```
module: 15
title: Customer-Portal (Endkunden-Login)
phase: 1
status: detail-spec-draft
last_updated: 2026-05-08
session_source: brainstorming-session-2026-05-07-2206.md
related_lps: [LP-1, LP-2, LP-3, LP-7, LP-9, LP-10, LP-13]
spec_style: requirements-pur
```

Modul 15 — Customer-Portal (Endkunden-Login)

> ***Detail-Spec gemäß LP-9.*** *Endkunden-Sicht auf eigene Projekte, Dokumente und Status. Kritisch für Geerkens-Launch (User-Korrektur). Eigene Auth-Schicht parallel zu M27 (separate* `PortalUser` *-Klasse,* ***NICHT*** `TenantUser` *). URL-Schema* `app.hivegrid.de/portal/{tenant}/...` *.*

Themenblöcke

```
A. Datenmodell (Portal, PortalUser, Auth, ProjectAccess, Documents)
B. Menü-Struktur und Routes (Portal-Seite + Tenant-Admin-Seite)
C. Auth-Schicht (Magic-Link + Pwd, Setup-Flow, Session)
D. Portal-Endkunden-Views (Dashboard, Projekte, Dokumente, Upload)
E. Tenant-Admin-Konfiguration (Phasen-Sichtbarkeit, Doc-Freigabe, Templates, Branding)
F. PortalUser-Lifecycle (Anlage, Einladung, Reset, Entfernen)
G. Auto-Status-Mails bei Phasenwechsel
H. Integration mit anderen Modulen
I. Permissions-Anwendung (Tenant-Seite + Portal-Seite)
J. DSGVO / Lösch-Workflow
K. Klartext-Hinweise/-Fehler
L. Phase 2 / spätere Features
```

Block A — Datenmodell

Architektur-Entscheidung

PortalUser ist **eigene User-Klasse**, vollständig getrennt vom internen `TenantUser` aus M27. Begründung:
- Andere Auth-Anforderungen (Magic-Link primär, kein 2FA-Pflicht, kein Tenant-Admin-Konzept)
- Andere Permissions (nur eigene Projekte sehen, keine Modul-Permissions)
- Andere Lifecycle-Events (keine Onboarding-Wizards, kein Tenant-Switcher)
- Andere DSGVO-Klassifizierung (Endkunde = Datensubjekt, MA = Mitarbeiter)
- Vermeidung von Permission-Eskalation (Endkunde darf niemals versehentlich Tenant-Permissions erhalten)

Kern-Entitäten

```
Portal                          – ein Portal pro Tenant (Phase 1: Default-Portal pro Tenant)
PortalUser                      – Endkunde mit Login
PortalUserRegistration          – Setup-Flow-Token (erstes Login + Pwd-Setzen + Profil)
CustomerPortalAccount           – Account-Daten zu PortalUser (Pwd-Hash, Profil, Status)
CustomerPortalMagicLinkToken    – kurzlebige Login-Token
CustomerPortalSession           – Server-Side-Session pro PortalUser
CustomerPortalProjectAccess     – welcher PortalUser sieht welches Project
CustomerPortalProjectDocument   – welche Files innerhalb eines Project sind freigegeben
PortalConfiguration             – Tenant-Konfiguration (Phasen-Sichtbarkeit, Doc-Freigabe-
Defaults, Branding)
PortalEmailTemplate             – Auto-Status-Mail-Templates pro Tenant
```

Portal

- `id`, `tenant_id` (unique pro Tenant in P1 — ein Default-Portal), `created_at`, `updated_at`
- `slug` (default `portal`, in P1 nicht änderbar — URL-Schema-Stabilität)
- `name` (User-sichtbar, z.B. „Geerkens Kundenbereich")
- `is_default` (true für P1)
- `enabled` (Boolean — Tenant kann Portal deaktivieren ohne Daten-Verlust)
- `archived_at`

Phase 2: mehrere Portale pro Tenant mit unterschiedlichem Branding/Slug.

PortalUser

- `id`, `tenant_id`, `portal_id`, `created_at`, `updated_at`, `created_by_user_id` (TenantUser, der Zugang anlegte)
- `email` (Pflicht, unique pro Portal — Login-Identifier)
- `first_name`, `last_name` (Pflicht)
- `phone` (optional)
- `language` (DE/EN, default DE — für Auto-Mails)
- `linked_contact_id` (FK auf `Contact` aus M1 — verknüpft mit Stammdaten, optional, kann nachträglich verknüpft werden)
- `linked_company_id` (FK auf `Company` aus M1, optional)
- `status` (Enum: `pending_setup | active | disabled | deleted`)
- `last_login_at`
- `archived_at`

Wichtig: `linked_contact_id` ist optional, weil PortalUser auch unabhängig vom CRM angelegt werden kann (z.B. Bauherr ohne CRM-Eintrag). Verknüpfung empfohlen für vollen Funktionsumfang.

CustomerPortalAccount

- `id`, `portal_user_id` (1:1)
- `password_hash` (nullable — Magic-Link-Only-Modus möglich)
- `password_set_at`
- `email_verified_at`
- `failed_login_attempts`, `locked_until`
- `last_password_reset_at`
- `terms_accepted_at` (DSGVO)
- `marketing_opt_in` (Boolean, default false)

CustomerPortalMagicLinkToken

- `id`, `portal_user_id`, `tenant_id`
- `token_hash` (64-Zeichen, kryptographisch sicher, URL-safe — gespeichert als Hash)
- `purpose` (Enum: `login | setup | password_reset | email_verification`)
- `created_at`, `expires_at`, `used_at` (NULL bis Verwendung)
- `requested_ip`, `requested_user_agent`

Lebenszeiten:
- `login`: 15 Minuten
- `setup`: 7 Tage
- `password_reset`: 1 Stunde
- `email_verification`: 24 Stunden

CustomerPortalSession

- `id`, `portal_user_id`, `tenant_id`, `portal_id`
- `created_at`, `last_activity_at`, `expires_at`
- `ip_address`, `user_agent`
- `revoked_at`

Default-Lebenszeit: 30 Tage Sliding-Window (analog M27 B.5, aber ohne 2FA-Re-Verify).

PortalUserRegistration

- `id`, `portal_user_id`, `tenant_id`, `setup_token_id` (FK auf MagicLinkToken mit `purpose=setup`)
- `created_at`, `completed_at`
- `created_by_user_id` (TenantUser)
- `welcome_message` (Freitext aus Einladungs-Modal — wird in Setup-Mail eingebettet)

CustomerPortalProjectAccess

- `id`, `tenant_id`, `portal_user_id`, `project_id`
- `granted_at`, `granted_by_user_id` (TenantUser)
- `revoked_at` (Soft-Revoke — Zugriff entzogen, History bleibt)
- `access_level` (Enum: `read_status_only | read_full` — `read_status_only` zeigt nur Phase, keine Files/Details; default `read_full`)

Indizes: `tenant_id, portal_user_id`, `tenant_id, project_id`.

Wichtig: Mehrere PortalUser können auf dasselbe Projekt Zugriff haben (z.B. Bauherr + Architekt). Ein PortalUser kann mehrere Projekte sehen.

