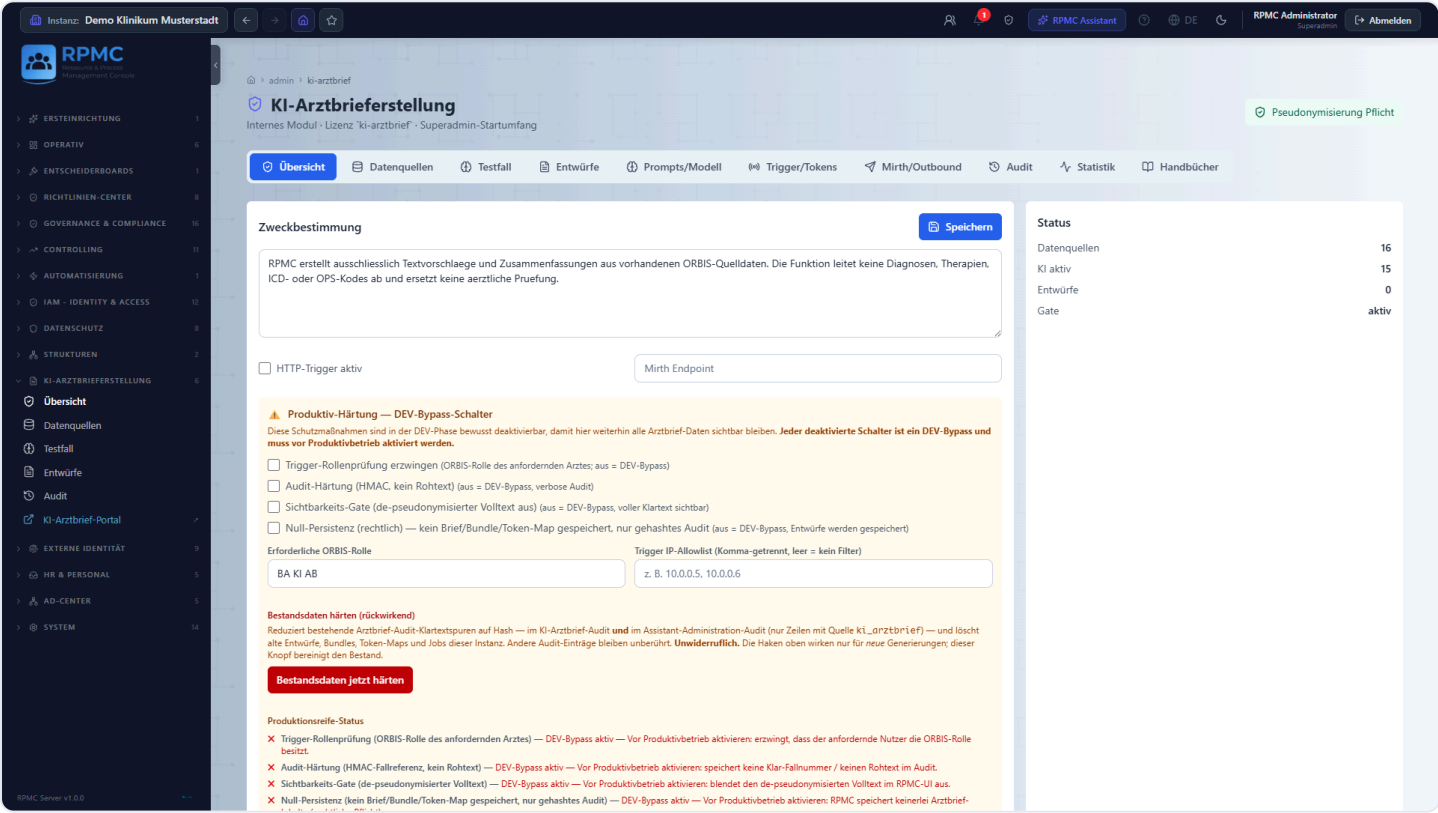
IN ENTWICKLUNG

ABGRENZUNG

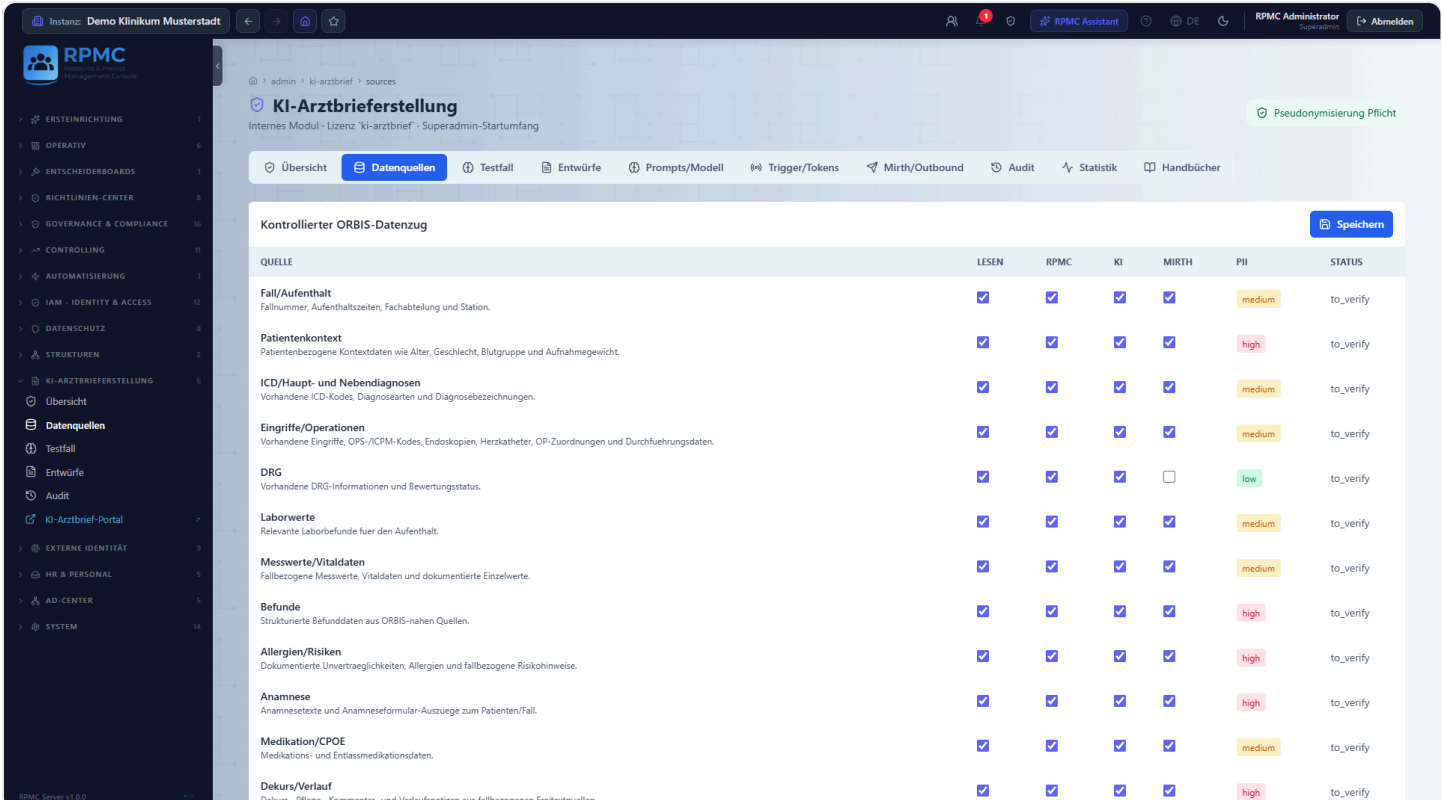
Die KI-Arztbrief-Pipeline ist ein separates Modul in Entwicklung. Sie ist nicht Bestandteil des aktuellen RPMC-Produkts und nicht in den derzeit angebotenen Editionen enthalten.

