```
module: 22
title: Notifications
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-8, LP-9, LP-10, LP-12, LP-13]
spec_style: requirements-pur
```

Modul 22 — Notifications

> ***Detail-Spec gemäß LP-9.*** *Drei-Kanal-Notification-System (In-App, Email, Mobile-Push) mit Pro-User-Präferenzen, Ruhezeiten, Anti-Spam-Bündelung und Mobile-Device-Registrierung. Behebt Lücke L-17 (Notification-Storm bei Massen-Events). Apple-Compliance für Push-Permission-Flows (LP-8).*

Themenblöcke

```
A. Datenmodell (Notification, Preference, Device, Bundle)
B. Kanäle (In-App, Email, Mobile-Push)
C. Menü-Struktur und Routes
D. Notification-Center (Listen + Detail)
E. Pro-User-Präferenzen
F. Ruhezeiten
G. Anti-Spam-Bündelung
H. Mobile-Device-Registrierung
I. Event-Typen-Katalog
J. Versand-Pipeline
K. Permissions-Anwendung
L. Klartext-Hinweise
M. Phase 2 / spätere Features
```

Block A — Datenmodell

`Notification`

- `id` (UUID)
- `tenant_id` (NOT NULL, RLS)
- `recipient_user_id` (FK auf User, NOT NULL)
- `created_at` (Timestamp, indexed)
- `event_type` (Enum, siehe Block I)
- `event_subject_type`, `event_subject_id` (FK auf Quelle, z.B. Lead, Deal, Task)
- `actor_user_id` (FK auf auslösenden User; NULL bei System/Automation)
- `actor_kind` (Enum: `user | system | automation | ki_agent | external`)
- `title` (Pflicht — kurzer Klartext, z.B. *„Neuer Lead: Müller GmbH"*)
- `body` (Pflicht — längere Beschreibung, z.B. *„Über Form ‚Kontakt SHK' eingegangen. [Lead öffnen]"*)
- `deeplink` (URL — z.B. `/{tenant}/leads/{leadId}`)
- `priority` (Enum: `low | normal | high | urgent`)
- `read_at` (Timestamp NULL — markiert Read-Status)

- `dismissed_at` (Timestamp NULL — User hat manuell weggeklickt)
- `bundle_id` (FK auf NotificationBundle; NULL falls einzeln versendet)
- `metadata` (JSONB — Event-spezifische Felder)
- `delivery_status` (JSONB pro Kanal — siehe unten)

`delivery_status` (JSONB)

```
{
  "in_app": "delivered",
  "email": "skipped:user_preference" | "queued" | "sent" | "bounced" | "failed:smtp_timeout",
  "push": "skipped:no_device" | "queued" | "delivered" | "failed:invalid_token"
}
```

`NotificationPreference`

- `id` (UUID)
- `tenant_id`, `user_id`
- `event_type` (Enum, siehe Block I)
- `channel_in_app` (Boolean — Default abhängig vom Event-Typ)
- `channel_email` (Boolean)
- `channel_push` (Boolean)
- `priority_threshold` (Enum: `all | normal_and_above | high_and_above | urgent_only`)
- `updated_at`

Default-Sets pro Rolle: beim Onboarding wird ein Preference-Set für Default-Rolle geseeded (z.B. Vertriebler bekommt In-App+Push für `lead.assigned`, Email aus).

`NotificationDevice` (Mobile-Push)

- `id`, `tenant_id`, `user_id`
- `device_kind` (Enum: `ios | android`)
- `push_token` (Text — APNs-Token oder FCM-Token)
- `device_label` (z.B. *„iPhone von Max"*, vom OS oder User benennbar)
- `os_version`, `app_version`
- `registered_at`, `last_seen_at`
- `revoked_at` (NULL falls aktiv)

`NotificationBundle` (Anti-Spam-Bündelung)