CustomerPortalProjectDocument

- `id`, `tenant_id`, `project_id`, `file_id` (FK auf File aus M23)
- `released_at`, `released_by_user_id`
- `revoked_at`
- `release_kind` (Enum: `manual | auto_by_doc_type | auto_by_acceptance` — wie wurde freigegeben)
- `customer_visible_filename` (optional Override des Dateinamens für Endkunde)

Default-Logik: Files aus Project sind **nicht** automatisch freigegeben. Tenant-Admin konfiguriert pro Doc-Typ (Angebot/Rechnung/Acceptance) automatische Freigabe-Regel; Einzel-Files können manuell freigegeben oder gesperrt werden.

PortalConfiguration

- `id`, `tenant_id`, `portal_id` (1:1 in P1)

- `visible_pipeline_stages` (JSON pro Pipeline: `{ pipeline_id: [stage_id, stage_id, ...] }`) — welche Stages sieht der Endkunde
- `stage_display_labels` (JSON: `{ stage_id: "Kunden-Label" }`) — Override für Klartext-Bezeichnung gegenüber Endkunde
- `auto_release_doc_types` (JSON-Array: `["angebot", "rechnung", "acceptance_pdf"]` — diese Doc-Typen werden bei Anlage/Generierung automatisch freigegeben)
- `auto_status_mail_enabled` (Boolean pro Stage-Wechsel-Event)
- `branding_logo_file_id` (Phase 1: nutzt Tenant-Logo aus M27; Phase 2: Portal-eigenes Logo)
- `branding_primary_color` (Phase 1: nutzt Tenant-Farbe; Phase 2: Portal-eigene Farbe)
- `welcome_message_default` (Freitext — wird im Setup-Flow gezeigt)
- `support_email` (Default = Tenant-Support-Email)
- `support_phone` (optional)
- `imprint_url`, `privacy_url` (Pflicht — Endkunde muss Tenant-Impressum + Datenschutz erreichen)
- `terms_url` (optional, falls Tenant Sonder-AGB für Portal hat)

PortalEmailTemplate

- `id`, `tenant_id`, `portal_id`
- `template_kind` (Enum: `setup_invitation | login_magic_link | password_reset | stage_changed | document_released | upload_received`)
- `subject` (mit Platzhaltern: `{{customer_name}}`, `{{project_title}}`, `{{stage_name}}`, ...)
- `body` (Markdown mit Platzhaltern)
- `from_email_address_id` (FK auf verbundene Sending-Domain aus M9; default Tenant-Default)
- `is_active` (Boolean)

Default-Templates werden beim Tenant-Anlegen geseedet (DE-Klartext, Tenant-Admin kann anpassen).

PortalSubscription* (Phase 2 — Stub)

- Vorgesehen für Abos im Portal (Wartungs-Abo, Service-Pakete) — nicht in P1.

Block B — Menü-Struktur und Routes

Endkunden-Routes (öffentlich erreichbar)

```
/portal/{tenant}/                          → Portal-Dashboard (Login-required)
/portal/{tenant}/login                     → Login (Magic-Link + Pwd)
/portal/{tenant}/login/magic-sent          → Bestätigung „Link versendet"
/portal/{tenant}/setup/{token}             → Erst-Login-Setup (Pwd setzen, Profil)
/portal/{tenant}/forgot-password           → Pwd-Reset-Anfrage
/portal/{tenant}/reset-password/{token}    → Neues Pwd setzen
/portal/{tenant}/verify-email/{token}      → Email-Verification

/portal/{tenant}/projects                  → Liste eigener Projekte
/portal/{tenant}/projects/:id              → Project-Detail (Endkunden-Sicht)
/portal/{tenant}/documents                 → Alle freigegebenen Dokumente (Cross-Project)
/portal/{tenant}/upload                    → Datei-Upload (z.B. Reklamations-Fotos)
/portal/{tenant}/forms/:formSlug           → Form ausfüllen (Reklamation, Service-Anfrage – über
M5)

/portal/{tenant}/settings/                 → Profil + Pwd ändern + Email ändern
/portal/{tenant}/settings/notifications    → Email-Notification-Präferenzen
/portal/{tenant}/settings/account-delete   → DSGVO-Lösch-Antrag
/portal/{tenant}/logout                    → Logout

/portal/{tenant}/imprint                   → Impressum (verlinkt aus PortalConfiguration)
/portal/{tenant}/privacy                   → Datenschutz
```

Wichtig: Portal-Routes nutzen **eigene Auth-Middleware** (`requirePortalUser`), unabhängig von M27 `requireTenantUser` . Cookies/Sessions sind getrennt — ein TenantUser mit aktiver M27-Session kann das Portal nicht ohne separaten PortalUser-Login betreten.

Tenant-Admin-Routes (im Tenant-Workspace)

```
/{tenant}/admin/portal/                    → Portal-Konfiguration (Phasen-Sichtbarkeit, Doc-
Freigabe, Branding, Auto-Mails)
/{tenant}/admin/portal/users               → PortalUser-Verwaltung (Liste, Anlage, Reset,
Entfernen)
/{tenant}/admin/portal/users/:id           → PortalUser-Detail
/{tenant}/admin/portal/access              → Cross-Project-Übersicht: welcher PortalUser sieht
welches Project
/{tenant}/admin/portal/email-templates     → Auto-Status-Mail-Templates editieren
/{tenant}/admin/portal/audit               → Portal-Audit (Logins, Uploads, Doc-Zugriffe)
```

Tenant-Workspace-Erweiterungen (in bestehenden Modulen)

- **Project-Detail (M4):** Sektion *„Customer-Portal"* mit:
- Liste der PortalUser mit Zugang zu diesem Project
- Button „PortalUser einladen" (öffnet Modal — kann aus verknüpftem Contact vorausgefüllt werden)
- Pro File: Toggle „Im Customer-Portal freigegeben" (mit Wirkung auf `CustomerPortalProjectDocument`)
- Toggle „Auto-Status-Mails an Kunde aktiv für dieses Project" (Override pro Project)
- **Contact-Detail (M1):** Sektion *„Portal-Zugang"* mit:
- Falls verknüpfter PortalUser: Status, Letzter Login, Liste sichtbarer Projekte
- Falls nicht: Button „Portal-Zugang einladen"
- **Deal-Detail (M3):** Toggle „Sales-Phase im Portal sichtbar" — aktiviert Portal-Zugang ab Lead/Deal-Phase (vor Project-Anlage)

Block C — Auth-Schicht

C.1 — Magic-Link-Login (primär)

Flow:

1. Endkunde öffnet `/portal/{tenant}/login`
2. Tippt Email → Submit
3. System prüft: existiert PortalUser mit Email + Status `active` für diesen Tenant?
   - **Ja:** Token erzeugen, Email senden mit Link `/portal/{tenant}/auth/magic/{token}` (15 Min Lebenszeit, einmalig)
   - **Nein:** trotzdem „Link versendet" anzeigen (kein User-Enumeration), aber keine Mail senden
4. Endkunde klickt Link → Token-Validierung → Session erzeugt → Redirect zu `/portal/{tenant}/`

Rate-Limits:
- Pro Email: max. 3 Magic-Link-Anfragen / 15 Min
- Pro IP: max. 10 / Stunde
- Captcha (hCaptcha) ab 3. Anfrage in Folge