22.1 Zielbild

Geplant ist eine unterstützende Entwurfspipeline; medizinische Bewertung und Freigabe verbleiben beim Arzt.



Entwicklungsoberfläche der separaten KI-Arztbrief-Pipeline. Die dargestellten Schalter, Datenquellen und Abläufe beschreiben den aktuellen Entwicklungsstand und keinen zugesagten Serienumfang.



Entwicklungsoberfläche für eine geplante Quellen-Matrix. Die Abbildung zeigt einen Zwischenstand und keinen Bestandteil des aktuellen RPMC-Lieferumfangs.

Geplante Schutz- und Freigabelogik

Vorgesehen sind getrennte Freigaben für Lesen, Anzeige, KI-Verarbeitung und Kommunikationsserver sowie eine PII-Einstufung je Quelle. Vor einer möglichen produktiven Nutzung sind technische Härtung, Datenschutzprüfung, klinische Validierung und vertragliche Festlegung erforderlich.

Geplanter Arzt-Workflow

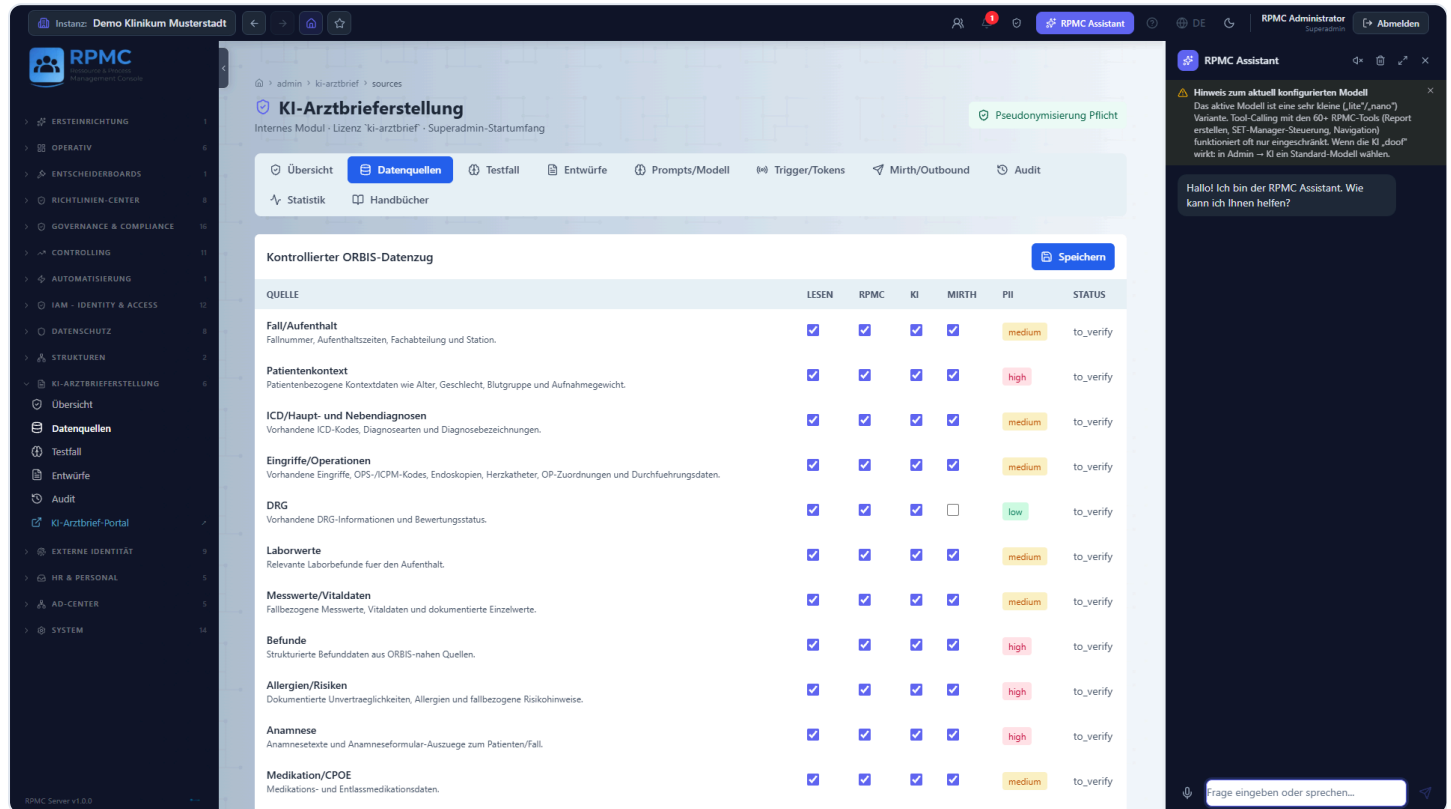
Das Zielbild umfasst einen fallbezogenen Aufruf aus ORBIS, die Erstellung eines Entwurfs, zwingende ärztliche Prüfung und einen konfigurierbaren Dokument-Rückweg. Einzelheiten können sich während der Entwicklung ändern.