- `id`, `tenant_id`, `recipient_user_id`
- `created_at`, `closed_at` (NULL solange Bundle offen)
- `event_type_group` (z.B. `lead.created`, `task.assigned` — gleichartige Events werden gebündelt)
- `count` (Anzahl gebündelter Events)
- `subject_summary` (Textuelle Zusammenfassung der gebündelten Subjects)
- `bundle_window_seconds` (Default 300 = 5 Min)

`NotificationQuietHours`

- `id`, `tenant_id`, `user_id`
- `weekday` (Enum: `mo | tu | we | th | fr | sa | su` ODER `weekend`)
- `start_time` (TIME)
- `end_time` (TIME — über Mitternacht erlaubt)
- `enabled` (Boolean)
- `urgent_override` (Boolean — `urgent`-Notifications überschreiben Ruhezeiten)

Indizes

- `(tenant_id, recipient_user_id, created_at DESC)` — Notification-Center-Default
- `(tenant_id, recipient_user_id, read_at)` — Unread-Count-Query
- `(tenant_id, user_id, push_token)` für Device-Lookup, UNIQUE-Constraint auf `push_token` pro Tenant

---

Block B — Kanäle

B.1 — In-App-Notification-Center

- Notification-Icon in Top-Bar mit Unread-Count-Badge
- Klick öffnet Notification-Center (Drawer oder Page — Designer-Wahl)
- Default-Kanal für jede Notification (kann nicht deaktiviert werden — In-App ist die Wahrheit)
- Real-time-Update über Server-Sent-Events oder WebSocket; Fallback auf Polling alle 30 Sek
- Bei Tab-Background: Browser-Tab-Title zeigt Unread-Count

B.2 — Email

- Versand über Tenant-Sending-Domain (Modul 9 Email-Domain mit DKIM)
- Email-Templates aus i18n-Locale-Files (LP-12) mit Tenant-Branding (Logo + Primärfarbe — Modul 31 Phase 1 Light/Dark + Logo)
- Bei Bundle: ein Email pro Bundle mit zusammengefasstem Inhalt
- Bei Urgent-Priority + offline-User: sofortiges Email (siehe Block G)
- Bounce-Handling: bei wiederholtem Bounce → Notification-Email für User pausiert (Klartext im Notification-Center: *„Emails an dich kommen aktuell nicht an — bitte Email-Adresse prüfen"*)
- Standard-Footer: Klartext „Du bekommst diese Email weil X — [Notifications-Settings]"

B.3 — Mobile-Push

- Provider: **Novu** als Abstraktions-Schicht
- APNs (iOS) und FCM (Android) als Backends
- Push-Payload enthält `title`, `body`, `deeplink`, `priority`, `bundle_count` falls Bundle
- Capacitor-Wrap (Modul 36) registriert Device-Token via `/api/v1/notifications/mobile-device`
- iOS: Notification-Permission-Flow nach Apple-Compliance (LP-8) — Erst-Use-Teaser-Screen erklärt warum, dann nativer Permission-Dialog
- Android: Permission ab API 33 ähnlicher Flow
- Bei Permission-Denied: Klartext im Settings-Notifications: *„Push ist auf diesem Gerät deaktiviert. [Geräte-Einstellungen öffnen]"*
- Silent-Push-Capability (Phase 2 — für Hintergrund-Sync der Mobile-App)

Block C — Menü-Struktur und Routes

Routen:

```
/{tenant}/notifications                          → Notification-Center
/{tenant}/notifications/:id                      → Notification-Detail (selten direkt;
Deeplink-First)
/{tenant}/settings/notifications                 → Pro-User-Präferenzen-Übersicht
/{tenant}/settings/notifications/preferences     → Event-Typ-Präferenzen-Editor
/{tenant}/settings/notifications/quiet-hours     → Ruhezeiten-Editor
/{tenant}/settings/notifications/devices         → Mobile-Devices-Liste
/{tenant}/admin/notifications/templates          → Email-Template-Anzeige (read-only Phase 1)
/{tenant}/admin/notifications/test               → Test-Notification senden (Tenant-Admin-
Werkzeug)
```

