```
module: 14
title: HR-Hub / Mitarbeiterplattform
phase: 1
status: detail-spec-draft
last_updated: 2026-05-08
session_source: brainstorming-session-2026-05-07-2206.md
related_lps: [LP-2, LP-3, LP-7, LP-9, LP-10, LP-13]
spec_style: requirements-pur
size: XL
```

Modul 14 — HR-Hub / Mitarbeiterplattform

> ***Detail-Spec gemäß LP-9.*** *Phase 1 voll (User-Korrektur). Quiply-Komplett-Ablösung. Sehr breites Modul mit vielen Sub-Bereichen (eigener MA-Bereich, Lohnabrechnungen, Krank/Urlaub als Forms, Announcements, MA-Verzeichnis, Password-Safe, Upload-Erinnerungen, Surveys, Requests, Quick-Links, Resources). Sensible Daten — strenge Permission-Gates.*

Themenblöcke

```
A. Datenmodell
B. Menü-Struktur und Routes
C. Persönlicher MA-Bereich
D. Announcements
E. Urlaubsantrag + Krankmeldung (Leave-Workflow)
F. Lohnabrechnungen (Payslips)
G. Upload-Erinnerungen (Reminders)
H. Generische Requests + Templates
I. MA-Verzeichnis + Locations
J. Password-Safe (Team-Vaults, verschlüsselt)
K. HR-Surveys
L. Quick-Links + Resources
M. Activity-Stream-Integration
N. Integration mit anderen Modulen
O. Permissions-Anwendung
P. Datenschutz / sensible Daten
Q. Klartext-Hinweise
R. Phase 2
```

Block A — Datenmodell

Kern-Entitäten

```
HrEmployeeProfile              – erweitertes MA-Profil pro TenantUser
HrAnnouncement                 – Firmen-Bekanntmachung
HrAnnouncementRead             – Read-Receipt pro User
HrAnnouncementReaction         – Emoji-Reaktion (1 Reaktion pro User pro Announcement)
HrAnnouncementComment          – Kommentar (chronologisch)
HrLocation                     – Firmenstandort
HrEmployeeDocument             – Dokument im MA-Profil (Vertrag, Bescheinigungen, Zeugnisse)
HrResource                     – kuratierte Ressource (intern/extern, mit Beschreibung)
HrQuickLink                    – Schnellzugriff (URL, Icon, Sortierung)
HrSurvey                       – MA-Umfrage
HrSurveyItem                   – Frage innerhalb Survey
HrSurveySubmission             – Antwort eines MA
HrSurveySubmissionAnswer       – pro Frage pro Submission
HrRequest                      – generischer MA-Antrag (Spesen, Hardware, Sonstiges)
HrRequestTemplate              – vorgefertigte Antrags-Vorlage
HrRequestComment               – Kommentar/Klärung pro Antrag
EmployeePayslip                – Lohnabrechnung (PDF, Monat/Jahr)
EmployeeUploadReminder         – Upload-Erinnerungs-Definition (z.B. Führerschein)
EmployeeUploadReminderDispatch – Versand/Erfüllungs-Tracking pro MA
EmployeeVacationRequest        – Urlaubsantrag mit Genehmigungs-Workflow
EmployeeSickLeaveReport        – Krankmeldung (selbst-eingereicht oder durch Büro)
EmployeePasswordSafeVault      – Team-Vault (z.B. „Disposition", „Marketing")
EmployeePasswordSafeEntry      – verschlüsselter Eintrag im Vault
EmployeePasswordSafeAccess     – Vault-Zugriffs-Berechtigung pro User/Group
```

HrEmployeeProfile

- `id`, `tenant_id`, `user_id` (1:1 mit `TenantUser`)
- `personal_number` (Personalnummer, Pflicht für Lohnabrechnungs-Upload-Match — Tenant-Admin pflegt)
- `birthdate` (optional, für Geburtstags-Hinweise im Hub)
- `hire_date` (Eintrittsdatum, optional)
- `position_label` (Positionsbezeichnung, Freitext)
- `team_label` (Team-Bezeichnung, Freitext — orthogonal zu Groups M27)
- `location_id` (FK auf `HrLocation`, optional)
- `phone_business`, `phone_private` (separate Felder)
- `address_street`, `address_zip`, `address_city`, `address_country`
- `emergency_contact_name`, `emergency_contact_phone`, `emergency_contact_relation` (Notfallkontakt)
- `manager_user_id` (FK auf TenantUser — Vorgesetzter für Antrags-Genehmigung)
- `bio` (Markdown, optional — sichtbar im MA-Verzeichnis)
- `avatar_file_id` (FK auf File, optional)
- `archived_at`

Sonderfall: Ein User kann nur **ein** Profil pro Tenant haben (1:1). Bei Tenant-User-Anlage wird leeres Profil automatisch geseedet.

HrAnnouncement

- `id`, `tenant_id`, `created_at`, `updated_at`, `created_by_user_id`
- `title` (Pflicht)
- `body` (Markdown, Pflicht)
- `is_pinned` (oben angeheftet)

- `published_at` (nullable — vor diesem Zeitpunkt = Draft)
- `expires_at` (optional — automatische Archivierung)
- `audience_kind` (Enum: `all | groups | locations | users`)
- `audience_group_ids[]`, `audience_location_ids[]`, `audience_user_ids[]` (je nach `audience_kind`)
- `requires_acknowledgement` (Boolean — Read-Receipt erforderlich)
- `allow_reactions` (Boolean, default true)
- `allow_comments` (Boolean, default true)
- `attached_file_ids[]` (FK auf Files M23)
- `archived_at`

HrAnnouncementRead

- `announcement_id`, `user_id`, `read_at`, `acknowledged_at` (optional — bei `requires_acknowledgement`)
- Unique-Index: `(announcement_id, user_id)`

HrAnnouncementReaction

- `announcement_id`, `user_id`, `emoji` (Enum oder Unicode-String aus Tenant-Whitelist)
- Unique-Index: `(announcement_id, user_id)` — eine Reaktion pro User pro Announcement

HrAnnouncementComment

- `id`, `announcement_id`, `user_id`, `created_at`, `updated_at`
- `body` (Markdown)
- `parent_comment_id` (optional — 1-Ebene-Threading in Phase 1)
- `archived_at`

HrLocation

- `id`, `tenant_id`, `name` (Pflicht, z.B. „Hauptstandort Geerkens", „Außenlager Süd")
- `address_street`, `address_zip`, `address_city`, `address_country`
- `phone`, `email`
- `geo_lat`, `geo_lon` (optional — für Map-Anzeige)
- `description` (Markdown — Anfahrt, Öffnungszeiten, Hinweise)
- `image_file_id` (optional)
- `is_default` (Boolean — Default-Standort für neue MA)
- `archived_at`

HrEmployeeDocument

- `id`, `tenant_id`, `employee_user_id`
- `document_kind` (Enum: `contract | reference | certificate | id_scan | drivers_license | other`)
- `title` (Pflicht)
- `description` (Freitext)
- `file_id` (FK auf File M23, Pflicht)
- `valid_from`, `valid_until` (optional — für ablauf-überwachte Dokumente wie Führerschein)
- `uploaded_by_user_id`
- `is_self_uploaded` (Boolean — vom MA selbst hochgeladen oder vom Büro)
- `visibility` (Enum: `employee_and_office | office_only` — z.B. Vertraulichkeitsstufe)
- `archived_at`

HrResource

- `id`, `tenant_id`, `title`, `description` (Markdown)

- `kind` (Enum: `internal_link | external_link | file | text`)
- `url` (für Links), `file_id` (für File)
- `category` (Freitext, z.B. „Onboarding", „Sicherheit", „IT")
- `audience_kind`, `audience_*` (analog Announcement)
- `position` (Sortierung)
- `archived_at`

HrQuickLink

- `id`, `tenant_id`, `label`, `url`
- `icon_key` (Lucide-Icon-Name oder Slug)
- `audience_kind`, `audience_*`
- `position`
- `open_in_new_tab` (Boolean, default true)
- `archived_at`

HrSurvey

- `id`, `tenant_id`, `created_by_user_id`, `created_at`
- `title`, `description` (Markdown)
- `is_anonymous` (Boolean — anonyme Auswertung möglich, Submitter-ID dann verschleiert)
- `audience_kind`, `audience_*`
- `opens_at`, `closes_at`
- `status` (Enum: `draft | open | closed | archived`)
- `allow_multiple_submissions` (Boolean, default false)
- `result_visibility` (Enum: `creator_only | hr_admins | all_participants`)

HrSurveyItem

- `id`, `survey_id`, `position`
- `item_type` (Enum: `text | textarea | rating_5 | rating_10 | nps | single_choice | multi_choice | boolean | date`)
- `label` (Pflicht), `description`
- `required` (Boolean)
- `options[]` (für Choice-Items)

HrSurveySubmission

- `id`, `survey_id`, `submitted_at`
- `submitter_user_id` (NULL bei `is_anonymous=true` — stattdessen Hash für Doppel-Einreichungs-Schutz)
- `submitter_hash` (nur bei anonym — `hash(survey_id, user_id)` für Doppel-Schutz, kein Reverse-Mapping)

HrSurveySubmissionAnswer

- `submission_id`, `item_id`, `value` (JSONB)