ENTWICKLUNGSSTATUS

Die Kombination der geplanten Pipeline-Komponenten wird derzeit entwickelt und technisch bewertet. Es wird keine Aussage getroffen, dass diese Architektur im Markt einzigartig oder ausschließlich bei RPMC verfügbar ist. Das Modul gehört nicht zum aktuellen RPMC-Produktumfang.

RPMC-Assistent — die mitgelieferte KI RELEASED

RPMC stellt eine lokal betreibbare Assistenzfunktion bereit; Voraussetzungen und Leistung hängen von der eingesetzten Hardware und Modellkonfiguration ab.



hier über der Konfiguration des separaten KI-Arztbrief-Moduls (IN ENTWICKLUNG)

23.1 On-Premise zuerst — Cloud nur auf Wunsch

- Lokale Modelle können im RPMC-Prozess betrieben werden. GPU-Unterstützung und die optionale Auslieferung vorkonfigurierter Modelle richten sich nach Hardware, Lizenzierung und Projektkonfiguration.
- **Alternativ Cloud-LLMs:** Häuser, die bewusst Cloud-Kapazität nutzen wollen, binden externe Modelle an — unter anderem über Google Vertex AI. Die Entscheidung liegt beim Haus, dokumentiert und jederzeit umkehrbar; für Patientendaten-Szenarien bleibt die Pflicht-Pseudonymisierung bestehen.
- **Vendor-neutral by Design:** Die Oberfläche nennt keine Modell- oder Herstellernamen — das Haus kommuniziert gegenüber Anwendern und Betriebsrat eine Funktion, kein Logo. Modellwechsel bleiben ein Konfigurationsdetail statt einer Schulungswelle.

23.2 Was der Assistent kann

- **Fragen in natürlicher Sprache:** „Welche Mitarbeiter meiner Station wurden seit über einem Jahr nicht rezertifiziert?“ — der Assistent erzeugt eine garantiert lesende, mandanten-gescope Abfrage und liefert die Tabelle.
- **Aktionen mit Bestätigung:** Workflows entwerfen, Reports anlegen, Fälle kommentieren — die KI schlägt vor, der Mensch bestätigt. Keine autonome Schreiboperation.
- **Peer-Wissen:** Die Wissensbasis erkennt Muster über vergleichbare Mitarbeiter („87 % der HNO-Pflege tragen diese 11 Rollen“) und begründet Vorschläge nachvollziehbar — auch als Zubringer für das Richtlinien-Center (Kapitel 11).

- **Proaktive Hinweise:** Ein Insight-Worker meldet Auffälligkeiten von sich aus per Live-Push — etwa neu aufgetauchte verwaiste Konten in einer OE.
- **Sprachbedienung:** Eingaben wahlweise per Text oder Sprache, Antworten in der Sprache des Anwenders (DE/EN/FR/IT).