Klartext-Hinweise:
- Token abgelaufen: *„Der Link ist abgelaufen. [Neuen Link anfordern]"*
- Token bereits genutzt: *„Dieser Link wurde bereits verwendet. [Neuen Link anfordern]"*
- Email nicht zugestellt: *„Email nicht angekommen? Prüfe Spam-Ordner oder kontaktiere [Support-Email]."*

C.2 — Email + Passwort (optional)

- Endkunde kann beim Setup oder in Settings ein Pwd setzen
- Pwd-Anforderungen analog M27 B.1 (NIST: 12 Zeichen min., HIBP-Check, Bcrypt Cost 12)
- Login mit Email + Pwd → Session erzeugt
- **Kein 2FA-Pflicht** in P1 für PortalUser
- Rate-Limit: 5 Fehlversuche / 15 Min → 15 Min Lockout pro Email

C.3 — Erst-Login-Setup (`/portal/{tenant}/setup/{token}`)

Flow:

1. TenantUser legt PortalUser an + verschickt Setup-Einladung → System erzeugt `PortalUserRegistration` mit 7-Tage-Setup-Token
2. Endkunde klickt Link → Setup-Page lädt mit:
   - Begrüßungs-Klartext (Tenant-Welcome-Message)
   - Vorausgefüllte Email (read-only)
   - Vor-/Nachname (vorausgefüllt, editierbar)
   - Telefon (optional)
   - Sprache (Default DE)
   - Pwd-Setzen-Felder (mit Live-Validation und HIBP-Check)
   - Pwd-Skip-Option (*„Lieber per Magic-Link einloggen"* — Pwd kann später jederzeit gesetzt werden)
   - DSGVO-Klartext + Akzeptanz-Checkbox (Pflicht)
   - Marketing-Opt-In (optional)
3. Submit → PortalUser-Status auf `active`, Setup-Token verbraucht, Session erzeugt, Redirect zu `/portal/{tenant}/`

Token abgelaufen oder bereits genutzt: Klartext + Funktion „Neuen Link bei [Tenant] anfordern" → erzeugt Support-Email.

C.4 — Pwd-Reset (`/portal/{tenant}/forgot-password`)

- Email eingeben → Magic-Link mit `purpose=password_reset` (1 Std)
- Klick → neue Pwd setzen → alle aktiven Sessions invalidiert
- Klartext analog C.1 (kein User-Enumeration)

C.5 — Email-Verification

- Beim Setup: Email gilt als verifiziert, weil Magic-Link erfolgreich war
- Beim Email-Ändern in Settings: Verification-Token an neue Email, alter Email-Adresse Klartext-Hinweis-Mail
- Bis Verification: alte Email bleibt aktiv

C.6 — Session-Management

- Server-Side-Sessions in Postgres (analog M27 B.5)
- HTTP-only, Secure, SameSite=Lax Cookie
- Cookie-Name **eindeutig vom TenantUser-Cookie getrennt** (`hg_portal_session` vs. `hg_session`) — verhindert Cross-Class-Verwechslung
- 30 Tage Sliding-Window
- Inaktivitäts-Timeout: 7 Tage ohne Aktivität → Re-Login
- Bei Pwd-Änderung: alle Sessions invalidiert
- Bei `PortalUser.status = disabled | deleted`: alle Sessions invalidiert
- Session-Übersicht in `/portal/{tenant}/settings/`: Liste aktiver Sessions mit Logout-Funktion + globaler „Von allen Geräten abmelden"

C.7 — Permission-Check pro Request

- Middleware prüft auf jeder `/portal/{tenant}/...`-Route:
- Existiert Session?
- Ist Session valid + nicht revoked + nicht expired?
- Ist `PortalUser.status = active`?
- Ist `Portal.enabled = true`?
- Ist `Tenant.status` nicht `suspended | deleted`?
- Bei `tenant.status = frozen`: Read-Only-Modus (analog M27 A.5 — Login + Read OK, Upload + Form-Submit gesperrt mit Klartext)
- Resource-Access-Check: bei Project-Detail-Aufruf wird `CustomerPortalProjectAccess` geprüft, bei File-Aufruf zusätzlich `CustomerPortalProjectDocument`
- Bei fehlender Permission: 404 (nicht 403 — keine Existenz-Offenlegung gegenüber Endkunde)

Block D — Portal-Endkunden-Views

D.1 — Portal-Dashboard (`/portal/{tenant}/`)

Zu zeigende Daten:

- Begrüßung mit Vorname
- Übersicht der eigenen Projekte (Anzahl aktiv, Anzahl abgeschlossen)
- Liste der **letzten Status-Änderungen** über alle eigenen Projekte (chronologisch)
- Liste der **zuletzt freigegebenen Dokumente**
- Schnell-Aktionen (Funktionen): Projekt anschauen, Datei hochladen, Reklamation melden
- Support-Kontakt (Tenant-Support-Email + ggf. Telefon aus PortalConfiguration)

Benötigte UI-Elemente:

- Anzeige der oben genannten Daten in sektionierter Form
- Quick-Action-Funktionen für die genannten Schnell-Aktionen
- Logout-Funktion erreichbar
- Branding-Komponente (Logo + Primärfarbe aus PortalConfiguration)

Permissions:

- Erfordert aktive Portal-Session
- Daten-Filter automatisch auf eigene Projekte (über `CustomerPortalProjectAccess`)

Klartext-Hinweise:

- Keine Projekte zugewiesen: *„Aktuell ist Ihnen kein Projekt zugewiesen. Bei Fragen kontaktieren Sie [Support-Email]."*

D.2 — Projekte-Liste (`/portal/{tenant}/projects`)

Zu zeigende Daten pro Project:

- Project-Titel + Project-Nummer
- **Aktuelle Phase** (mit Tenant-konfiguriertem Klartext-Label aus `stage_display_labels`)
- Phasen-Fortschritt (visuelle Komponente — nur sichtbare Stages laut `visible_pipeline_stages`)
- Zeitraum (Start + erwartetes Ende)
- Baustellen-Adresse-Kurzform
- Letzte Status-Änderung (Datum)
- Anzahl freigegebener Dokumente
- Verantwortlicher Ansprechpartner (PL aus M4 mit Email + Telefon)

Benötigte UI-Elemente:

- Listen- oder Karten-Anzeige (Designer entscheidet)
- Filter-Funktion: aktiv / abgeschlossen / alle
- Sortier-Funktion: zuletzt aktualisiert / Start-Datum / Phase
- Such-Funktion (Volltext über Titel + Adresse)
- Klick auf Eintrag → Project-Detail

Permissions / Datenfilter:

- Server-side gefiltert nach `CustomerPortalProjectAccess.portal_user_id = self`
- Nur Einträge mit `revoked_at IS NULL`
- Bei `access_level = read_status_only`: keine Detail-Verlinkung, nur Phase + Phasen-Fortschritt

Klartext-Hinweise:

- Leere Liste: *„Sie haben aktuell keinen Projekt-Zugang. Bei Fragen kontaktieren Sie [Support]."*

D.3 — Project-Detail (`/portal/{tenant}/projects/:id`)

Zu zeigende Daten:

- Project-Titel + Project-Nummer
- Aktuelle Phase (Klartext-Label) + Phasen-Fortschritt (sichtbare Stages)
- Zeitraum + Baustellen-Adresse
- PL als Ansprechpartner mit Klick-zum-Mailen-Funktion
- **Status-Historie** (chronologisch, nur sichtbare Phasen-Wechsel)
- **Freigegebene Dokumente** (Liste mit Download-Funktion + Datum + Doc-Typ)
- **Mängel aus Acceptance** (falls vorhanden + freigegeben)
- **Form-Submissions des Endkunden zu diesem Projekt** (eigene Reklamationen etc.)
- Upload-Funktion für eigene Files (siehe D.5)

- Reklamations-Form-Funktion (über M5 Form mit Project-Vorausfüllung)

Benötigte UI-Elemente:

- Sektionierte Anzeige der oben genannten Daten
- Visuelle Phasen-Komponente (nur freigegebene Stages, Zwischenphasen werden zusammengefasst angezeigt — z.B. wenn 5 von 8 Stages sichtbar sind, dann 5 Schritte)
- Dokument-Liste mit Download-Funktion pro Eintrag
- Upload-Funktion (Drag-&-Drop + File-Picker, Mobile-Kamera-Direkt-Upload)
- Map-Anzeige der Baustellen-Adresse (optional, falls Tenant-Maps-Integration aktiv)
- Klartext-Anzeige zu Doc-Releases (*„Neu freigegeben am [Datum]"*)

Operationen:

- Dokumente runterladen (Audit-Log-Eintrag bei jedem Download)
- File hochladen (siehe D.5)
- Reklamation/Service-Anfrage absenden (siehe D.6)
- Email an PL schreiben (öffnet Mail-Client mit `mailto:` — keine portal-eigene Compose in P1)

Permissions / Datenfilter:

- Resource-Check via `CustomerPortalProjectAccess` (404 bei fehlendem Zugang)
- Nur Daten der `visible_pipeline_stages`-Liste
- Nur Files mit aktivem `CustomerPortalProjectDocument`-Eintrag (`revoked_at IS NULL`)
- Bei `access_level = read_status_only`: kein Detail-View, Redirect mit Klartext

Klartext-Hinweise:

- Project archiviert/abgeschlossen: Banner *„Dieses Projekt ist abgeschlossen. Bei Service-Anfragen melden Sie sich gerne — [Service-Funktion]."* (Portal bleibt nach Abschluss offen für Wartung/Service)
- Project gelöscht/Zugang entzogen: 404 mit generischem *„Projekt nicht gefunden"*

D.4 — Dokumente-Cross-View (`/portal/{tenant}/documents`)

Zu zeigende Daten:

- Liste aller freigegebenen Dokumente über alle eigenen Projekte
- Pro Eintrag: Datei-Name (oder `customer_visible_filename`), Doc-Typ, Project-Zuordnung, Freigabe-Datum, Größe

Benötigte UI-Elemente:

- Tabellarische Liste
- Filter-Funktion: Project, Doc-Typ, Zeitraum
- Such-Funktion
- Sortier-Funktion: Datum / Name / Project
- Download-Funktion pro Eintrag
- Bulk-Download (ZIP) — Phase 2

Permissions / Datenfilter:

- Filter über Join `CustomerPortalProjectAccess` × `CustomerPortalProjectDocument`

D.5 — Upload-Funktion (`/portal/{tenant}/upload`)

Zu zeigende Daten:

- Project-Auswahl (Dropdown der eigenen Projekte mit `read_full`-Access)
- Optional: Kategorie-Auswahl (Reklamation, Foto, Anhang, Sonstiges)
- Optional: Beschreibung (Freitext)

- Datei-Auswahl

Benötigte UI-Elemente:

- Project-Selektor
- Kategorie-Selektor
- Beschreibungs-Feld
- File-Picker + Drag-&-Drop-Zone
- Mobile-Kamera-Direkt-Funktion
- Multi-File-Upload (max. 10 gleichzeitig)
- Progress-Indikatoren pro Datei
- Klartext-Hinweis nach erfolgreichem Upload

Operationen:

- Datei wird in M23-Storage geschrieben (Pfad `tenants/{tenantId}/projects/{projectId}/portal-uploads/...`)
- Eintrag in M23 mit Quelle = `customer_portal_upload` + `uploaded_by_portal_user_id`
- Eintrag in Project-Activity-Stream mit Klartext: *„Kunde [Name] hat Datei [Filename] hochgeladen"*
- Trigger M17: `portal.kunde_uploaded_file` (Automation-Engine)
- Notification an PL via M22 (Push + Email-Digest)

Restriktionen:

- Max. 50 MB pro Datei (Tenant-konfigurierbar)
- Erlaubte Mime-Types: Bilder (jpg/png/webp/heic), PDF, Office-Docs, Audio (m4a/mp3 für Sprach-Notiz)
- Tenant-Admin kann pro Project Upload sperren
- Bei `Tenant.status = frozen`: Upload-Funktion gesperrt mit Klartext

Klartext-Hinweise:

- Upload erfolgreich: *„Datei [Filename] wurde an [Tenant-Name] gesendet. Sie erhalten eine Bestätigung per Email."*
- Datei zu groß: *„Die Datei ist größer als das erlaubte Maximum von 50 MB. Bitte komprimieren oder in mehrere Dateien aufteilen."*
- Mime-Type nicht erlaubt: *„Dieser Dateityp ist nicht erlaubt. Erlaubte Typen: [Liste]."*
- Project-Auswahl leer: *„Aktuell ist kein Projekt für Uploads verfügbar."*

D.6 — Forms (Reklamation, Service-Anfrage)

- Tenant-Admin definiert Forms via M5 (Subtyp `portal_form`)
- Endkunde ruft `/portal/{tenant}/forms/:formSlug` auf
- Form-Submission wird mit `portal_user_id` + ggf. `project_id` versehen
- Trigger M17: `portal.kunde_replied`
- Eintrag im Project-Activity-Stream

D.7 — Settings (`/portal/{tenant}/settings/`)

Profil:

- Vor-/Nachname editieren
- Telefon editieren
- Sprache wechseln
- Email ändern (mit Verification an neue + Hinweis-Mail an alte)

Sicherheit:

- Pwd setzen / ändern (HIBP-Check)
- Pwd entfernen (Magic-Link-Only-Modus)

- Aktive Sessions verwalten (Logout pro Session, Global-Logout)

Notifications:

- Email-Präferenzen pro Event-Typ (Stage-Wechsel / Doc-Freigabe / Upload-Bestätigung)
- Marketing-Opt-In-Toggle (NUR falls Tenant Marketing-Mails versendet)

Account:

- Daten-Export (DSGVO — JSON-Download aller eigenen Daten, siehe Block J)
- Account-Löschung (siehe Block J)

Block E — Tenant-Admin-Konfiguration

E.1 — Portal-Konfiguration (`/{tenant}/admin/portal/`)

Zu zeigende Daten:

- Portal-Status (aktiv / deaktiviert)
- Portal-Name + Slug (Slug read-only in P1)
- Phasen-Sichtbarkeit pro Pipeline (welche Stages sieht Endkunde)
- Stage-Klartext-Labels (Override für Endkunden-Sicht)
- Doc-Typen mit Auto-Freigabe
- Auto-Status-Mail-Settings pro Stage-Wechsel-Event
- Branding (P1: nutzt Tenant-Branding aus M27; Portal-eigenes Branding ist P2)
- Welcome-Message-Default
- Support-Email + Telefon
- Pflicht-Links (Impressum, Datenschutz)

Benötigte UI-Elemente:

- Sektion „Phasen-Sichtbarkeit pro Pipeline":
- Pipeline-Selektor
- Pro Stage Toggle: sichtbar im Portal ja/nein
- Pro Stage Text-Input für Klartext-Label-Override (Platzhalter zeigt Original-Stage-Name)
- Klartext: *„Aktivieren Sie nur die Phasen, die für den Kunden relevant sind. Interne Phasen wie ‚Disposition' bleiben verborgen."*
- Sektion „Doc-Typen-Auto-Freigabe":
- Multi-Select-Toggle pro Doc-Typ aus Tenant-Doc-Type-Liste (z.B. Angebot, Rechnung, Acceptance-PDF, Bauplan)
- Klartext: *„Beim Erzeugen oder Hochladen von Dokumenten dieses Typs wird der Kunde automatisch Zugriff erhalten."*
- Sektion „Auto-Status-Mails":
- Pro Pipeline + Stage-Wechsel-Event Toggle „Mail an Kunde versenden"
- Auto-Mail-Template-Auswahl
- Klartext-Beispiel-Vorschau mit Platzhaltern
- Sektion „Pflicht-Links": Eingaben für Impressum-URL, Datenschutz-URL, AGB-URL (Tenant-Default oder eigene URLs)

Operationen:

- Portal aktivieren / deaktivieren (mit Warnung: alle PortalUser können nicht mehr einloggen)
- Phasen-Sichtbarkeit speichern
- Auto-Mail-Settings speichern
- Branding-Override (P2)

E.2 — PortalUser-Verwaltung (`/{tenant}/admin/portal/users`)

Zu zeigende Daten pro PortalUser:

- Avatar / Initialen
- Name
- Email
- Status (`pending_setup | active | disabled | deleted`)
- Anzahl zugewiesener Projekte
- Letzter Login
- Verknüpfter Contact (falls vorhanden)
- Erstellt-Datum + Erstellt-von

Benötigte UI-Elemente:

- Tabellarische Listen-Anzeige
- Filter: Status, Erstellt-Zeitraum, mit/ohne Contact-Verknüpfung
- Such-Funktion (Email, Name)
- Sortier-Funktion
- Bulk-Auswahl
- Bulk-Actions: Deaktivieren / Aktivieren / Setup-Mail erneut senden / Hard-Delete (mit DSGVO-Hinweis)
- Funktion „Neuen PortalUser anlegen" (Modal)

Operationen:

- PortalUser anlegen (siehe F.1)
- Bestehenden PortalUser editieren
- Setup-Mail erneut senden (bei `pending_setup` mit abgelaufenem Token)
- Pwd-Reset-Mail erzwingen
- Deaktivieren (Status `disabled` , alle Sessions invalidiert)
- Reaktivieren
- Hard-Delete (DSGVO-Workflow)
- Liste der Project-Accesses anzeigen + revoke

E.3 — PortalUser-Detail (`/{tenant}/admin/portal/users/:id`)

Zu zeigende Daten:

- Stammdaten (Email, Name, Telefon, Sprache, Status, Verknüpfter Contact)
- Account-Status (Pwd gesetzt? Email verifiziert? Letzter Login? Letzter Pwd-Reset?)
- Project-Access-Liste (alle CustomerPortalProjectAccess + access_level)
- Doc-Release-Liste (Cross-Project)
- Aktive Sessions
- Login-Historie (letzte 30 Logins mit IP + Datum)
- Upload-Historie (alle vom PortalUser hochgeladenen Files)
- Form-Submissions des PortalUsers
- Audit-Log (Anlage, Statuswechsel, Zugang-Änderungen)

Operationen:

- Stammdaten editieren
- Project-Access hinzufügen (Project-Auto-Complete + access_level wählen)
- Project-Access entfernen / `access_level` ändern
- Sessions invalidieren
- Pwd-Reset triggern
- Mit Contact verknüpfen / Verknüpfung lösen

- Status setzen (Deaktivieren / Reaktivieren / Hard-Delete)
- Setup-Mail erneut senden
- Daten-Export (DSGVO — JSON aller Daten dieses PortalUsers)

E.4 — Cross-Project-Access-Übersicht (`/{tenant}/admin/portal/access`)

Zu zeigende Daten:

- Matrix-/Listen-Anzeige: PortalUser × Project mit access_level
- Filter: Project (oder Pipeline), PortalUser, access_level

Benötigte UI-Elemente:

- Listen- oder Tabellen-Anzeige
- Filter-Funktionen
- Bulk-Actions: Access entziehen / access_level ändern
- Funktion „Access für Project an PortalUser geben" (Modal mit beiden Selektoren)

E.5 — Auto-Status-Mail-Templates (`/{tenant}/admin/portal/email-templates`)

Zu zeigende Daten pro Template:

- Template-Kind (`setup_invitation | login_magic_link | password_reset | stage_changed | document_released | upload_received`)
- Subject (mit Platzhalter-Vorschau)
- Body (Markdown mit Platzhalter-Vorschau)
- From-Address
- Aktiv ja/nein
- Letzte Bearbeitung

Operationen:

- Editieren (Subject + Body) mit Platzhalter-Hilfe (`{{customer_name}}` , `{{project_title}}` , `{{stage_name}}` , `{{stage_klartext_label}}` , `{{tenant_name}}` , `{{support_email}}` , `{{magic_link_url}}` , `{{document_name}}` , `{{document_link}}`)
- Test-Mail an eigene Adresse senden
- Auf Default zurücksetzen
- Aktivieren / Deaktivieren

E.6 — Portal-Audit (`/{tenant}/admin/portal/audit`)

Zu zeigende Daten:

- Chronologische Liste aller Portal-Events
- Event-Typen: Login, Logout, Pwd-geändert, Doc-runtergeladen, File-hochgeladen, Project-Access-Änderung, Status-Mail-versendet
- Pro Eintrag: PortalUser, Event, IP, User-Agent, Datum, ggf. Project/Doc-Bezug

Benötigte UI-Elemente:

- Filter: PortalUser, Event-Typ, Zeitraum, Project
- Such-Funktion
- Export-Funktion (CSV, gefilterte Auswahl)

Block F — PortalUser-Lifecycle

F.1 — Anlage / Einladung

Drei Wege:

(A) Manuell aus PortalUser-Verwaltung (`/{tenant}/admin/portal/users`):

1. TenantUser klickt „Neuen PortalUser anlegen"
2. Modal-Eingaben: Email (Pflicht), Vor-/Nachname (Pflicht), Sprache, optional Verknüpfung mit existierendem Contact (Auto-Complete), optional Project-Access-Liste, persönliche Welcome-Message
3. Submit → PortalUser angelegt mit Status `pending_setup` , Setup-Mail mit 7-Tage-Token versendet

(B) Aus Contact-Detail (M1):