HrRequest

- `id`, `tenant_id`, `created_at`, `updated_at`
- `requester_user_id`
- `template_id` (FK, optional — bei Antrag aus Template)
- `title`, `body` (Markdown)
- `request_kind` (Enum: `expense | hardware | training | reference | document_request | generic`)
- `form_submission_id` (optional — wenn Template ein M5-Form referenziert)

- `attached_file_ids[]`
- `status` (Enum: `submitted | in_review | approved | rejected | withdrawn | completed`)
- `assigned_approver_user_id` (FK auf TenantUser — Default aus Template oder aus Manager des Requesters)
- `decision_at`, `decision_by_user_id`, `decision_note`
- `priority` (Enum: `normal | urgent`)
- `archived_at`

HrRequestTemplate

- `id`, `tenant_id`, `name`, `description`
- `request_kind`
- `default_assigned_approver_user_id` (optional)
- `default_approver_kind` (Enum: `manager | fixed_user | role | group` — Default für Genehmiger-Auflösung)
- `default_approver_role_id`, `default_approver_group_id`
- `linked_form_id` (optional — M5-Form für Antrag)
- `instructions` (Markdown)
- `position`
- `archived_at`

HrRequestComment

- `id`, `request_id`, `user_id`, `created_at`, `body` (Markdown)
- `is_internal_note` (Boolean — Approver-only sichtbar)

EmployeePayslip

- `id`, `tenant_id`, `employee_user_id`
- `period_year`, `period_month` (z.B. 2026, 4)
- `file_id` (FK auf File M23, Pflicht — PDF)
- `uploaded_by_user_id`, `uploaded_at`
- `is_read_by_employee` (Boolean — wird gesetzt wenn MA das PDF öffnet)
- `read_at`
- `note` (Freitext, z.B. „Korrektur 04/2026")
- `archived_at`
- Unique-Index: `(tenant_id, employee_user_id, period_year, period_month, note)` — gleicher Monat darf mit unterschiedlicher Note doppelt vorkommen (Korrektur-Lauf)

EmployeeUploadReminder

- `id`, `tenant_id`, `created_by_user_id`
- `title` (Pflicht, z.B. „Führerschein-Scan")
- `description` (Markdown)
- `document_kind` (Enum aus `HrEmployeeDocument.document_kind`)
- `audience_kind`, `audience_*` (welche MA betroffen)
- `cadence_kind` (Enum: `once | yearly | every_n_months | on_expiry`)
- `cadence_n_months` (für `every_n_months`)
- `expiry_lookahead_days` (für `on_expiry` — z.B. 30 Tage vor `valid_until`)
- `due_date` (für `once`)
- `is_mandatory` (Boolean — bei `true` erscheint im Dashboard als Block)
- `linked_form_id` (optional — M5-Form für Upload statt nur File)
- `archived_at`

EmployeeUploadReminderDispatch

- `id`, `reminder_id`, `employee_user_id`
- `due_at`, `dispatched_at`
- `status` (Enum: `pending | sent | fulfilled | overdue | dismissed`)
- `fulfilled_document_id` (FK auf `HrEmployeeDocument`)
- `fulfilled_at`
- `reminder_count` (wie oft erinnert)

EmployeeVacationRequest

- `id`, `tenant_id`, `requester_user_id`
- `start_date`, `end_date` (Pflicht, inklusiv)
- `working_days_count` (berechnet — netto Arbeitstage zwischen `start_date` und `end_date` ohne Wochenende und Feiertage des Bundeslands)
- `request_kind` (Enum: `paid_vacation | unpaid_vacation | overtime_compensation | special_leave`)
- `note` (Freitext aus Form-Feld)
- `form_submission_id` (FK — Antrag wird als M5-Form-Submission abgelegt)
- `status` (Enum: `submitted | approved | rejected | withdrawn`)
- `assigned_approver_user_id`
- `decided_at`, `decided_by_user_id`, `decision_note`
- `calendar_event_id` (FK auf M25-Calendar-Event, gesetzt bei `approved`)
- `auto_archive_at`

EmployeeSickLeaveReport

- `id`, `tenant_id`, `employee_user_id`
- `reported_at`, `start_date`, `expected_return_date` (optional — kann später aktualisiert werden)
- `actual_return_date` (gesetzt bei Rückmeldung)
- `has_certificate` (Boolean — AU-Bescheinigung vorhanden)
- `certificate_file_id` (FK auf File, optional — verschlüsselter Storage)
- `certificate_due_date` (Pflicht-Vorlage-Datum, z.B. 3. Tag bei DE-Recht)
- `note` (Freitext)
- `form_submission_id` (FK — Krankmeldung als M5-Form)
- `reported_by_user_id` (kann von `employee_user_id` abweichen — Büro meldet im Auftrag)
- `status` (Enum: `active | returned | cancelled`)

EmployeePasswordSafeVault

- `id`, `tenant_id`, `name` (Pflicht, z.B. „IT-Disposition")
- `description`
- `created_by_user_id`, `created_at`
- `archived_at`

EmployeePasswordSafeEntry

- `id`, `tenant_id`, `vault_id`
- `title` (Pflicht, z.B. „Aircall Admin-Login")
- `username` (verschlüsselt at-rest)
- `password` (verschlüsselt at-rest, AES-256-GCM mit per-Tenant-Key aus Master-KMS)
- `url`, `notes_encrypted` (verschlüsselt)
- `tags[]`
- `created_by_user_id`, `updated_by_user_id`, `updated_at`

- `last_rotated_at` (optional — Rotation-Hinweis)
- `archived_at`

Sonderfall: Werte werden **nie** im Klartext in DB gespeichert. Entschlüsselung erst beim API-Read mit Permission-Check + Audit-Log-Eintrag *„User X hat Eintrag Y entschlüsselt am Z"*.

EmployeePasswordSafeAccess

- `id`, `vault_id`, `principal_kind` (Enum: `user | group | role`)
- `principal_id` (FK auf TenantUser/Group/Role je nach Kind)
- `permission_level` (Enum: `read | write | admin` — read = Werte sehen; write = Einträge anlegen/ändern; admin = Vault-Verwaltung + Access-Verwaltung)
- `granted_by_user_id`, `granted_at`

Indizes (Performance-Pflicht)

- `HrAnnouncement (tenant_id, published_at DESC, archived_at)` für Feed-Default-Sortierung
- `HrAnnouncementRead (announcement_id, user_id)` Unique
- `EmployeePayslip (tenant_id, employee_user_id, period_year DESC, period_month DESC)` für Liste
- `EmployeeVacationRequest (tenant_id, status, start_date, end_date)` für Plantafel-Lookup
- `EmployeeSickLeaveReport (tenant_id, employee_user_id, status, start_date)` für aktive Sicht
- `EmployeeUploadReminderDispatch (tenant_id, employee_user_id, status, due_at)` für Dashboard
- `EmployeePasswordSafeEntry (tenant_id, vault_id)` mit RLS-Layer durch Vault-Access

RLS / Datenisolation

- Alle Tabellen tenant-scoped mit `tenant_id NOT NULL`
- Sensible Tabellen (`EmployeePayslip`, `EmployeeSickLeaveReport`, `EmployeePasswordSafeEntry`, `HrEmployeeDocument`) haben **zusätzlich** App-Code-Permission-Layer über reine RLS hinaus — nicht jeder Tenant-User darf alle Sätze sehen, auch wenn RLS sie nicht ausschließt
- Storage-Pfade (M23): Lohnabrechnungen unter `tenants/{tenantId}/payslips/{userId}/...` mit Bucket-Policy auch dort
- Krankmeldungs-AU-Bescheinigungen unter `tenants/{tenantId}/sick-certs/{userId}/...` (verschlüsselt at-rest separat)