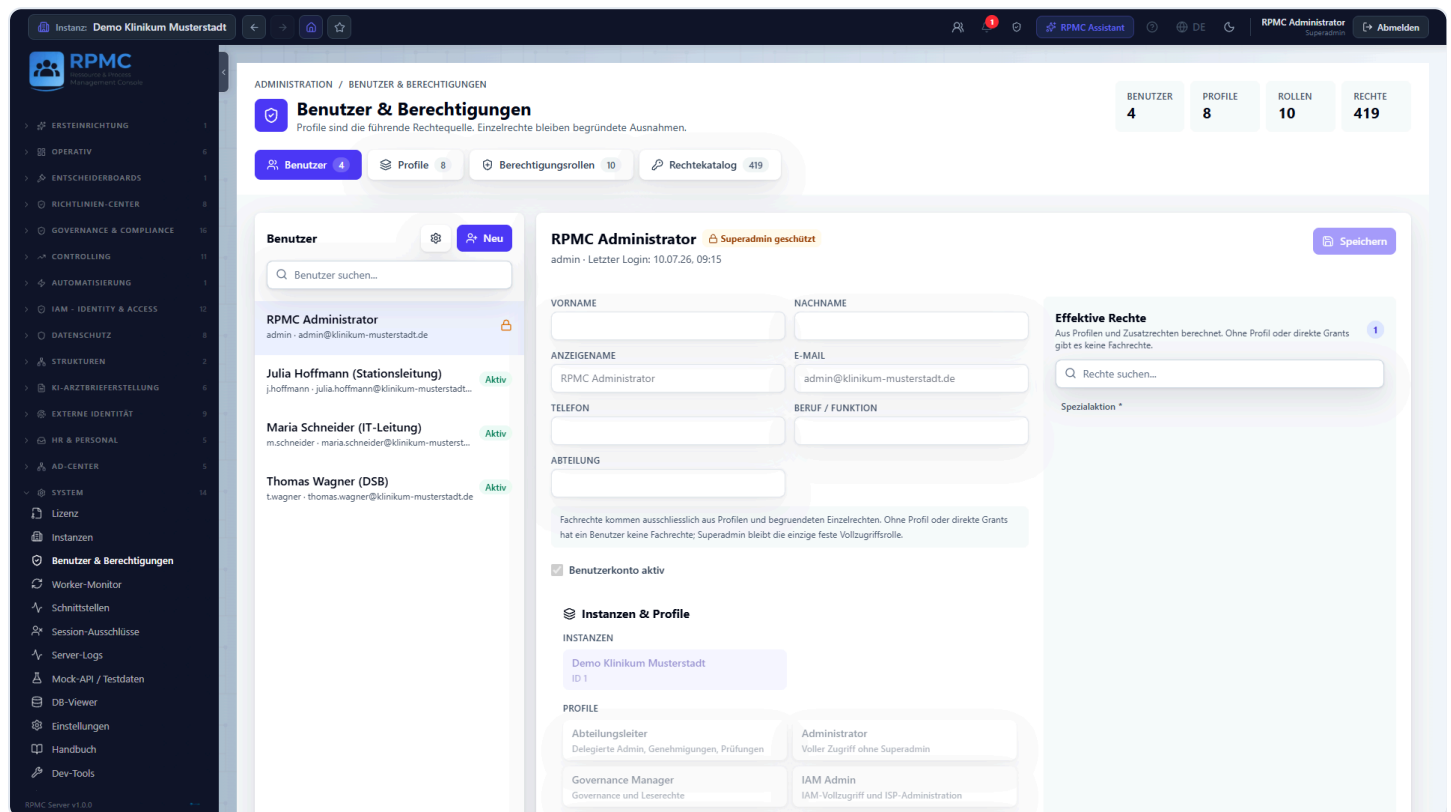
NUTZEN

Die KI senkt die Einstiegshürde der gesamten Plattform: Auswertungen ohne SQL, Workflows ohne Schulung, Auffälligkeiten ohne aktives Suchen. Und weil sie im Haus läuft, entfallen Cloud-Datenschutzprüfung, AVV-Verhandlung und Betriebsrats-Sonderrunden — die häufigsten Gründe, warum KI-Projekte in Kliniken scheitern, bevor sie beginnen.

Benutzer, RBAC & Sicherheit — LDAP, SSO, MFA, SIEM

RELEASED

Wer eine Governance-Plattform betreibt, muss bei der eigenen Sicherheit Maßstab sein. RPMC bringt ein vollständiges, feingranulares Rechtemodell für seine Bediener mit — plus die Integrationen in die Sicherheits-Landschaft des Hauses.



Benutzer & Berechtigungen — 4 Benutzer, 8 Profile, 10 Rollen, 419 Einzelrechte; rechts die Detailansicht mit Instanz-Zuordnung, Profilen und dem Panel „Effektive Rechte“, das die tatsächliche Rechtesumme deterministisch anzeigt.

24.1 RBAC: Profile, Rollen, Direct-Grants

- **Dreistufiges Modell:** Profile bündeln Berechtigungsrollen, Rollen bündeln Einzelrechte aus dem Berechtigungsbaum (~420 Rechte); Direct-Grants ergänzen begründete Einzelfälle. Die effektive Rechtesumme ist serverseitig deterministisch und vor dem Speichern sichtbar.
- **Instanz-Scope:** Jeder Benutzer wirkt nur in den ihm zugewiesenen ORBIS-Instanzen — Mandantentrennung auch für Administratoren.
- **Benutzeranlage flexibel:** manuell mit Passwort-Generator und Willkommens-Mail — oder direkt aus dem AD mit Live-Suche: AD-Benutzer authentifizieren per LDAP und führen kein separates RPMC-Passwort.
- **Portale explizit:** Zugänge zu Zusatz-Portalen (außer MyIdentity) werden bewusst einzeln freigeschaltet — kein stilles Mitwachsen von Zugriffsflächen.

24.2 Authentifizierung: LDAP, SSO, MFA

- **Hybrid-Login:** lokal (BCrypt-Hash) mit LDAP-Fallback — fällt das AD aus, bleiben hinterlegte Notfall-Zugänge funktionsfähig; der Vorfall wird protokolliert.
- **SSO:** SAML2 und OpenID Connect gegen Entra ID, ADFS, Keycloak u. a.; SCIM 2.0 für Push-Provisionierung aus dem IdP. Client-Secrets liegen AES-256-verschlüsselt.

- **MFA (TOTP):** zeitbasierte Einmal-Passwörter mit verschlüsseltem Secret und Recovery-Codes; per Policy je Rolle erzwingbar — NIS2-Pflicht für administrative Zugänge, hier ein Haken statt eines Projekts.
- **Härtung:** Account-Lockout, Refresh-Token-Rotation, Audit je Login-Versuch, regelmäßige eigene Sicherheits-Audits der Plattform.

24.3 SIEM-Integration

Über 30 Ereignistypen — Logins, Rechteänderungen, Break-the-Glass, Provisionierung, Worker-Gesundheit — fließen im CEF-Standardformat an das SIEM des Hauses, mit definierten Schweregraden und konfigurierbaren Filtern. Die IAM-Plattform wird damit Teil der Sicherheits-Leitstelle statt blinder Fleck daneben.

FALLBEISPIEL

Das SOC sieht nachts eine Break-the-Glass-Aktivierung mit hoher Severity im SIEM, korreliert sie mit dem gleichzeitigen ORBIS-Notfallzugriff und bestätigt den legitimen Klinik-Notfall in Minuten — inklusive fertigem Bericht aus der RPMC-Audit-Kette. Ohne Integration wäre derselbe Vorgang eine mehrtägige Nachforschung gewesen.

Plattform & Betrieb — ServerManager, Updates, Multi-Instanz

RELEASED

Die beste Fachlichkeit nützt nichts, wenn der Betrieb hakt. RPMC ist auf einen wartungsarmen, selbsterklärenden Betrieb durch die Klinik-IT gebaut — vom signierten Update bis zur Datenbank-Migration im laufenden Betrieb.

25.1 ServerManager: das Fundament

RPMC wird auf dem **ServerManager** betrieben — dem Installations- und Betriebs-Werkzeug, auf dem die gesamte Software-Auslieferung aufbaut. Er installiert RPMC, verwaltet Dienste und Lizenzen vor Ort und importiert Updates:

- **RPKG-Updates:** Jedes Update kommt als signiertes RPKG-Paket. Der ServerManager verifiziert die Signatur, stoppt den Dienst kontrolliert (laufende Synchronisationen werden zuvor sauber ausgeleitet), tauscht die Dateien und startet neu — ein Update dauert Minuten, nicht Wartungsfenster-Nächte.
- **Lizenz-Verwaltung:** ECDSA-signierte Lizenzdateien werden importiert und geprüft; die Lizenz ist die einzige Wahrheitsquelle für aktive Module — keine versteckten Schalter.
- **Self-Contained:** keine .NET-Vorinstallation, keine Fremdabhängigkeiten — ein Windows-Server genügt.