1. TenantUser im Contact-Detail klickt „Portal-Zugang einladen"
2. Modal vorausgefüllt mit Contact-Daten + Auto-Verknüpfung
3. Optional: Project-Access aus Contact-Projekten vorausgewählt

(C) Aus Project-Detail (M4):

1. TenantUser im Project klickt „Customer-Portal-Zugang einladen"
2. Modal mit Auto-Vorbelegung aus `Project.contact` (falls Contact verknüpft)
3. `CustomerPortalProjectAccess` automatisch mit diesem Project erzeugt

(D) Aus Deal-Detail (M3, ab Sales-Phase):

1. TenantUser aktiviert „Portal-Zugang ab Sales-Phase" → PortalUser mit Sales-Deal-Access
2. Endkunde sieht Deal-Phase im Portal (gegated über `deals.read_via_portal` -Toggle in PortalConfiguration)

Edge-Cases:

- Email bereits existierender PortalUser im selben Portal: Klartext *„[Name] ist bereits PortalUser. Soll der existierende User Zugang zu diesem Project erhalten? [Bestehenden nutzen] [Abbrechen]*"
- Email bereits TenantUser: Erlaubt — getrennte Auth-Klassen, keine Verwechslung möglich (siehe Architektur-Hinweis)
- Setup-Token abgelaufen: TenantUser kann „Setup-Mail erneut senden"

F.2 — Setup-Flow

Siehe C.3.

F.3 — Pwd-Reset

- Endkunde-initiiert via `/portal/{tenant}/forgot-password` (siehe C.4)
- Tenant-initiiert: TenantUser im PortalUser-Detail klickt „Pwd-Reset-Mail versenden" → Magic-Link mit `purpose=password_reset`

F.4 — Deaktivierung / Reaktivierung

- Tenant-Admin setzt Status `disabled` → alle Sessions invalidiert, Login gesperrt mit Klartext
- Reaktivierung: Status zurück auf `active` , kein neuer Setup-Flow nötig

F.5 — Entfernen / Hard-Delete

- Hard-Delete: PortalUser-Status `deleted` , PII-Felder anonymisiert (`[deleted-{userId}]`)
- Sessions, Magic-Tokens, Setup-Tokens entfernt
- `CustomerPortalProjectAccess` entfernt
- Form-Submissions, Uploads bleiben (mit anonymisiertem User-Bezug — Audit-Trail)

- Audit-Eintrag mit User-ID + Lösch-Datum
- DSGVO-Workflow analog M35 (siehe Block J)

F.6 — Wenn Portal-Zugang nach Auftrag-Abschluss bleibt

- Default: PortalUser bleibt **aktiv** auch wenn alle Projekte abgeschlossen sind
- Service/Wartungs-Anfragen weiterhin möglich
- Tenant-Admin kann manuell deaktivieren oder Auto-Deaktivierung-Regel definieren („nach 365 Tagen ohne Login deaktivieren" — Phase 2)

Block G — Auto-Status-Mails bei Phasenwechsel

Auslöse-Logik

- Trigger: `project.stage_changed`-Event (M4)
- Bedingungen:
- `PortalConfiguration.auto_status_mail_enabled` für diese Stage = true
- Neue Stage in `visible_pipeline_stages` enthalten
- PortalUser hat aktiven `CustomerPortalProjectAccess` mit `access_level != revoked`
- PortalUser hat Email-Notification für `stage_changed` aktiv (Default: an)
- `Tenant.status != frozen` (in `frozen` keine Outbound-Mails — analog M27)
- Mail-Template: `PortalEmailTemplate` mit `kind = stage_changed`
- Versand über M9 verbundene Sending-Domain (Default Tenant-Default-Adresse)

Mail-Inhalte

- Subject mit Platzhaltern (z.B. *„Update zu Ihrem Projekt {{project_title}}: {{stage_klartext_label}}"*)
- Body mit Klartext-Beschreibung der neuen Phase + Magic-Link zur direkten Project-Detail-Page
- Tenant-Branding (Logo + Farbe aus PortalConfiguration / Tenant-Default)
- Footer mit Impressum-Link + Notification-Settings-Link

Edge-Cases

- Mehrere PortalUser pro Project: Mail an alle aktiven mit Access
- Stage-Wechsel rückwärts (Reverse): Mail nur wenn `stage_klartext_label` sich ändert (sonst stumm — kein Spam)
- Schneller Mehrfach-Wechsel innerhalb 5 Min: Debounce, nur letzte Stage gemailt
- Mail-Bounce: Eintrag im Portal-Audit + Notification an verantwortlichen TenantUser

Doc-Released-Mail

- Trigger: `CustomerPortalProjectDocument` neu angelegt (manuell oder auto)
- Bedingung: PortalUser-Notification für `document_released` aktiv
- Template `kind = document_released`
- Debounce: bei Bulk-Release (>5 Files in 1 Min) eine Sammel-Mail mit Liste

Upload-Received-Mail

- Trigger: PortalUser hat erfolgreich File hochgeladen
- Empfänger: PortalUser (Bestätigung) + verantwortlicher TenantUser (Info)
- Template `kind = upload_received`

Block H — Integration mit anderen Modulen

M1 CRM

- `PortalUser.linked_contact_id` verknüpft mit Contact
- Im Contact-Detail: Sektion „Portal-Zugang"
- Activity-Stream des Contacts erhält Portal-Events (Login, Upload, Form-Submission) als Activity-Typ `portal_event` mit `actor_kind = portal_user`

M3 Sales-Pipeline (Deals)

- Optional Portal-Zugang ab Lead/Deal-Phase (für Pre-Sales-Transparenz)
- Tenant-Admin-Toggle „Sales-Phase im Portal sichtbar"
- Endkunde sieht Deal-Stage wenn aktiviert

M4 Auftragspipeline (Projects)

- `CustomerPortalProjectAccess` verknüpft PortalUser mit Project
- Project-Detail im Tenant-Workspace zeigt Portal-Sektion (verknüpfte PortalUser, Doc-Freigabe-Toggles)
- Acceptance-PDF wird (bei Tenant-Konfiguration) automatisch im Portal freigegeben
- Project-Stage-Wechsel triggert Auto-Status-Mail (Block G)
- `project.stage_changed` mit visibility-Filter

M5 Form Builder

- Forms mit Subtyp `portal_form` sind im Portal aufrufbar
- Form-Submission wird mit `portal_user_id` + ggf. `project_id` versehen
- Trigger M17: `portal.kunde_replied`

M9 Email Inbox / Sending

- Portal-Auto-Mails versendet über verbundene Sending-Domain (Tenant-Default)
- Bounce-Handling über M9-Bounce-Pipeline
- Reply-Adresse zeigt zurück auf Tenant-Inbox (Threading mit M9)

M17 Automation-Engine

Trigger:
- `portal.user_created`
- `portal.user_setup_completed`
- `portal.user_logged_in`
- `portal.kunde_uploaded_file`
- `portal.kunde_replied` (Form-Submission)
- `portal.access_granted`
- `portal.access_revoked`
- `portal.document_released`
- `portal.document_downloaded`
- `portal.status_mail_sent`