Block B — Menü-Struktur und Routes

Sidebar-Hauptpunkt: *HR-Hub* mit kontextabhängigen Sub-Punkten (siehe Permissions Block O).

```
/{tenant}/hr                                  → Hub-Startseite mit Tabs
/{tenant}/hr/announcements                    → Announcement-Feed
/{tenant}/hr/announcements/:id                → Announcement-Detail
/{tenant}/hr/announcements/new                → neue Announcement (Permission-gegated)

/{tenant}/hr/documents                        → MA-Verzeichnis-Dokumente (HR-Admin-Sicht)
/{tenant}/hr/my-documents                     → eigene Dokumente

/{tenant}/hr/leave                            → Urlaub + Krank (Übersicht)
/{tenant}/hr/leave/new                        → neuer Antrag (Auswahl Urlaub/Krank)
/{tenant}/hr/leave/vacation/:id               → Urlaubsantrag-Detail
/{tenant}/hr/leave/sick/:id                   → Krankmeldungs-Detail

/{tenant}/hr/locations                        → Standort-Liste
/{tenant}/hr/locations/:id                    → Standort-Detail

/{tenant}/hr/payslips                         → eigene Lohnabrechnungen
/{tenant}/hr/payslips/:id                     → einzelne Lohnabrechnung (PDF-Viewer)

/{tenant}/hr/password-safe                    → Vault-Liste (sichtbar nur mit Vault-Access)
/{tenant}/hr/password-safe/:vaultId           → Vault-Detail (Einträge)
/{tenant}/hr/password-safe/:vaultId/:entryId  → Eintrag-Detail (mit Reveal-Funktion)

/{tenant}/hr/quick-links                      → Quick-Links-Liste
/{tenant}/hr/resources                        → Ressourcen-Übersicht
/{tenant}/hr/surveys                          → offene Surveys
/{tenant}/hr/surveys/:id                      → Survey-Teilnahme
/{tenant}/hr/surveys/:id/results              → Survey-Auswertung (Permission-gegated)

/{tenant}/hr/requests                         → eigene Anträge + zur Genehmigung anstehende
/{tenant}/hr/requests/new                     → neuer Antrag (Template-Auswahl)
/{tenant}/hr/requests/:id                     → Antrags-Detail

/{tenant}/hr/directory                        → MA-Verzeichnis (alle Mitarbeiter)
/{tenant}/hr/directory/:userId                → MA-Detail-Profil

/{tenant}/admin/hr/announcements              → Announcement-Verwaltung
/{tenant}/admin/hr/documents                  → Dokumenten-Verwaltung (alle MA)
/{tenant}/admin/hr/locations                  → Standort-Verwaltung
/{tenant}/admin/hr/payslips                   → Payslip-Upload (Bulk + Einzel)
/{tenant}/admin/hr/payslips/upload            → Bulk-Upload-Workflow
/{tenant}/admin/hr/leave                      → Urlaubs-/Krank-Übersicht aller MA
/{tenant}/admin/hr/upload-reminders           → Upload-Reminder-Definitionen
/{tenant}/admin/hr/upload-reminders/:id       → Reminder-Detail mit Dispatch-Liste
/{tenant}/admin/hr/quick-links                → Quick-Link-Verwaltung
/{tenant}/admin/hr/resources                  → Ressourcen-Verwaltung
/{tenant}/admin/hr/surveys                    → Survey-Verwaltung
/{tenant}/admin/hr/surveys/new                → neuer Survey (Editor)
/{tenant}/admin/hr/request-templates          → Request-Template-Verwaltung
/{tenant}/admin/hr/request-templates/:id      → Template-Editor
/{tenant}/admin/hr/password-safe              → Vault-Verwaltung (Tenant-weite Sicht)
/{tenant}/admin/hr/employees                  → MA-Profil-Verwaltung (Personalnummer, Manager,
Location)
```

Mobile-Sichtbarkeit (LP-2):
- `/{tenant}/hr` als Mobile-Default-Tab für Monteure (eigene Anträge, Payslips, Announcements)
- Foto-Upload für Krankmeldungs-AU-Bescheinigung mobile-optimiert
- Touch-Signatur nicht relevant in M14

Block C — Persönlicher MA-Bereich

Hub-Startseite (`/{tenant}/hr`)

Zu zeigende Daten (für jeden MA):
- Aktuelle Pinned-Announcements
- Offene Acknowledgement-Pflichten (rote Hinweise)
- Pendente eigene Anträge (Urlaub/Krank/Request) mit Status
- Pendente Upload-Erinnerungen (z.B. „Führerschein abläuft in 14 Tagen")
- Heute aktive Krankmeldungen / Urlaube im Team (gegated)
- Letzte Lohnabrechnung (Hinweis falls ungelesen)
- Quick-Links
- Geburtstags-Hinweise im Team (heute / diese Woche — falls Profil `birthdate` gepflegt und Sichtbarkeit erlaubt)

Benötigte UI-Elemente:
- Tab-/Sektions-Navigation für: Announcements / Anträge / Dokumente / Lohnabrechnungen / Surveys / Requests / Verzeichnis / Standorte / Resources / Quick-Links / Password-Safe (nur sichtbare Tabs je nach Permission)
- Card-/Widget-Anzeige der Hub-Inhalte
- Action-Funktionen *„Krankmeldung melden"*, *„Urlaub beantragen"*, *„Antrag stellen"* prominent zugänglich

Operationen:
- Klick auf Announcement → Detail
- Acknowledgement-Klick (bei `requires_acknowledgement`)
- Klick auf eigenen Antrag → Detail
- Klick auf Upload-Erinnerung → öffnet Upload-Workflow / verlinktes Form
- Klick auf Quick-Link → externes Ziel
- Klick auf Lohnabrechnungs-Hinweis → PDF-Viewer

Eigenes Profil (`/{tenant}/hr/directory/:userId` mit `userId == self`)

Zu zeigende Daten:
- Persönliche Stammdaten (Profil-Felder, Avatar, Position, Team, Standort)
- Notfallkontakt (nur self + HR-Admins sichtbar)
- Eigene hochgeladene Dokumente (nur self-sichtbar)
- Manager (Vorgesetzter)
- Eigener Resturlaub (Phase 2 — Kontingent-Tracking)
- Eigene aktive Krankmeldung (falls vorhanden)

Benötigte UI-Elemente:
- Sektionierte Anzeige aller Felder
- Inline-Edit-Funktion für Felder, die der MA selbst pflegen darf (`phone_private` , `address_*` , `emergency_contact_*` , `bio` , `avatar_file_id`)
- Read-only-Anzeige für Felder, die nur HR-Admin pflegt (`personal_number` , `position_label` , `manager_user_id` , `hire_date` , `team_label` , `location_id`)
- Avatar-Upload-Funktion
- Markdown-Editor für `bio`

Operationen:
- Persönliche Daten editieren (siehe oben)
- Dokumente hochladen (eigene)
- DSGVO-Datenexport (eigene Daten als JSON+Files-ZIP) — siehe M35

Eigene Dokumente (`/{tenant}/hr/my-documents`)

Zu zeigende Daten pro Dokument:
- Titel, `document_kind` , Upload-Datum, Uploader, `valid_from` / `valid_until` (falls relevant)

- Datei-Vorschau (PDF/Bild)
- Visibility-Hinweis (`employee_and_office` / `office_only` — Letzteres erscheint hier nicht!)

Benötigte UI-Elemente:
- Liste mit Filter nach `document_kind`
- Upload-Funktion (`is_self_uploaded = true`)
- File-Viewer
- Download-Funktion

Operationen:
- Eigenes Dokument hochladen (Default `visibility = employee_and_office`, Tenant-Admin-Setting kann erzwingen)
- Eigenes selbst-hochgeladenes Dokument löschen (mit Klartext-Warnung)
- Vom Büro hochgeladene Dokumente: nur Read

Block D — Announcements

Feed-View (`/{tenant}/hr/announcements`)

Zu zeigende Daten pro Announcement-Eintrag:
- Titel, Vorschau-Body (gekürzt), Autor + Avatar, Veröffentlichungs-Datum
- Pinned-Indikator
- Audience-Hinweis (z.B. „An: Alle" / „An: Team Süd" / „An: Marketing")
- Anzahl Reads / Reaktionen / Kommentare
- Acknowledgement-Status (eigene Sicht: noch offen / bereits bestätigt)
- Anhang-Hinweis (Anzahl Dateien)

Benötigte UI-Elemente:
- Chronologische Liste mit Pinned-Sektion oben
- Filter-Funktionen: nur ungelesen / mit Acknowledgement / nach Autor / Zeitraum / Tag
- Search-Funktion über Titel + Body
- Pagination (Cursor-basiert, 20 pro Seite)

Operationen:
- Klick → Detail-View
- Schnell-Reaktion direkt aus Feed (Phase 2)

Detail-View (`/{tenant}/hr/announcements/:id`)

Zu zeigende Daten:
- Titel, Body (Markdown gerendert), Autor, Datum, Audience-Hinweis
- Anhänge mit Vorschau
- Reaktionen (gruppiert nach Emoji mit Anzahl + Hover-Liste der User)
- Kommentare chronologisch (1-Ebene-Threading)
- Read-Receipt-Liste (nur sichtbar für Autor + HR-Admins): Wer hat gelesen / acknowledged / nicht
- Acknowledgement-Funktion (falls `requires_acknowledgement` und User noch nicht bestätigt)

Benötigte UI-Elemente:
- Markdown-Renderer
- Attachment-Liste mit Download/Vorschau
- Reaction-Picker (Emoji-Auswahl aus Tenant-Whitelist, Default: 6 Emojis)
- Comment-Editor mit Markdown
- Comment-Liste mit Reply-Funktion
- Read-Receipt-Tabelle (Permission-gegated)
- Acknowledgement-Button mit Bestätigungs-Counter

Operationen:
- Read-Receipt automatisch beim Öffnen (`HrAnnouncementRead.read_at = now`)
- Acknowledgement-Klick (separater Schritt: `acknowledged_at = now`)
- Reaktion setzen / ändern / entfernen (1 pro User, ändert ersetzt)
- Kommentar schreiben / löschen (eigenen) / bearbeiten (eigenen, mit Edit-Indikator)
- Anhang öffnen / herunterladen
- Announcement bearbeiten / archivieren (nur Autor + HR-Admin)
- Pin / Unpin (HR-Admin)

Klartext-Hinweise:
- Acknowledgement offen: *„Bitte bestätige, dass du diese Information gelesen hast."*
- Kommentare deaktiviert: *„Zu dieser Bekanntmachung können keine Kommentare hinterlegt werden."*

Verwaltung (`/{tenant}/admin/hr/announcements`)

Zu zeigende Daten:
- Alle Announcements (inkl. Drafts und archivierte)
- Pro Eintrag: Status (Draft / Veröffentlicht / Archiviert), Audience, Reads/Reactions/Comments-Counts

Operationen:
- Neue Announcement anlegen (Editor)
- Editor: Titel, Body (Markdown), Audience-Wahl, `requires_acknowledgement` -Toggle, Reactions/Comments-Toggles, Anhänge, Pin-Toggle, Veröffentlichungs-Zeitpunkt (sofort / geplant), Ablaufdatum
- Veröffentlichen (löst Notifications M22 aus)
- Archivieren / Reaktivieren
- Hard-Delete (nur HR-Admin, mit Klartext-Warnung)

Block E — Urlaubsantrag + Krankmeldung (Leave-Workflow)

Übersicht (`/{tenant}/hr/leave`)

Zu zeigende Daten:
- Eigene aktive + zukünftige Urlaube + Krankmeldungen (chronologisch)
- Eigene Antrags-Historie (alle Status)
- Falls Approver: anstehende Genehmigungen (eigene Team-Sicht oder Alle, je nach Permission)
- Team-Übersicht (gegated): Wer ist heute / diese Woche im Urlaub / krank

Benötigte UI-Elemente:
- Tab-Navigation: *Meine Anträge* / *Genehmigungen* / *Team-Übersicht*
- Filter-Komponenten: nach Status, Zeitraum, Antragsart
- Listen-Anzeige
- Action-Funktionen *„Urlaub beantragen"* und *„Krankmeldung melden"* prominent

Antrag stellen (`/{tenant}/hr/leave/new`)

Schritt 1 — Auswahl: Urlaub / Krankmeldung.