Aktive Lizenz

RPMC Enterprise Core ✓ Aktiv 🔒 Signiert

ENT-DEMO-2026-MESSE • Demo Klinikum Musterstadt

Gültig bis 10.7.2027 (in 364 Tagen)

Max. Identitäten: 810 / 100.000

RPMC-Benutzer: 4 / 100

Max. Instanzen: 2 / 99

[Lizenz importieren](#) [Details / Roh-JSON](#) [Lizenz-Anforderungsdaten](#) [Lizenz hart löschen](#)

Aktive Module (99 von 99)

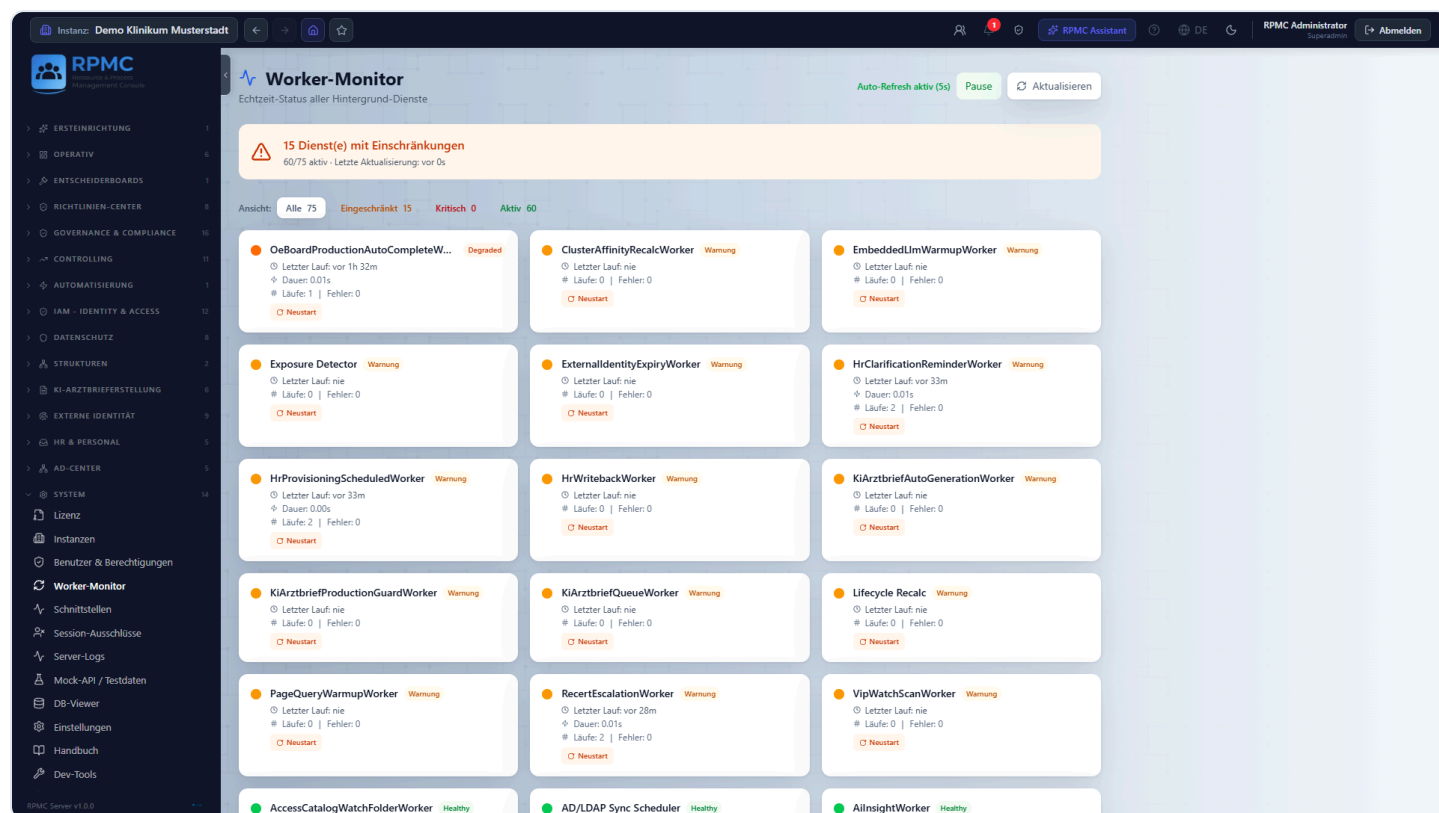
✓ Abteilungs-Genehmiger ten-department_approvers Konfiguration der Default-Genehmiger pro Abteilung fuer Berechtigungs-Workflows. Handout	✓ Active Directory Sync ad-sync LDAP/AD-Synchronisation mit Staging-Tabellen, Cross-Reference gegen ORBIS und HR sowie konfigurierbarem Schreib-Modus (read-only oder write-back). Handout	✓ Analytics (alle Module) analytics.full HR-, ORBIS-, AD-Analytics mit Trend- und Korrelationsanalysen Handout	✓ Arzt-/Behandlerverzeichnis orbis-db-physicians Arzt-Teams, Fachrichtungen und Behandlungsrollen aus der ORBIS-Datenbank Handout
✓ Audit-Attestierung audit_attestation Formale Attestierungs-Workflows: Vorgesetzte bestätigen periodisch die Berechtigungen ihrer Mitarbeiter mit signierter Profiler-Bestätigung. Handout	✓ Belegungs-Tagesaggregation orbis-db-occupancy-daily Tägliche Aggregation der Bett-/Raum-/Stations-Belegung aus ORBIS FALL_AUFENTHALT, Inkrement-Sync + 90-Tage-Backfill, Teil von Capacity-Reporting. Handout	✓ Benutzer-Compliance-Score user-compliance-score Individuelle Compliance-Bewertung pro Mitarbeiter (7 Komponenten) Handout	✓ Berechtigungs-Baselines governance-baselines Monatliche Snapshots des kompletten Berechtigungs-Zustands + Diff-Viewer für KRITIS-Audits und Rezerifizierung. Handout
✓ Berechtigungs-Gap-Analyse rights-gap-analysis Erkennt OEs auf die Benutzer Zugriff haben aber nie besuchen Handout	✓ Case Desk case-desk Zentrales Ticket- und Fall-Management für IAM- und Compliance-Vorgänge mit SLA-Steuerung, Eskalation und Verlaufsprotokoll. Handout	✓ Checklisten governance.checklists Manuelle Onboarding-/Offboarding-Checklisten (UI-Modul); Worker-Flows laufen separat weiter Handout	✓ Cloud-LLM-Provider cloud-llm Optionale Cloud-LLM-Anbindung für externe Anbieter als Alternative zum eingebetteten lokalen Modell. API-Schlüssel werden über die Lizenzdatei verteilt. Handout
✓ Cluster-Affinity-Engine analytics.cluster-affinity Handout	✓ Cross-Dept-Reporting cross-dept-reporting Handout	✓ Datenschutz-Folgenabschätzung dspro.dafa Handout	✓ DB-Viewer db-viewer Handout