Actions:
- `portal.create-user` (PortalUser anlegen)
- `portal.send-setup-invitation`
- `portal.grant-project-access`
- `portal.revoke-project-access`
- `portal.release-document`

- `portal.send-status-mail` (manuell triggern)
- `portal.disable-user`

M22 Notifications

- Auto-Status-Mails an Endkunde (siehe Block G)
- Push/In-App-Notification an verantwortlichen TenantUser bei `portal.kunde_uploaded_file` und `portal.kunde_replied`

M23 Files

- `CustomerPortalProjectDocument` referenziert M23-File
- File-Aufruf aus Portal: zusätzlicher Permission-Check + Audit-Eintrag
- Upload-Pfad: `tenants/{tenantId}/projects/{projectId}/portal-uploads/{fileId}`
- Tenant-File-Detail zeigt Quelle = `customer_portal_upload`

M27 Auth / Multi-Tenancy

- **Getrennte User-Klasse**: `PortalUser` ≠ `TenantUser`
- Eigene Cookie-Domäne / Cookie-Name
- Eigenes Session-Modell
- Eigene Login-Routen
- **Keine** Permission-Vermischung (PortalUser kann niemals TenantUser-Permissions erlangen)
- RLS-Pattern analog: `tenant_id` auf allen Portal-Tabellen mit Policy
- Tenant-Status-Wirkung: `frozen` → Portal read-only; `suspended/deleted` → Portal-Login gesperrt mit Klartext

M35 DSGVO / Account-Lösch-Workflow

- PortalUser-Lösch-Flow analog TenantUser-Flow (Multi-Step + 24h-Reverse-Window)

Block I — Permissions-Anwendung

I.1 — Tenant-seitige Permissions (TenantUser)

Permission	Erlaubt
`portal.read`	Sehen, welche Endkunden Zugang haben (Liste, Details, Access-Übersicht)
`portal.manage_users`	PortalUser anlegen / einladen / deaktivieren / reaktivieren / Setup erneut senden
`portal.manage_access`	Project-Access pro PortalUser hinzufügen/entfernen, `access_level` ändern, Doc-Freigabe pro Project schalten
`portal.delete_user`	Hard-Delete + DSGVO-Lösch-Workflow auslösen
`portal.admin`	Portal-Konfiguration (Phasen-Sichtbarkeit, Doc-Auto-Freigabe, Branding, Auto-Mail-Templates), Portal-Audit-Sicht, Portal aktivieren/deaktivieren

Bundle-Mapping (Variante 2):

Bundle	Atomare Permissions
`portal.none`	(keine)
`portal.read`	`portal.read`
`portal.manage_users`	`portal.read` + `portal.manage_users`
`portal.manage_access`	obigen + `portal.manage_access`
`portal.admin`	obigen + `portal.delete_user` + `portal.admin`

SHK-Template-Default-Rollen:

Rolle	Portal-Permissions
GF	`portal.admin`
Vertriebsleiter	`portal.manage_access` (kann Sales-Phase-Zugang freischalten)
Vertriebler	`portal.read` + `portal.manage_users` (kann Endkunden einladen ab Lead)
Projektleiter / Bauleiter	`portal.manage_access` (verwaltet Doc-Freigabe + Mail-Settings für eigene Projekte)
Büro / Backoffice	`portal.manage_access`
Marketing	`portal.read`
Monteur	`portal.none`

Anwendung in Tenant-Routes:

- `/{tenant}/admin/portal/` → `portal.admin`
- `/{tenant}/admin/portal/users` → `portal.read` (Liste) + `portal.manage_users` (Mutations)
- `/{tenant}/admin/portal/users/:id` → `portal.read`
- `/{tenant}/admin/portal/access` → `portal.manage_access`
- `/{tenant}/admin/portal/email-templates` → `portal.admin`
- `/{tenant}/admin/portal/audit` → `portal.admin`
- Project-Detail-Portal-Sektion (Doc-Freigabe-Toggles): `portal.manage_access` + `projects.write` (für dieses Project)
- Contact-Detail-Portal-Sektion (Einladung): `portal.manage_users`

I.2 — Portal-seitige Permissions (PortalUser)

PortalUser hat **keine** atomaren Permissions im M27-Stil. Stattdessen wirken implizite Resource-Checks:

- **Listen-Filter:** automatisch über `CustomerPortalProjectAccess.portal_user_id = self`
- **Detail-Access:** Server prüft pro Request `CustomerPortalProjectAccess` (Project), `CustomerPortalProjectDocument` (File)
- **Stage-Sichtbarkeit:** Server filtert Stages nach `PortalConfiguration.visible_pipeline_stages`
- **Funktion-Sichtbarkeit:** Upload/Form-Funktionen nur bei `access_level = read_full` sichtbar; bei `read_status_only` nicht sichtbar

I.3 — Klartext-Fehler

- TenantUser ohne `portal.manage_users` versucht Einladen: Funktion nicht sichtbar
- TenantUser ohne `portal.admin` versucht Konfiguration: Route nicht erreichbar (404)
- PortalUser greift auf Project ohne Access: 404 (keine Existenz-Offenlegung)
- PortalUser bei `Tenant.status = frozen` versucht Upload: Klartext *„Aktuell sind keine Uploads möglich. Bei Fragen wenden Sie sich an [Support]."*

- PortalUser bei `Tenant.status = suspended/deleted` versucht Login: Klartext *„Dieses Portal ist aktuell nicht erreichbar."* (kein technisches Detail)

Block J — DSGVO / Lösch-Workflow

J.1 — Datenklassifizierung

- **Sensible Daten** (Endkunden-PII): Email, Name, Telefon, IP-Logs, hochgeladene Files, Form-Submissions
- **Aufbewahrungspflichten:** Acceptance-PDFs + rechtlich aufbewahrungspflichtige Files bleiben (siehe M4); PortalUser-PII wird bei Löschung anonymisiert, nicht gelöscht, soweit verknüpfte Aufbewahrungspflicht besteht

J.2 — Endkunde-initiiertes Löschen (`/portal/{tenant}/settings/account-delete`)

Multi-Step-Flow (analog M35):

1. **Erklärung** — Klartext was passiert (Account weg, Login nicht mehr möglich, Daten anonymisiert, aufbewahrungspflichtige Dokumente bleiben Tenant-seitig)
2. **Identität** — Pwd-Eingabe oder Magic-Link
3. **Final-Klick** mit 3-Sek-Countdown
4. **Bestätigungs-Email** mit 24h-Reverse-Window
5. **Nach 24h:** Hard-Delete-Job läuft

J.3 — Tenant-initiiertes Löschen

- TenantUser mit `portal.delete_user` triggert Lösch-Workflow im PortalUser-Detail
- Klartext-Warnung: *„Dies löscht den PortalUser-Account. Hochgeladene Files und Form-Submissions bleiben mit anonymisiertem Bezug für Audit-Pflicht."*
- 24h-Reverse-Window
- Audit-Eintrag

J.4 — Daten-Export (DSGVO-Auskunft)

- Endkunde in `/portal/{tenant}/settings/` : Funktion „Meine Daten exportieren" → JSON-Download mit allen PortalUser-bezogenen Daten (Profil, Sessions-Historie, Project-Access-Liste, Doc-Releases, Uploads, Form-Submissions)
- Tenant-seitig: TenantUser mit `portal.read` kann Export für PortalUser anfordern (z.B. Auskunfts-Anfrage)