Urlaubsantrag

Form-basierter Workflow (M5 Template `Urlaubsantrag` als Subtyp `standard`):

Felder im Form-Template (Default, anpassbar pro Tenant):
- `start_date` (Date)
- `end_date` (Date)
- `request_kind` (Select: bezahlter Urlaub / unbezahlter Urlaub / Überstundenausgleich / Sonderurlaub)

- `note` (Textarea — Begründung, optional)
- `assigned_approver_user_id` (Select — Default: `manager_user_id` aus Profil; bei Multi-Manager-Setup wählbar)

Validation beim Submit:
- `end_date >= start_date`
- `start_date >= today` (kein rückwirkender Antrag — Klartext-Hinweis bei Versuch)
- Konflikt-Check (Klartext-Hinweis, kein Block):
- Wenn auf gleichen Tag bereits genehmigter Urlaub existiert: *„Du hast für diesen Zeitraum bereits einen genehmigten Urlaub. Trotzdem fortfahren?"*
- Wenn aktive Krankmeldung im Zeitraum: *„Du bist im Zeitraum krankgemeldet. Krankmeldung beendet sich automatisch ab Genehmigung dieses Urlaubs?"* (Hinweis, nicht-blockierend)
- `working_days_count` automatisch berechnet aus DE-Feiertagskalender des Standortes (Bundesland aus `HrLocation.address_*`)

Auto-Submit-Aktionen:
- `EmployeeVacationRequest` angelegt mit Status `submitted` und `form_submission_id`
- Notification (M22) Push + Email an `assigned_approver_user_id`: *„[Mitarbeiter] hat einen Urlaubsantrag gestellt"*
- Activity-Stream-Eintrag (Subject: User-Profil)
- Automation-Trigger `hr.vacation_requested` (M17)

Approver-View (Detail `/{tenant}/hr/leave/vacation/:id`):

Zu zeigende Daten:
- Antragsteller (Avatar + Name + Position + Team)
- Zeitraum + Working-Days-Count
- Antragsart, Note
- Konflikt-Hinweise (siehe Plantafel-Integration unten)
- Bisherige Anträge des Antragstellers (Historie)

Operationen Approver:
- Genehmigen (mit optionaler Notiz)
- Ablehnen (mit Pflicht-Notiz für Klartext-Begründung an Antragsteller)
- Rückfrage stellen (Status bleibt `submitted`, Comment angelegt; Antragsteller bekommt Notification)

Operationen Antragsteller:
- Zurückziehen (nur in Status `submitted`) → Status `withdrawn`
- Comment hinzufügen / lesen
- Bei Ablehnung: neuen Antrag mit anderen Daten stellen

Auto-Aktionen bei Genehmigung:
- Status → `approved`
- Calendar-Event-Anlage in M25 (eigener Kalender Antragsteller + abonnierte Tenant-Kalender wie „Team-Urlaube")
- ScheduleEntry-Konflikt-Hinweis in M4-Plantafel:
- Falls bereits ScheduleEntries im Zeitraum existieren: rote Konflikt-Indikatoren in Plantafel
- PL bekommt Notification *„Genehmigter Urlaub von [MA] kollidiert mit Schedule"*
- Activity-Stream-Eintrag
- Email an Antragsteller mit Klartext-Bestätigung
- Automation-Trigger `hr.vacation_approved`

Auto-Aktionen bei Ablehnung:
- Status → `rejected`
- Notification an Antragsteller mit Klartext-Begründung aus `decision_note`
- Activity-Stream-Eintrag
- Kein Calendar-Event

Krankmeldung

Form-basierter Workflow (M5 Template `Krankmeldung`):

Felder im Form-Template:
- `start_date` (Date — Default heute)
- `expected_return_date` (Date, optional)
- `has_certificate` (Boolean)
- `certificate_file_upload` (File — nur sichtbar wenn `has_certificate=true`; verschlüsselter Upload)
- `note` (Textarea, optional)

Validation:
- `start_date <= today + 1` (max. 1 Tag in Zukunft)
- `expected_return_date >= start_date`

Auto-Submit-Aktionen (kein Approval-Workflow):
- `EmployeeSickLeaveReport` angelegt, Status `active`
- Auto-Versand ans Büro: Email + Notification an alle User mit Permission `hr.read_all` UND opt-in für Sick-Notifications
- Direkter Manager-Notification (`HrEmployeeProfile.manager_user_id`)
- Activity-Stream-Eintrag (gegated — nur HR-Admin und Manager sehen)
- Plantafel-Integration M4: aktive Krankmeldung erscheint als Konflikt-Indikator für ScheduleEntries im Zeitraum
- Automation-Trigger `hr.sick_leave_reported`
- Bei `has_certificate=false` und `start_date >= today + 3` (DE-Recht): automatischer Reminder-Eintrag *„AU-Bescheinigung bis [3. Tag] vorlegen"*

Operationen Antragsteller:
- Verlängern (`expected_return_date` aktualisieren) → erneute Notification
- Bescheinigung nachreichen (File-Upload)
- Rückkehr melden (`actual_return_date` setzen, Status → `returned`)
- Stornieren falls fälschlicherweise gemeldet (Status → `cancelled`, mit Pflicht-Notiz)

Operationen Büro / HR-Admin:
- Krankmeldung im Auftrag eines MA erfassen (`reported_by_user_id != employee_user_id`)
- AU-Bescheinigung nach Erhalt einsehen / herunterladen (Audit-Log-Eintrag)
- Status-Korrektur

Datenschutz:
- AU-Bescheinigung **streng** permission-gegated (nur `hr.read_all` + `hr.upload_payslip`-Bundle)
- Standard-MA / Manager sieht nur „Krank von X bis Y" — keine Diagnose-Details, keine Bescheinigungs-Inhalte

Verwaltung Leave (`/{tenant}/admin/hr/leave`)

Zu zeigende Daten:
- Tabellarische Übersicht aller Anträge / Meldungen aller MA mit Filter
- Kalender-Sicht (Monatsansicht aller MA-Abwesenheiten)
- KPI-Tiles: Heute krank / Diese Woche im Urlaub / Pendente Genehmigungen / Offene AU-Bescheinigungen

Operationen:
- Bulk-Approve (Phase 2)
- Export als CSV
- Direkt-Erfassung im Auftrag eines MA

Block F — Lohnabrechnungen (Payslips)

Eigene Sicht (`/{tenant}/hr/payslips`)

Zu zeigende Daten:
- Liste eigener Lohnabrechnungen, sortiert nach Periode absteigend

- Pro Eintrag: Periode (z.B. „04/2026"), Note (falls Korrektur), Upload-Datum, Read-Status, PDF-Link
- Optional: Zusatzhinweise vom Büro

Benötigte UI-Elemente:
- Liste mit Periode-Filter (Jahr-Auswahl)
- PDF-Viewer / Download-Funktion

Operationen:
- PDF öffnen → automatisch `is_read_by_employee = true`, `read_at = now`
- Herunterladen (mit Audit-Log)

Klartext-Hinweise:
- Keine Lohnabrechnungen vorhanden: *„Hier erscheinen deine Lohnabrechnungen, sobald das Büro sie hochlädt."*

Verwaltung (`/{tenant}/admin/hr/payslips`)

Zu zeigende Daten:
- Tabelle aller Payslips über alle MA mit Filter (MA, Periode, Read-Status)
- Bulk-Upload-Status

Operationen:
- Einzel-Upload für bestimmten MA + Periode
- Bulk-Upload (siehe Workflow unten)
- Löschen (nur HR-Admin, mit Klartext-Warnung — `is_read_by_employee` Audit bleibt)

Bulk-Upload-Workflow (`/{tenant}/admin/hr/payslips/upload`)

Schritte:
1. Periode wählen (Jahr + Monat)
2. PDF-Files hochladen (mehrere via Drag-&-Drop oder ZIP)
3. Auto-Match-Logik:
- PDF-Dateiname-Pattern wird konfiguriert (z.B. `{personal_number}-{yyyy-mm}.pdf` oder `{lastname}-{yyyy-mm}.pdf`)
- System matcht jede PDF zu MA über Personalnummer / Lastname-Match
4. Match-Vorschau: Liste mit pro PDF zugeordnetem MA + Confidence
- Hard-Match (Personalnummer eindeutig): grün
- Soft-Match (Name): gelb mit Bestätigungs-Funktion
- Kein Match: rot, manuell zuordnen
5. Bestätigen → Auto-Anlage `EmployeePayslip` pro MA
6. Notification an MA: *„Neue Lohnabrechnung verfügbar"* (Push + Email konfigurierbar)
7. Aktivitäts-Bericht (Anzahl Erfolg / Fehler / Übersprungen)