Lizenz-Verwaltung — aktive Lizenz „RPMC Enterprise Core“ mit Laufzeit, Limits (Identitäten, Benutzer, Instanzen) und den aktiven Modulen als Karten: Jede lizenzierte Funktion ist mit Klartext-Beschreibung direkt im Produkt einsehbar.

25.2 DB-Migration im laufenden Betrieb

Jedes Update bringt seine Datenbank-Änderungen selbst mit: Beim Start führt RPMC ausstehende Migrationen automatisch, transaktional und versioniert aus — inzwischen über 530 Migrationen, ohne dass je ein Kunde ein SQL-Skript einspielen musste. Rückwärtskompatible Schritte erlauben Updates ohne Datenverlust-Risiko; der Migrationsstand ist jederzeit einsehbar. **Für die Klinik-IT heißt das: Ein RPMC-Update ist ein Import im ServerManager — die Datenbank kümmert sich um sich selbst.**

25.3 Systemmonitor & Worker



Worker-Monitor — Status aller Background-Worker mit Laufzeiten und Diagnose. Rund 80 Worker erledigen Synchronisation, Scoring, Rezertifizierung, Aufräumarbeiten und Überwachung — jeder einzeln sichtbar, mit Heartbeat, Fehlerzählern und letztem Exit-Grund.

Der Systemmonitor zeigt Serverdaten (CPU, RAM, Datenbank), Sync-Läufe und die Gesundheit aller Worker. Ausgeschaltete Funktionen melden ehrlich „übersprungen“ statt falscher Erfolge; ein Watchdog überwacht die Wächter. Betriebsprobleme werden sichtbar, bevor Anwender sie bemerken.

25.4 Multi-Instanz & Instanz-Provisioning

- **Bis zu 99 ORBIS-Instanzen** je Installation (editionabhängig), isoliert auf Datenbank-Ebene; Administratoren mit Mehrfach-Zugriff wechseln per Auswahl zwischen Häusern.
- **Instanz-Provisioning:** Eine neue Instanz wird beim Anlegen vollautomatisch ausgestattet — Mail-Vorlagen, Checklisten, Sync-Zeitpläne, Datenschutz-Konfiguration, Erst-Synchronisation in der richtigen Reihenfolge. Ein neues Haus im Verbund ist in Minuten arbeitsfähig statt in Beratungstagen; eine Boot-Heilung ergänzt fehlende Ausstattung auch bei Bestandsinstanzen nach.

25.5 Hochverfügbares Multi-Tenant-System IN ENTWICKLUNG

Für große Klinikverbünde entsteht derzeit die nächste Ausbaustufe: ein **hochverfügbares Multi-Tenant-System** mit redundanter Auslegung (kein Single Point of Failure), zentraler Mandanten-Steuerung über Standorte hinweg und Skalierung auf Verbund-Größenordnungen. Bestehende Installationen wachsen per Update in diese Architektur hinein — die heutige Multi-Instanz-Basis ist dafür ausgelegt. Verbindliche Ausbaustufen werden mit Pilot-Verbünden abgestimmt; wir kennzeichnen den Stand bis dahin ehrlich als Entwicklung.

NUTZEN

Betriebskosten entscheiden über Gesamtkosten: signierte Ein-Klick-Updates, selbstmigrierende Datenbank und automatisches Instanz-Provisioning halten den Administrationsaufwand einer RPMC-Installation im Bereich weniger Stunden pro Monat — auch im Verbund.

Editionen

RPMC ist in vier produktiven Editionen verfügbar. Die Architektur folgt dem License-as-SSoT-Prinzip: Die signierte Lizenz-Datei ist die einzige Wahrheitsquelle für aktive Module — eine Edition ist ein klar definiertes Modul-Set, keine versteckte Backend-Logik. Konditionen werden im Vertriebsgespräch auf Basis von Edition und Anforderungen festgelegt.

Edition	Zielgruppe & Limits	Umfang (kumulativ)
Pilot Befristete Evaluierung	500 Mitarbeiter · 1 Instanz · 6 Monate	ORBIS-Anbindung (lesend), AD-Sync, HR-Import, Match Center (3-Wege), Status Center Basis, 1–2 Ergebnis-Workshops.
Core	Kleine und mittlere Häuser; Fokus Übersicht & Bereinigung. 1.500 Mitarbeiter · 1 Instanz · 15 Admin-User	+ Status Center komplett, OE-Struktur inkl. Import/Export, Mail-System, kontrollierte Schnellbereinigung, Standard-Reports, RBAC mit Standard-Rollen.
Core Plus HAUPTPRODUKT	Mittlere und große Häuser mit Governance-Bedarf (NIS2-Audit steht an). 5.000 Mitarbeiter · 3 Instanzen · 30 Admin-User	+ Entscheiderboard (Kanban/Voting/Quorum/Vier-Augen), Governance-Dashboard, Audit-Kette mit HMAC-Integrität, ORBIS-Rollen-Manager, Unified Audit, Compliance-Score, erweiterte RBAC-Rollen, Exportpakete für IT-Leitung/Datenschutz/Audit.
Enterprise Core	Unikliniken, Maximalversorger, Verbünde mit KRITIS-Pflicht. 100.000 Mitarbeiter · 99 Instanzen · 100 Admin-User	+ Multi-Instanz (bis 99), Rezertifizierungs-Kampagnen mit Auto-Revoke, Compliance-Engine (NIS2/B3S/ISO 27001/DSGVO), Lifecycle-Engine (JML), Delegated Admin, Audit-Attestation, Überprivilegierungs-Erkennung, Kapazitäts-Reporting, dedizierte Einführungsbegleitung, Premium-Support optional.