J.5 — Tenant-Lifecycle-Wirkung

- `Tenant.status = deletion_pending` : Portal-Login bleibt 30 Tage offen mit Banner *„Dieser Anbieter hat sein Konto gekündigt. Daten werden am [Datum] gelöscht."*
- `Tenant.status = deleted` : Portal nicht mehr erreichbar; alle PortalUser-Daten via Tenant-Lösch-Job anonymisiert/gelöscht

---

Block K — Klartext-Hinweise / -Fehler (Sammlung)

Login-Page:
- *„Wir haben Ihnen einen Login-Link an [Email] gesendet. Der Link ist 15 Minuten gültig."*
- *„Probleme beim Login? Kontaktieren Sie [Support-Email]."*

Setup-Page:
- *„Willkommen bei [Tenant-Name]. Bitte vervollständigen Sie Ihr Profil, um auf Ihre Projekte zuzugreifen."*
- *„Sie können später jederzeit ein Passwort setzen oder per Magic-Link einloggen."*

Project-Detail (leer):
- *„Aktuelle Phase: [Phase]. Es gibt noch keine freigegebenen Dokumente. Sie werden per Email informiert, sobald sich der Status ändert."*

Doc-Download:
- *„Datei wird heruntergeladen. Diese ist nur für Sie und Ihr Projektteam bestimmt."*

Upload-Funktion:
- *„Maximal 10 Dateien gleichzeitig, je max. 50 MB."*
- *„Wir benachrichtigen [Tenant-Name] automatisch über Ihren Upload."*

Tenant frozen:
- *„Aktuell sind keine schreibenden Aktionen möglich. Bei Fragen wenden Sie sich an [Support]."*

Permissions-Block (Tenant-Seite):
- *„Hierfür benötigst du erweiterte Portal-Berechtigungen. Tenant-Admin kontaktieren."*

Konfigurations-Hinweise:
- Phasen-Sichtbarkeit leer: *„Aktuell sieht der Endkunde keine Phasen. Aktivieren Sie mind. eine Phase pro Pipeline."*
- Auto-Mail-Templates inaktiv: *„Stage-Wechsel-Mails sind aktuell deaktiviert. Endkunden werden nicht automatisch über Phasenwechsel informiert."*

Block L — Phase 2 / spätere Features

- **Bidirektionale Kommunikation** (Chat zwischen Kunde und Firma im Portal-Kontext, separat von M13 Team-Chat)
- **Blog/CMS im Portal** (Tenant kann redaktionelle Inhalte für Endkunden veröffentlichen — Wartungs-Tipps, News)
- **Mehrere Portale pro Tenant** mit unterschiedlichem Branding/Slug (z.B. Privatkunden vs. Bauträger)
- **Portal-eigenes Branding** (eigenes Logo + Farben + Custom-Domain `portal.geerkens.de`)
- **PortalSubscription** (Wartungs-Abos, Service-Pakete im Portal abschließbar mit Stripe-Integration)
- **Multi-Faktor-Auth für PortalUser** (TOTP-optional)
- **In-App-Notifications im Portal** (statt nur Email)
- **Bulk-Download** (ZIP) aller freigegebenen Dokumente
- **Push-Notifications** an Endkunden (über installierbare PWA)
- **Auto-Deaktivierung** von PortalUser nach X Tagen ohne Login (konfigurierbar)
- **Direkte Mail-Compose** im Portal (statt nur `mailto:`)
- **Endkunden-Empfehlungs-/Referral-Programm**
- **Portal-Analytics** für Tenant (welche Endkunden sind aktiv, welche Docs werden geöffnet)

Architektur-Vorschriften (Querschnitt)

- **LP-1, AV #2 — User-Klassen-Trennung:** PortalUser strikt getrennt von TenantUser, eigene Auth-Schicht, eigene Cookies, eigene Routes — verhindert Permission-Eskalation
- **LP-2 — Mobile-Ready:** Portal-Endkunden-Views (Project-Detail, Upload, Forms) mobile-first; Tenant-Admin-Konfiguration desktop-fokussiert
- **LP-3, AV #3 — Branchen-Templates deklarativ:** SHK-Default-PortalConfiguration (Phasen-Sichtbarkeit + Auto-Doc-Freigabe + Mail-Templates) als Seeding
- **LP-7 — Konsolidierung:** Customer-Portal löst externe Tools wie Plan-Radar/Trello-Kunden-Boards ab
- **LP-9 — Spec-Stil:** UI-Anforderungen als Liste, kein Layout

- **LP-10, AV #1 — Klartext-Diagnostik:** alle Endkunden-Texte freundlich, lösungsorientiert, ohne technische Details
- **LP-13 — EU-Stack:** Portal-Daten in EU-Storage, Auto-Mails über EU-Sending-Domain
- **AV #5 — Permissions-aware-Default:** alle Listen automatisch nach `CustomerPortalProjectAccess` gefiltert
- **AV #6 — Audit-Trail-Default:** alle PortalUser-Aktionen (Login, Download, Upload, Doc-Release-Änderung) in Portal-Audit
- **AV #20 — Action-Boundary für KI:** KI darf keine Portal-Access-Änderungen direkt vornehmen, nur User-Bestätigt

---

Detail-Spec-Status: DRAFT

Erste vollständige Detail-Spec für Modul 15. **Vor Bau:** Verifizierung mit Noah (zusammen mit Pflichtenheft-Sweep + Geerkens-Launch-Anforderungen).

Offene Detail-Punkte (nicht-blockierend, beim Bau zu klären):
- Konkrete SHK-Default-Phasen-Sichtbarkeit pro Pipeline (welche Stages aus M4-Templates sind kunden-relevant)
- Konkrete SHK-Default-Doc-Auto-Freigabe-Liste (Angebot/Rechnung/Acceptance-PDF/Bauplan?)
- Konkrete SHK-Default-Auto-Mail-Templates (Subject + Body für `setup_invitation`, `stage_changed`, `document_released`)
- Konkrete Upload-Restriktionen (Max-Größe pro File, erlaubte Mime-Types final)
- Konkrete Email-Bounce-Handling-Strategie (welcher TenantUser wird informiert)
- Konkrete Storage-Pfad-Struktur für Portal-Uploads (Folder-Konvention)
- Konkrete Branding-Vererbung Phase 1 (Tenant-Logo + Farbe in welcher Form auf Portal-Seiten)
- Subframe-UI-Designs (separat)

Verweise auf abhängige Module:
- M27 (Auth-Pattern + Tenant-Lifecycle-Wirkung)
- M4 (Project-Stage-Wechsel-Trigger + Acceptance-PDF-Auto-Freigabe)
- M1 (Contact-Verknüpfung + Activity-Stream)
- M3 (Sales-Phase-Sichtbarkeit ab Lead/Deal)
- M5 (Portal-Forms)
- M9 (Sending-Domain für Auto-Mails)
- M17 (Automation-Trigger + -Actions)
- M22 (Notifications an TenantUser bei Portal-Events)
- M23 (Files-Storage + Doc-Freigabe-Architektur)
- M35 (DSGVO-Lösch-Workflow)