Klartext-Validation:
- PDF ohne erkennbare Personalnummer: *„Konnte keine Personalnummer im Dateinamen erkennen. Bitte manuell zuordnen oder Dateiname-Pattern anpassen."*
- MA ohne Personalnummer im Profil: *„Mitarbeiter [Name] hat keine Personalnummer hinterlegt. Bitte im Profil ergänzen oder per Lastname-Match fortfahren."*
- Doppel-Upload (gleicher MA + Periode + leere Note): *„Für [MA] existiert bereits eine Lohnabrechnung 04/2026. Als Korrektur hochladen (mit Note)?"*

Audit:
- Pro Upload: User, Datum, Anzahl Files, Match-Resultat geloggt
- Pro Read: Audit-Eintrag (Compliance — Zugang nachweisbar)

Block G — Upload-Erinnerungen (Reminders)

Verwaltung (`/{tenant}/admin/hr/upload-reminders`)

Zu zeigende Daten:
- Liste aller Reminder-Definitionen
- Pro Eintrag: Titel, Cadence, Audience, Anzahl pendender Dispatches, Anzahl überfälliger

Benötigte UI-Elemente:
- Liste mit Filter
- Editor für neue Reminder
- Detail-View pro Reminder mit Dispatch-Liste

Editor-Felder:
- Titel, Beschreibung
- `document_kind` (welche Dokumentart wird erwartet)
- Audience (alle / Group / Location / einzelne User)
- Cadence (`once | yearly | every_n_months | on_expiry`)
- Bei `once` : Due-Date
- Bei `every_n_months` : N
- Bei `on_expiry` : Lookahead-Days
- Mandatory-Toggle
- Linked-Form (optional — z.B. Form-Template *„Führerschein-Update"* mit Felder zur Fahrerlaubnis-Klasse + File)

Operationen:
- Reminder anlegen / bearbeiten / archivieren
- Manueller Re-Dispatch an einzelnen MA
- Dispatch dismiss (z.B. MA hat aus dem Unternehmen ausgeschieden)

Cron-Logik (Scheduler)

- Täglicher Cron prüft pro Reminder:
- Bei `once` : einmalig dispatchen wenn `due_date - 14 Tage` erreicht
- Bei `yearly` : jährlich dispatchen am gleichen Tag wie Erst-Dispatch
- Bei `every_n_months` : alle N Monate
- Bei `on_expiry` : wenn `HrEmployeeDocument.valid_until - lookahead_days` erreicht
- Erstellt `EmployeeUploadReminderDispatch` mit Status `pending`
- Sendet Notification (Push + Email konfigurierbar in M22) an betroffenen MA: *„Bitte [Dokument] hochladen — fällig am [Datum]"*
- Bei Überfälligkeit (>7 Tage nach `due_at`): Status → `overdue` + Eskalations-Notification an Manager + HR-Admin
- Reminder zählt `reminder_count` hoch, wiederholt Notification alle 3 Tage bis `fulfilled`

Erfüllung

- MA klickt Reminder → wird zu Upload-Workflow geleitet
- Falls `linked_form_id` : Form öffnet sich, Submit erzeugt `HrEmployeeDocument` automatisch
- Falls keine Form: direkter Upload mit Auto-Vorausfüllung (`document_kind` , `valid_from` , `valid_until` falls Pattern erkennbar)
- Dispatch-Status → `fulfilled` , `fulfilled_document_id` gesetzt
- Notification an HR-Admin: *„[MA] hat [Dokument] eingereicht"*

Eigene Sicht im Hub

- Pendente Reminders erscheinen prominent auf Hub-Startseite
- Mandatory-Reminders blocken den Hub mit Klartext-Hinweis (nicht aber andere Module)

Block H — Generische Requests + Templates

Templates (`/{tenant}/admin/hr/request-templates`)

Zu zeigende Daten:
- Liste aller Templates mit Kind, Default-Approver-Logik, Linked-Form (falls)
- Anzahl Anträge aus Template

Editor-Felder:
- Name, Beschreibung, `request_kind`
- Default-Approver-Logik (`manager | fixed_user | role | group`)
- Linked-Form (M5-Form, optional)
- Instructions (Markdown — User-Hinweise beim Anträgen)
- Audience für Sichtbarkeit (welche MA dürfen Antrag aus diesem Template stellen)

SHK-Default-Templates (geseedet):
- „*Spesenabrechnung*" — Linked-Form mit Datum, Anlass, Betrag, Beleg-Upload; Approver = Manager
- „*Hardware-Anfrage*" — Linked-Form mit Hardware-Typ, Begründung; Approver = IT-Rolle
- „*Schulung / Weiterbildung*" — Approver = Manager; Linked-Form mit Anbieter, Termin, Kosten
- „*Arbeitszeugnis*" — Approver = HR-Rolle
- „*Sonstiger Antrag*" — Generisch, freier Text

Antrag stellen (`/{tenant}/hr/requests/new`)

Schritte:
1. Template-Auswahl (Liste der für User sichtbaren Templates) — alternativ „*Sonstiger Antrag*" für freien Antrag
2. Linked-Form wird gerendert (falls vorhanden) — sonst Titel + Body-Eingabe
3. Approver-Vorauswahl basierend auf Template-Logik (User kann ändern falls Permission)
4. Priority setzen (normal / urgent)
5. Anhänge hochladen
6. Submit → `HrRequest` Status `submitted` , Notification an Approver

Detail-View (`/{tenant}/hr/requests/:id`)

Zu zeigende Daten:
- Requester + Approver + Status + Datum
- Form-Submission-Inhalte (rendered) oder Title/Body
- Anhänge
- Comment-Stream (chronologisch — `is_internal_note` ausgeblendet für Requester)
- Decision-Note (bei abgeschlossenem Antrag)

Operationen Requester:
- Comment hinzufügen
- Zurückziehen (nur in `submitted` / `in_review`)
- Editieren der Form-Submission (Phase 2)

Operationen Approver:
- Status ändern (`submitted → in_review → approved | rejected | completed`)
- Internal-Note hinterlegen
- Reassign (an anderen Approver delegieren)

Operationen HR-Admin:
- Hard-Delete
- Bulk-Status-Update

Block I — MA-Verzeichnis + Locations

MA-Verzeichnis (`/{tenant}/hr/directory`)

Zu zeigende Daten pro MA-Eintrag:
- Avatar, Name, Position, Team, Standort
- Phone-Business, Email
- Manager
- (Geburtstag falls eigene Sichtbarkeitsfreigabe)

Benötigte UI-Elemente:
- Tabellarische oder Kartenliste
- Filter: Standort, Team, Manager, Position
- Search (Volltext über Name, Position, Team)
- Wahlweise Karten- oder Listen-Ansicht

Operationen:
- Klick → Profil-Detail
- Direkt-Telefon-Klick (Click-to-Call M12)
- Direkt-Mail-Klick
- Direkt-Chat-Start (M13)

Standort-Liste (`/{tenant}/hr/locations`)

Zu zeigende Daten pro Standort:
- Name, Adresse, Telefon, Email
- Map-Vorschau
- Anzahl zugeordneter MA
- Beschreibung (Anfahrt, Öffnungszeiten)
- Bild

Operationen:
- Standort öffnen → Detail
- Direkt-Map-Link / Anfahrts-Funktion

Standort-Verwaltung (`/{tenant}/admin/hr/locations`)

Operationen:
- Standort anlegen / bearbeiten / archivieren
- Default-Standort setzen
- Bulk-Reassign von MA bei Standort-Schließung

Block J — Password-Safe (Team-Vaults, verschlüsselt)

Vault-Liste (`/{tenant}/hr/password-safe`)

Zu zeigende Daten:
- Nur Vaults, für die User Access hat (`EmployeePasswordSafeAccess`)
- Pro Vault: Name, Beschreibung, Anzahl Einträge, Permission-Level (Read/Write/Admin)

Benötigte UI-Elemente:
- Liste / Kacheln
- Suchfunktion über Vaults

Vault-Detail (`/{tenant}/hr/password-safe/:vaultId`)

Zu zeigende Daten:
- Vault-Stammdaten
- Liste der Einträge (Title, Tags, letztes Update — **keine** Werte sichtbar in Liste!)
- Access-Liste (wer hat Zugang) — nur für Vault-Admin

Benötigte UI-Elemente:
- Liste der Einträge mit Suche
- Add-Eintrag-Funktion (bei `write` / `admin`)
- Add-Access-Funktion (nur `admin`)

Eintrag-Detail (`/{tenant}/hr/password-safe/:vaultId/:entryId`)

Zu zeigende Daten:
- Title, Username, Password, URL, Notes, Tags, last_rotated_at
- Werte werden **nicht automatisch** angezeigt — Reveal-Funktion erforderlich

Benötigte UI-Elemente:
- Reveal-Buttons pro Wert (Username/Password/Notes)
- Copy-to-Clipboard mit Auto-Clear nach 30 Sekunden
- Edit-Funktion (bei `write` / `admin`)
- Audit-Log-Anzeige (wer hat wann entschlüsselt) — bei `admin`