EXTRA- und DISABLED-Logik

Innerhalb jeder Edition sind einzelne Module gezielt zu- oder abschaltbar: **EXTRA** schaltet ein Modul außerhalb der Edition frei (z. B. Cloud-LLM-Anbindung in Core Plus), **DISABLED** deaktiviert ein enthaltenes Modul bewusst (z. B. wenn das Haus eine eigene Audit-Pipeline betreibt). Jeder Override ist auditiert; freigeschaltet werden können ausschließlich lizenzierte Module.

FAIRNESS-PRINZIP

Jedes der über 90 Katalog-Module trägt im Produkt eine Klartext-Beschreibung — der Kunde sieht in der Lizenz-Ansicht jederzeit, was er lizenziert hat und was nicht. Keine Überraschungen, keine versteckten Zusatzkosten für Kernfunktionen.

Compliance-Mapping

Die folgende Matrix ordnet regulatorische Themen den unterstützenden RPMC-Modulen zu. Sie dient der Orientierung und ist keine Konformitäts- oder Rechtszusage.

KRITIS (BSIG § 8a)

Anforderung	RPMC-Modul
Patientenakten-Zugriffs-Audit	Patientenzugriffs-Audit, Fall-Zugriffs-Audit, Audit-Kette, SIEM
Infektionsverfolgung (Hygiene)	Patienten-Kontakt-Tracing (Exposure-Radar)
Notfall-Login-Dokumentation	Notfall-Login-Auswertung, Break-the-Glass-Audit
Manipulationserkennendes Logging	Audit-Kette (HMAC-SHA256), Append-only-DB-Rolle
SIEM-Anbindung in Echtzeit	SIEM-Integration (CEF, 30+ Event-Typen)

NIS2 (EU-Richtlinie 2022/2555)

Anforderung	RPMC-Modul
Art. 21 (2) (h) — Zugriffskontroll-Richtlinien	RBAC, Richtlinien-Center, Berechtigungsbaum, Audit-Kette
Art. 21 (2) (a/b) — Risikomanagement	Risk-Scoring, SoD-Engine, Compliance-Score
Art. 21 (2) (e) — Lieferketten-Sicherheit	Externe Identitäten, ITSM-HMAC-Webhooks, SSO-Secret-Verschlüsselung
MFA für administrative Zugänge	MFA (TOTP) mit Policy-Zwang je Rolle
Rezertifizierung kritischer Zugänge	Rezertifizierungs-Kampagnen + kontinuierliche Rezertifizierung
GF-Haftung — Management-Sicht	Compliance-Score, Governance-Dashboard, Exportpakete

BSI B3S Krankenhaus

Anforderung	RPMC-Modul
B3S 8.4 — Patienten-Fluss-Analyse	Cluster-Affinität, Verlegungs-Analytics
Risikobewertung	Risk-Scoring, Compliance-Score
Zugriffs-Audit	Audit-Kette, Patientenzugriffs-Audit, Unified Audit
Funktionstrennung	SoD-Engine mit Exception-Workflow
Prüfer-Nachweise	Evidence-Pack-Export, Audit-Attestation, Ketten-Verifikation

DSGVO

Anforderung	RPMC-Modul
Art. 5 (1) (c/e) — Datenminimierung, Speicherbegrenzung	Pseudonymisierung (Tracing, VIP-Schutz, KI), Löschfristen-Verwaltung
Art. 15 — Auskunftsrecht	MyIdentity-Selbstauskunft („Meine Berechtigungen“, Profil-Transparenz)
Art. 30 — Verarbeitungsverzeichnis	VVT-Modul

Anforderung	RPMC-Modul
Art. 32 — TOMs	RBAC, MFA, Audit-Kette, Match-Quote als Reifegrad-Nachweis
Auskunftssperre Patient	Pfortenauskunft inkl. Nach-Todesdatum
Auditierung sensibler Zugriffe	Audit-of-Audit, Patientensuche-Überwachung

§ 393 SGB V

Anforderung	RPMC-Modul
Patientenakten-Auswertungen	Patientenzugriffs-Audit (tägliche Auswertung), Fall-Zugriffs-Audit
OE-Konsistenz-Dokumentation	Zugriffs-Analysen, OE-Struktur mit Versionierung
Meldung irregulärer Zugriffe	Irregulär-Quoten je Mitarbeiter/OE, SIEM-Events, Prüf-Fälle

Roadmap — kontinuierliche Weiterentwicklung

Diese Roadmap beschreibt Entwicklungsrichtungen und keine Vertragszusage. Verbindliche Liefertermine und Funktionsumfänge werden ausschließlich schriftlich vereinbart.

Freigegebener Stand

- Generisches Dienstplan-Gateway für SP-Expert, Polypoint und ATOSS: RELEASED
- Match-Center-Integration als vierte Datenquelle: abhängig von kundenseitigem Mapping und Projektkonfiguration

In aktiver Entwicklung

- KI-Arztbrief-Pipeline als separates, nicht editionsgebundenes Entwicklungsmodul
- AD-Center-Vollausbau
- hochverfügbares Multi-Tenant-Zielbild für Klinikverbünde
- weiterer Feinschliff des Report Studio

Nächste Ausbaustufen

- schichtbasierte Berechtigungen und Vertretungsmanagement
- vertiefte Compliance-Report-Automatik
- weitere FHIR-/ISiK- und DCS-Evaluierung
- zusätzliche Hochverfügbarkeits- und Disaster-Recovery-Optionen

GRUNDSATZ

RPMC wird modular weiterentwickelt. Neue Funktionen werden mit ihrem Reifegrad gekennzeichnet und erst nach gesonderter Freigabe Bestandteil des angebotenen Produktumfangs.