Operationen:
- Reveal-Klick: API-Call an Server, der Wert entschlüsselt mit Tenant-Key, Audit-Log-Eintrag erstellt, Wert für 30 Sekunden im Frontend hält, dann clear
- Copy: gleiche Audit-Wirkung
- Edit: optimistic-Locking (last `updated_at` Mitschicken, Block bei Konflikt)
- Hard-Delete: Klartext-Warnung *„Eintrag wird unwiderruflich gelöscht."*

Vault-Verwaltung (`/{tenant}/admin/hr/password-safe`)

Tenant-Admin-Sicht — alle Vaults sichtbar (auch ohne Access am Inhalt):
- Vault-Anlage / Archivierung / Hard-Delete
- Access-Verwaltung pro Vault
- Audit-Log-Übersicht (alle Reveals, Group-by-User, Group-by-Vault)

Verschlüsselung (Architektur-Pflicht)

- Per-Tenant-Master-Key in KMS (z.B. Scaleway-KMS)
- Per-Eintrag-DEK (Data Encryption Key) gewrappt mit Master-Key
- Algorithmus: AES-256-GCM
- DB speichert nur verschlüsselte Werte + Wrapped-DEK
- Server entschlüsselt **on-demand** beim Read mit Permission-Check
- Frontend bekommt Klartext nur über HTTPS-Antwort, hält max. 30 Sekunden, ist nicht persistent
- Audit-Log: jede Entschlüsselung mit User, Eintrag-ID, Timestamp, IP, User-Agent geloggt

Edge-Cases

- User wird aus Tenant entfernt → Vault-Access automatisch revoked, aktive Sessions invalidiert
- Vault-Owner verlässt Tenant → falls einziger `admin` : Tenant-Admin wird `admin` (Auto-Reassign mit Klartext-Hinweis)
- Master-Key-Rotation: Phase 2

Block K — HR-Surveys

Liste (`/{tenant}/hr/surveys`)

Zu zeigende Daten:
- Offene Surveys, an denen User teilnehmen darf (Audience-Match)
- Pro Eintrag: Titel, Beschreibung-Vorschau, Frist, Eigener Submission-Status

Operationen:
- Klick → Teilnahme

Teilnahme (`/{tenant}/hr/surveys/:id`)

Workflow:
- Survey-Items werden gerendert wie M5-Form
- Pflicht-Validation
- Bei `is_anonymous=true` : Klartext-Hinweis *„Diese Umfrage ist anonym — deine Antworten werden ohne Namens-Zuordnung gespeichert."*
- Submit → `HrSurveySubmission` + Answers
- Bei `allow_multiple_submissions=false` : nach Submit kein erneuter Zugriff (`submitter_hash` blockiert)

Auswertung (`/{tenant}/hr/surveys/:id/results`)

Zu zeigende Daten je nach `result_visibility` :
- Antworten-Counts pro Item
- Visualisierungen (Bar-Chart für Choice-Items, Avg-Score für Rating-Items, NPS-Score, Word-Cloud für Text-Items — Phase 1 mindestens Counts und Avg)
- Bei `is_anonymous=false` : Liste der Submitter (Permission-gegated)
- Bei `is_anonymous=true` : nur Aggregate, keine Submitter-IDs

Operationen:
- Export als CSV (Permission-gegated)
- Survey schließen / wieder öffnen

Verwaltung (`/{tenant}/admin/hr/surveys`)

Operationen:
- Survey anlegen / Items konfigurieren
- Audience setzen
- Veröffentlichung steuern
- Schließen / Archivieren
- Reminder an Nicht-Teilnehmer schicken

Block L — Quick-Links + Resources

Quick-Links (`/{tenant}/hr/quick-links`)

Zu zeigende Daten:
- Audience-gefilterte Liste mit Icon, Label, URL
- Sortierung nach `position`

Operationen User: Klick → externes Ziel (Tab je nach Setting)

Verwaltung (`/{tenant}/admin/hr/quick-links`):
- Anlegen / sortieren / archivieren
- Audience setzen

Resources (`/{tenant}/hr/resources`)

Zu zeigende Daten:
- Audience-gefilterte Ressourcen, gruppiert nach Kategorie
- Pro Eintrag: Titel, Beschreibung, Kind-Icon (Link / File / Text)

Operationen User:
- Klick auf Link → öffnet
- Klick auf File → Download / Vorschau
- Klick auf Text → Inline-Detail

Verwaltung (`/{tenant}/admin/hr/resources`):
- Anlegen / sortieren / archivieren
- Audience setzen
- Kategorien pflegen

Block M — Activity-Stream-Integration

Activity-Typen (Erweiterung M1 Block E)

- `hr.announcement_published`
- `hr.announcement_acknowledged`
- `hr.vacation_requested` / `hr.vacation_approved` / `hr.vacation_rejected` / `hr.vacation_withdrawn`
- `hr.sick_leave_reported` / `hr.sick_leave_returned` / `hr.sick_leave_cancelled`
- `hr.payslip_uploaded` (Subject = User-Profil; sichtbar nur User selbst + HR-Admin)
- `hr.payslip_read` (gegated)
- `hr.document_uploaded` (Subject = User-Profil; gegated nach Visibility)
- `hr.document_expiring_soon` (System-Activity bei `valid_until` Annäherung)
- `hr.upload_reminder_sent` / `hr.upload_reminder_fulfilled` / `hr.upload_reminder_overdue`
- `hr.request_submitted` / `hr.request_approved` / `hr.request_rejected` / `hr.request_completed`
- `hr.password_safe_revealed` (Subject = Vault; sichtbar nur Vault-Admin + HR-Admin)
- `hr.survey_published` / `hr.survey_submitted` (gegated nach Anonymität)

Verknüpfungen:
- HR-Activities erscheinen im User-Profil-Stream und (gegated) im Aggregat-Stream der Tenant-Admins
- Plantafel-Konflikt-Indikatoren beziehen sich auf `hr.vacation_approved` und `hr.sick_leave_reported`

Block N — Integration mit anderen Modulen

M4 Auftragspipeline / Plantafel

- Genehmigte Urlaube + aktive Krankmeldungen werden als **Konflikt-Indikatoren** in der Plantafel angezeigt
- Beim Anlegen einer ScheduleEntry, die Urlaub/Krank überschneidet: Klartext-Warnung (siehe M4 Block G)
- Plantafel kann „Abwesenheits-Layer" toggeln (ein/aus)

M5 Form Builder

- Krankmeldung + Urlaubsantrag laufen als Forms (Templates `Krankmeldung` / `Urlaubsantrag`)
- Request-Templates können Forms referenzieren
- Upload-Reminder können Forms referenzieren
- Form-Action `create_hr_vacation_request`, `create_hr_sick_leave`, `create_hr_request`, `create_hr_employee_document`

M22 Notifications

- Push + Email an Approver bei Antrag
- Push + Email an Antragsteller bei Entscheidung
- Push + Email an HR-Admin bei AU-Bescheinigungs-Versäumnis
- Push an Audience bei neuer Announcement (mit `requires_acknowledgement`-Markierung)
- Push bei Reminder-Fälligkeit

M25 Calendar

- Genehmigter Urlaub → Calendar-Event in eigenem Kalender Antragsteller (Tenant-default-konfigurierbar: ganztags / sichtbar als „Außer Haus")
- Optional Tenant-Kalender „Team-Urlaube" (alle MA-Urlaube aggregiert) für PL-Sicht
- Sync zu Google/Microsoft (Modul 25)

M17 Automation-Engine

Trigger:
- `hr.announcement_published`
- `hr.vacation_requested` / `hr.vacation_approved` / `hr.vacation_rejected`
- `hr.sick_leave_reported`
- `hr.request_submitted` / `hr.request_status_changed`
- `hr.upload_reminder_overdue`
- `hr.document_expiring_soon`
- `hr.payslip_uploaded`
- `hr.survey_submitted`

Actions:
- `hr.send_announcement` (System postet auto-Announcement, z.B. Welcome bei neuem MA)
- `hr.create_request` (z.B. Auto-Antrag bei Trigger)
- `hr.create_upload_reminder_dispatch`
- `hr.notify_manager`
- `hr.set_request_status`
- `hr.archive_announcement`

M23 Files

- Alle Dokument-Anhänge (Payslips, Employee-Docs, Sick-Certs, Announcement-Attachments, Request-Attachments, Survey-Attachments) liegen in M23 unter tenant-isolierten Pfaden
- Sensible Pfade (Payslips, Sick-Certs, Password-Safe-Backups Phase 2) zusätzlich App-Permission-gegated
- Ablauf-Tracking für `valid_until`-Felder läuft über M23-Integration mit `expires_at`-Setting (Phase 2)

M13 Team-Chat

- Direkt-Chat-Start aus MA-Verzeichnis
- Optional: Auto-Chat-Channel pro Standort (Phase 2)

M27 Auth / Permissions

- Permissions-Definition siehe Block O
- Tenant-Admin → automatisch alle HR-Permissions
- 2FA-Pflicht für `hr.read_all` und `hr.upload_payslip` empfohlen (Tenant-Admin-Setting)

M35 DSGVO-Export / Löschung

- HR-Daten werden vollständig in MA-Datenexport eingeschlossen
- Bei MA-Löschung aus Workspace: HR-Profil + Dokumente + Payslips bleiben **Audit-Compliance-konform** archiviert (gesetzliche Aufbewahrungspflichten 6/10 Jahre); PII anonymisiert wo möglich