Glossar

Die wichtigsten Fachbegriffe und Abkürzungen dieser Infomappe — bewusst laienverständlich erklärt.

AD (Active Directory) — Microsofts Verzeichnisdienst für Benutzer- und Gruppenverwaltung.

Append-only — „nur anfügen“: Einträge können nie geändert oder gelöscht werden — Pflicht-Eigenschaft für beweissichere Protokolle.

Audit-Kette — manipulationserkennende Nachweiskette: Jeder Eintrag ist kryptografisch mit seinem Vorgänger verkettet.

Audit-of-Audit — Protokoll darüber, wer wann welche Audit-Einträge eingesehen hat.

B3S — Branchenspezifischer Sicherheitsstandard Krankenhaus des BSI; konkretisiert KRITIS-Anforderungen.

Break-the-Glass — kontrollierter Notfallzugriff („Glas einschlagen“): befristete Rechteerhöhung mit Pflicht-Begründung und Voll-Protokoll.

CEF — Common Event Format; Standardformat für Sicherheits-Ereignisse Richtung SIEM.

DCS — Kopplung über die Dedalus-Kommunikations-Infrastruktur (Kommunikationsserver-Strecken).

Delta-Sync — Synchronisation nur der Änderungen seit dem letzten Lauf.

DirectDB — direkter Lesezugriff auf die ORBIS-Oracle-Datenbank.

DSB — Datenschutzbeauftragte/-r.

DSGVO — Datenschutz-Grundverordnung (EU 2016/679).

ECDSA — kryptografisches Signaturverfahren (elliptische Kurven); sichert RPMC-Lizenzen und Pakete.

FHIR — moderner Interoperabilitäts-Standard für Gesundheitsdaten.

Grace Period — Übergangsfrist, in der alte Rechte nach einem Wechsel kontrolliert auslaufen.

HL7 / MLLP — etablierter Nachrichtenstandard der Medizin-IT und sein Übertragungsprotokoll.

HMAC — Hash mit geheimem Schlüssel; Grundlage der manipulationserkennenden Audit-Kette

IAM — Identity and Access Management: Verwaltung von Identitäten und Zugriffsrechten.

IdP — Identity Provider; führendes Anmeldesystem bei SSO (z. B. Entra ID).

ITSM — IT Service Management (Ticketsysteme, Service-Prozesse).

JML — Joiner/Mover/Leaver: Eintritt, Wechsel, Austritt als automatisierbare Prozesse.

KIS — Krankenhaus-Informationen-System (hier: Dedalus ORBIS).

KRITIS — Kritische Infrastrukturen (BSIG § 8a); Krankenhäuser ab 30.000 stationären Fällen/Jahr.

LANR — lebenslange Arztnummer; Pflichtangabe für Abrechnung und Arztbriefe.

LDAP — Verzeichnisprotokoll für die AD-Anbindung.

MFA / TOTP — Mehr-Faktor-Anmeldung mit zeitbasierten Einmal-Passwörtern (Authenticator-App).

NIS2 — EU-Richtlinie 2022/2555 zur Netz- und Informationssicherheit; regelt u. a. Geschäftsführer-Haftung.

OE — Organisationseinheit (Klinik, Fachabteilung, Station ...).

On-Premise — Betrieb vollständig im eigenen Rechenzentrum, ohne Cloud-Abhängigkeit.

Pseudonymisierung — Ersetzen von Klarnamen durch Kennungen; Rückauflösung nur kontrolliert und begründet.

Quorum — Mindestanzahl von Stimmen für einen gültigen Gremien-Beschluss.

RBAC — Role-Based Access Control: rollenbasierte Zugriffskontrolle.

Rezertifizierung — periodische Bestätigung, dass vergebene Rechte weiterhin gebraucht werden.

RPKG — signiertes RPMC-Update-Paket, importiert über den ServerManager.

SAML2 / OIDC — Standards für Single Sign-On.

SCIM — Standardprotokoll für automatische Benutzer-Provisionierung aus einem IdP.

SET — wiederverwendbares Berechtigungs-Bündel (Rollen, OE-Gruppen, Einrichtungen) als Norm einer Funktion.

§ 393 SGB V — gesetzliche Pflicht zur Auswertung von Patientenakten-Zugriffen.

SIEM — Security Information and Event Management: zentrale Sicherheits-Ereignis-Verwaltung.

SoD — Segregation of Duties (Funktionstrennung): unvereinbare Rechte dürfen nicht zusammenfallen.

SSO — Single Sign-On: eine Anmeldung für viele Systeme.

TOM — technisch-organisatorische Maßnahmen (DSGVO Art. 32).

VVT — Verzeichnis von Verarbeitungstätigkeiten (DSGVO Art. 30).

Watchfolder — überwachtes Verzeichnis, aus dem Dateien automatisch importiert werden.

Worker — Hintergrund-Dienst für periodische Aufgaben (Sync, Scoring, Aufräumen ...).

Zwiebelschalen-Prinzip — mehrstufiges Matching von harter zu weicher Evidenz mit sichtbarer Konfidenz je Stufe.

RPMC

RESSOURCE & PROCESS MANAGEMENT CONSOLE

ANHANG B · KONTAKT

Bereit für ein Pilotgespräch?

RPMC befindet sich im Bugfixing und in der Vorbereitung weiterer Pilotierungen. Der konkrete Pilotumfang, der Reifegrad einzelner Module und die Erfolgskriterien werden vor Einsatz schriftlich festgelegt. Die KI-Arztbrief-Pipeline bleibt ein separates Modul in Entwicklung; das Dienstplan-Gateway ist freigegeben.

medivaris Software

INHABER KARL-HEINZ ROTH

Produktentwicklung

NIKOLAS ROTH

Vertrag & Zeichnung

AUSSCHLIESSLICH KARL-HEINZ ROTH

Kontakt

INFO@MEDIVARIS.DE

Hersteller, Anbieter und Lizenzgeber: medivaris Software, Inhaber Karl-Heinz Roth