---

Block O — Permissions-Anwendung

Permission-IDs

Permission	Erlaubt
`hr.read_own`	Eigene Profildaten, eigene Dokumente, eigene Payslips, eigene Anträge, eigene Krankmeldungen, eigene Survey-Submissions
`hr.read_team`	Profile + Anträge des eigenen Teams (User mit `manager_user_id = self`) — typisch PL/Bauleiter
`hr.read_all`	Alle MA-Profile (außer sensible Felder), alle Anträge, alle Krankmeldungen-Stammdaten (kein AU-Cert), Standorte, Verzeichnis voll
`hr.read_sensitive`	AU-Bescheinigungen, Notfallkontakt-Daten, Lohnabrechnungen aller MA, sensible Dokumente
`hr.write_own`	Eigene Profilfelder editieren, eigene Anträge stellen, eigene Dokumente hochladen, eigene Krankmeldung melden, eigenen Urlaub beantragen
`hr.approve_team`	Anträge und Urlaube des eigenen Teams genehmigen/ablehnen
`hr.approve_all`	Anträge und Urlaube tenant-weit genehmigen/ablehnen
`hr.upload_payslip`	Payslips hochladen / löschen
`hr.write_announcement`	Announcements anlegen + bearbeiten
`hr.publish_announcement`	Announcements veröffentlichen + pinnen
`hr.write_resource`	Resources / Quick-Links anlegen + verwalten
`hr.write_survey`	Surveys anlegen + veröffentlichen + auswerten
`hr.write_request_template`	Request-Templates verwalten
`hr.write_upload_reminder`	Upload-Reminder verwalten
`hr.manage_employees`	MA-Profile editieren (Personalnummer, Manager, Position, Location, Hire-Date)
`hr.password_safe.access`	Genereller Zugang zum Password-Safe-Modul (zusätzlich pro Vault `EmployeePasswordSafeAccess`)
`hr.password_safe.admin`	Vault-Verwaltung tenant-weit
`hr.admin`	Voll-Verwaltung HR (alles obige)

Bundle-Mapping (Variante 2)

Bundle	Atomare Permissions
`hr.none`	(keine — User hat keinen HR-Hub-Tab in Sidebar)
`hr.employee`	`read_own` + `write_own` + `password_safe.access` (Vault-Access kommt pro Vault)
`hr.team_lead`	obigen + `read_team` + `approve_team`
`hr.office`	obigen + `read_all` + `read_sensitive` + `upload_payslip` + `manage_employees` + `write_announcement` + `write_resource`
`hr.admin`	alle

Default-Rollen-Zuweisung (SHK-Template)

Rolle	HR-Bundle
GF	`hr.admin`
Vertriebsleiter	`hr.team_lead`
Vertriebler	`hr.employee`
Projektleiter / Bauleiter	`hr.team_lead`
Büro / Backoffice	`hr.office`
Marketing	`hr.employee`
Monteur	`hr.employee`

Anwendung in Routes

Route	Permission
`/{tenant}/hr`	`hr.read_own` (alle eingeladenen User mind.)
`/{tenant}/hr/announcements`	`hr.read_own`
`/{tenant}/hr/announcements/new`	`hr.write_announcement`
`/{tenant}/hr/documents`	`hr.read_all`
`/{tenant}/hr/my-documents`	`hr.read_own`
`/{tenant}/hr/leave`	`hr.read_own` (eigene); `hr.approve_team` / `hr.approve_all` (Genehmigungs-Tab); `hr.read_team` / `hr.read_all` (Team-Übersicht)
`/{tenant}/hr/leave/new`	`hr.write_own`
`/{tenant}/hr/leave/vacation/:id`	Owner-Check (Antragsteller) ODER `hr.approve_team` mit Team-Match ODER `hr.approve_all`
`/{tenant}/hr/leave/sick/:id`	Owner-Check ODER `hr.read_team` / `read_all` (ohne Cert) bzw. `hr.read_sensitive` (mit Cert)
`/{tenant}/hr/locations`	`hr.read_own` (jeder im Tenant)
`/{tenant}/hr/payslips`	`hr.read_own`
`/{tenant}/hr/payslips/:id`	Owner-Check (eigener User) ODER `hr.read_sensitive` (HR-Admin / Büro)
`/{tenant}/hr/password-safe`	`hr.password_safe.access` (zusätzlich pro Vault Access)
`/{tenant}/hr/quick-links`	`hr.read_own`
`/{tenant}/hr/resources`	`hr.read_own`
`/{tenant}/hr/surveys`	`hr.read_own` (für Audience-Match)
`/{tenant}/hr/surveys/:id/results`	`hr.write_survey` ODER `result_visibility=all_participants`
`/{tenant}/hr/requests`	`hr.read_own` (eigene); `hr.approve_team` / `approve_all` für Genehmigungs-Sicht
`/{tenant}/hr/requests/new`	`hr.write_own`
`/{tenant}/hr/directory`	`hr.read_own` (alle eingeladenen User dürfen Verzeichnis sehen, aber sensible Felder gegated)
`/{tenant}/hr/directory/:userId`	analog (sensible Felder über `hr.read_sensitive`)
`/{tenant}/admin/hr/announcements`	`hr.write_announcement` + `hr.publish_announcement`
`/{tenant}/admin/hr/documents`	`hr.read_all` + `hr.read_sensitive`
`/{tenant}/admin/hr/locations`	`hr.admin`
`/{tenant}/admin/hr/payslips`	`hr.upload_payslip`
	`hr.upload_payslip`

Route	Permission
`/{tenant}/admin/hr/payslips/upload`	
`/{tenant}/admin/hr/leave`	`hr.read_all` + `hr.approve_all`
`/{tenant}/admin/hr/upload-reminders`	`hr.write_upload_reminder`
`/{tenant}/admin/hr/quick-links`	`hr.write_resource`
`/{tenant}/admin/hr/resources`	`hr.write_resource`
`/{tenant}/admin/hr/surveys`	`hr.write_survey`
`/{tenant}/admin/hr/request-templates`	`hr.write_request_template`
`/{tenant}/admin/hr/password-safe`	`hr.password_safe.admin`
`/{tenant}/admin/hr/employees`	`hr.manage_employees`

Owner-Check-Logik

- `read_own` / `write_own`: Server-Side-Prüfung `entity.user_id = current_user.id` für User-bezogene Tabellen
- `approve_team`: Server-Side-Prüfung `request.requester.manager_user_id = current_user.id`
- `read_team`: gleiches Manager-Pattern
- Bei Fehl-Match: 404 statt 403 (LP-9 Information-Hiding)

UI-Anwendung

- Sidebar-Sub-Menü dynamisch je nach Permissions: ein User mit nur `hr.employee` sieht keinen Admin-Bereich
- Action-Buttons (z.B. *„Genehmigen"*) nur sichtbar mit passender Permission
- Sensible Feld-Werte (Notfallkontakt, AU-Cert-Link) maskiert/ausgeblendet ohne `hr.read_sensitive`
- Lohnabrechnungs-Datei: Download-Link nur für Owner ODER `hr.read_sensitive`

Klartext-Fehler

- Antragsteller versucht Genehmigungs-Tab zu öffnen ohne Permission: Tab gar nicht sichtbar
- Approver versucht zu genehmigen, ist aber nicht Manager des Antragstellers: 404 mit *„Antrag nicht gefunden"*
- MA versucht fremde Krankmeldung anzusehen: 404
- HR-Admin versucht Payslip zu löschen: Klartext *„Lohnabrechnungen sind 10 Jahre aufzubewahren. Stattdessen archivieren?"* — tatsächlicher Hard-Delete erfordert sekundären Bestätigungs-Schritt + Audit-Log

---

Block P — Datenschutz / sensible Daten

Klassifizierung

Stufe 1 — Öffentlich im Tenant:
- MA-Verzeichnis-Stammdaten (Name, Position, Team, Standort, Business-Phone, Avatar, Bio)

- Quick-Links, Resources, Locations
- Announcements (audience-gemäß)

Stufe 2 — Mitarbeiter-vertraulich (eigener User + HR-Admin):
- Profil-Felder (Birthdate, Hire-Date, Address, Private-Phone, Notfallkontakt)
- Eigene Dokumente
- Eigene Anträge / Surveys
- Eigene Krankmeldungs-Stammdaten

Stufe 3 — Streng vertraulich (`hr.read_sensitive` only):
- Lohnabrechnungen
- AU-Bescheinigungs-Files
- Personalnummer
- Vertragliche Detail-Dokumente

Stufe 4 — Verschlüsselt (Password-Safe):
- Vault-Einträge — siehe Block J

Compliance-Pflichten

- **DSGVO-Auskunftsrecht:** MA kann alle eigenen Daten als JSON+Files exportieren (siehe M35)
- **DSGVO-Löschungsrecht:** auf Anfrage werden Daten anonymisiert wo gesetzliche Aufbewahrungspflicht es nicht verbietet
- **Aufbewahrungspflichten DE:**
- Lohnabrechnungen: 10 Jahre
- Arbeitsverträge / Kündigungen: 10 Jahre
- AU-Bescheinigungen: 4 Jahre
- Genehmigte Urlaube / Krankmeldungen: 4 Jahre
- Bei MA-Austritt: Daten werden archiviert mit `archived_at`, automatischer Hard-Delete-Job nach Aufbewahrungsfrist + 1 Monat (Cron, mit Klartext-Vorschau-Hinweis an HR-Admin 30 Tage vorher)

Audit

- Jeder Read auf `hr.read_sensitive`-Daten: Audit-Eintrag (User, Subject, Timestamp, IP)
- Jede Password-Safe-Reveal-Action: Audit-Eintrag (Block J)
- Jede Payslip-Download-Action: Audit-Eintrag
- Audit-Log einsehbar nur durch Tenant-Admin / HR-Admin

2FA-Empfehlung

- Tenant-Admin-Setting: 2FA-Pflicht für User mit `hr.read_sensitive` und `hr.password_safe.admin`
- Default empfohlen, aber per Tenant-Admin überschreibbar (siehe M27 B.4)

Block Q — Klartext-Hinweise

Allgemein

- Empty-State Hub ohne Inhalt: *„Hier wirst du Bekanntmachungen, deine Lohnabrechnungen und mehr finden."*
- HR-Hub für deaktivierten Tenant (frozen): nur Read, Klartext-Banner *„Workspace ist pausiert — neue Anträge nicht möglich"*

Urlaub

- Antrag erfolgreich gestellt: *„Dein Urlaubsantrag wurde an [Manager] gesendet. Du erhältst eine Benachrichtigung, sobald über deinen Antrag entschieden wurde."*
- Genehmigung: *„Dein Urlaub vom [Datum] bis [Datum] wurde genehmigt — Calendar-Eintrag wurde erstellt."*
- Ablehnung: *„Dein Urlaubsantrag wurde abgelehnt. Begründung: [decision_note]"*
- Konflikt: *„In diesem Zeitraum sind bereits 2 Mitarbeiter im Urlaub (Max M., Lisa K.). Trotzdem genehmigen?"*
- Approver-Notification: *„[Mitarbeiter] beantragt Urlaub vom [Datum] bis [Datum] ([N] Arbeitstage). [Genehmigen] [Ablehnen]"*

Krankmeldung

- Erfasst: *„Krankmeldung für [Datum] wurde aufgenommen — dein Vorgesetzter und das Büro sind informiert. Gute Besserung!"*
- AU-Bescheinigung-Reminder am 3. Tag: *„Bitte lade bis morgen die AU-Bescheinigung hoch."*
- Rückkehr melden: *„Willkommen zurück! Bitte trage deinen ersten Arbeitstag ein."*

Payslip

- Neue Lohnabrechnung verfügbar: *„Deine Lohnabrechnung [Monat/Jahr] ist bereit. [Öffnen]"*
- Bulk-Upload-Erfolg: *„42 von 45 Lohnabrechnungen erfolgreich zugeordnet. 3 Files ohne Match — bitte manuell prüfen."*
- Upload Doppel-Versuch: *„Für [MA] existiert bereits eine Lohnabrechnung [Monat/Jahr]. Als Korrektur hochladen?"*

Upload-Reminder

- Pendant: *„Bitte aktualisiere deinen Führerschein-Scan bis [Datum]."*
- Überfällig: *„Dein Führerschein-Scan ist seit [Datum] überfällig — bitte zeitnah einreichen."*
- Überfällig + Manager-Eskalation: *„[MA] hat den Reminder ‚Führerschein' seit 7+ Tagen nicht erfüllt."*

Password-Safe

- Reveal: *„Wert wird für 30 Sekunden angezeigt und automatisch ausgeblendet."*
- Eintrag-Anlage erfolgreich: *„Eintrag verschlüsselt gespeichert. Nur User mit Vault-Zugriff können den Wert entschlüsseln."*
- Vault-Access entzogen: *„Dein Zugriff auf Vault [Name] wurde entfernt."*

Announcements

- Acknowledgement-Pflicht: *„Bitte bestätige, dass du die Information gelesen hast."*
- Veröffentlichung: *„Bekanntmachung wurde an [Audience-Beschreibung, z.B. „alle Mitarbeiter (28)"] veröffentlicht. Push-Benachrichtigungen wurden ausgelöst."*

Requests

- Antrag pending: *„Dein Antrag ‚[Titel]' wurde an [Approver] geschickt."*
- Approver-Internal-Note: *„[Notiz] (intern, nur für Genehmiger sichtbar)"*

Surveys

- Anonym-Hinweis: *„Diese Umfrage ist anonym — deine Antworten werden nicht mit deinem Namen verknüpft gespeichert."*
- Bereits teilgenommen: *„Du hast an dieser Umfrage bereits teilgenommen. Mehrfach-Teilnahme ist nicht möglich."*

Block R — Phase 2

- **Resturlaub-Kontingent-Tracking:** pro MA Soll/Ist-Vergleich, automatische Verrechnung, Übertrag ins Folgejahr
- **Mehr-Stufen-Genehmigungs-Workflows:** Manager → HR → GF
- **Bulk-Approve** für Anträge
- **Anonyme Whistleblower-Inbox** als spezielle Request-Variante
- **Onboarding-Checklisten** pro neuem MA (mit verlinkten Forms, Tasks, Reminders)
- **Offboarding-Checklisten**
- **Resource-Booking** (z.B. Firmenwagen, Werkstatt-Zeitfenster)
- **MA-Befragung-Auto-Versand** (z.B. monatlich Pulse-Survey)
- **Geburtstags-Auto-Announcement** an MA selbst und Team
- **Krankheits-Statistiken** für HR-Admin (anonymisiert nach DSGVO)
- **Multi-Sprachen-Profil** (i18n M30)
- **Master-Key-Rotation** für Password-Safe
- **2FA-Hardware-Key-Pflicht** für Password-Safe-Admin
- **Vacation-Calendar-Sharing** auf Standort-Ebene mit konfigurierbaren Sicht-Levels
- **Quiply-Migrations-Tool** (Datenimport für Bestandskunden)
- **Skill-/Qualifikations-Matrix** pro MA
- **Integration mit externen Lohn-Systemen** (DATEV, Lexware) — über Apps Engine M33a
- **Survey-Word-Cloud / Sentiment-Analyse** (KI M18, EU-Provider)
- **Erweiterte Audit-Reports** (DSGVO-Compliance-Reports)
- **Custom-Felder pro HrEmployeeProfile** (analog M1 Custom-Felder)
- **Mehr Reaction-Emojis** (Tenant-Admin-konfigurierbar)
- **Threading-Tiefe > 1** für Announcement-Comments
- **Conditional-Audience** (z.B. nur User mit Tag X)

Architektur-Vorschriften (Querschnitt)

- **LP-2:** Mobile-First für eigene Anträge, Krankmeldung, Payslip-Viewer
- **LP-3, AV #3:** SHK-Template-Seeding für Request-Templates, Default-Reminder, Default-Announcements
- **LP-7:** Quiply-Komplett-Ablösung — alle dort genutzten Funktionen müssen in Phase 1 abgedeckt sein
- **LP-9:** UI-Element-Anforderungen als Liste, kein Layout
- **LP-10, AV #1:** Klartext-Diagnostik überall (Beispiele in Block Q)
- **LP-13:** EU-Stack für sensible Daten — Storage in Scaleway-Buckets, KMS in Scaleway, kein US-Cloud-Provider
- **AV #5:** Permissions-aware-Default in allen Listen/Suchen
- **AV #6:** Audit-Trail-Default für alle schreibenden Aktionen UND für sensible Reads (Payslip, Sick-Cert, Password-Safe)
- **AV #7:** Feature-Flag-Hülle für neue HR-Features (z.B. `hr.feature_resturlaub_tracking`)
- **AV #20:** KI darf keine Anträge / Genehmigungen ohne User-Bestätigung auslösen

---

Detail-Spec-Status: DRAFT

Erste vollständige Detail-Spec für Modul 14 (HR-Hub). **Vor Bau:** Verifizierung mit Noah, speziell zu:
- DE-Aufbewahrungsfristen-Mapping (10/4 Jahre)
- Quiply-Feature-Parität-Sweep (welche Features fehlen ggf. noch)
- Default-Approver-Logik bei Multi-Manager-MA
- Master-Key-Architektur und KMS-Integration (Scaleway-KMS-Details)

Offene Detail-Punkte (nicht-blockierend):
- DE-Feiertagskalender pro Bundesland (Datenquelle / Library)
- AU-Bescheinigungs-Pflicht-Tag konfigurierbar pro Tenant (3-Tage-Default)
- Auto-Match-Pattern für Payslip-Bulk-Upload (Tenant-konfigurierbar)
- Konkrete SHK-Default-Templates für Request, Survey, Announcement
- Subframe-UI-Designs (separat)
- Cron-Frequenz für Reminder-Engine (täglich vs. stündlich)
- Performance-Strategie für Aggregat-Queries auf Plantafel-Konflikt-Detection bei 50+ MA
- Mehrfach-Sprache der Klartext-Fehler in Phase 2 (heute DE-only)

Abhängige Module:
- M27 (Auth/Permissions) — Permission-IDs werden hier registriert
- M5 (Form Builder) — Templates für Krankmeldung/Urlaubsantrag/Request-Forms
- M4 (Auftragspipeline) — Plantafel-Konflikt-Detection
- M22 (Notifications) — alle Push/Email-Versende
- M25 (Calendar) — Urlaubs-Calendar-Events
- M17 (Automation) — Trigger + Actions
- M23 (Files) — Storage für alle Anhänge
- M35 (DSGVO-Export) — HR-Daten in Export inkludieren