Permission-Anforderungen:
- `/notifications` → eingeloggt (Self-Scope)
- `/settings/notifications/*` → eingeloggt (Self-Scope)
- `/admin/notifications/*` → `tenant.admin` ODER `notifications.admin`

Block D — Notification-Center

Zu zeigende Daten pro Notification

- `title` als Hauptzeile
- `body` als Sekundär-Zeile (gekürzt bei Listen-Anzeige)
- Datum/Zeit (relativ < 7 Tage, sonst absolut)
- Actor (Avatar + Name oder Marker für System/Automation/KI)
- Event-Typ-Marker (visuelle Kategorie — Designer-Wahl)
- Read-Status (gelesen/ungelesen visuell unterscheidbar)
- Deeplink-Indikator (Ziel der Aktion)
- Bei Bundle: `count` + Subject-Summary statt Einzel-Anzeige (z.B. *„7 neue Leads"*)
- Priority-Marker für `high` / `urgent`

Benötigte UI-Elemente

- Listen-Anzeige (Designer-Wahl: Drawer / Page / Stream)
- Tab- oder Filter-Funktion für „Alle / Ungelesen / Markiert"
- Filter-Komponenten:
- Event-Typ (Multi-Select gruppiert)
- Actor
- Zeitraum
- Priority
- Such-Funktion über `title` + `body`
- Pagination (Cursor-basiert, „Mehr laden", 50 pro Page)
- Bulk-Auswahl (Checkboxes)
- Quick-Action-Funktionen pro Eintrag:
- Als gelesen markieren / als ungelesen markieren
- Wegklicken (`dismissed_at`)
- Klick öffnet Deeplink (markiert automatisch als gelesen)
- Bei Bundle: „Alle anzeigen" expandiert in Einzel-Notifications

Operationen

- Mark-as-read / Mark-as-unread (einzeln + bulk)
- Mark-all-as-read (mit Klartext-Bestätigung bei mehr als 50 ungelesenen)

- Bulk-Clear (`dismissed_at` setzen — Notifications bleiben für Audit-/Replay-Zwecke aber sind nicht mehr im Center sichtbar)
- Filter speichern (Phase 2)
- Klick auf Notification → Deeplink + Mark-as-read

Performance-Anforderungen

- Server-side-Filter
- Index siehe Block A
- Unread-Count via Cached-Counter (Redis), invalidiert bei Mark-as-read / neue Notification
- Real-time-Updates über SSE/WebSocket
- Notifications älter als 90 Tage werden ausgeblendet (gelöscht: siehe Phase 2 Auto-Cleanup); Filter „Alle" zeigt aktuelle 90 Tage Default

Klartext-Hinweise

- Leerer Center: *„Keine Benachrichtigungen — sobald etwas Wichtiges passiert, erscheint es hier."*
- Filter ohne Treffer: *„Keine Benachrichtigungen passen zu deinem Filter. [Filter zurücksetzen]"*
- Mark-all-as-read mit > 50: *„124 Benachrichtigungen als gelesen markieren? [Bestätigen] [Abbrechen]"*
- Email-Bounce-Hinweis (siehe B.2)

Block E — Pro-User-Präferenzen

Routen-Spezifikation `/settings/notifications/preferences`

Zu zeigende Daten

- Liste aller Event-Typen, gruppiert nach Modul (CRM, Leads, Projekte, Aufgaben, Termine, Chat, ...)
- Pro Event-Typ:
- Event-Label (Klartext, z.B. *„Mir wird ein Lead zugewiesen"*)
- Toggle pro Kanal (In-App, Email, Push)
- Priority-Threshold-Selektor (`all | normal+ | high+ | urgent only`)
- Aktueller Default-Hinweis falls User noch nicht angepasst

Benötigte UI-Elemente

- Sektionierte Anzeige nach Modul
- Pro Event-Typ: 3 Toggles (In-App, Email, Push) + Priority-Selektor
- Search-Funktion über Event-Label
- „Alle Email-Notifications deaktivieren"-Master-Toggle (mit Klartext: betrifft auch zukünftige Event-Typen)
- „Auf Default zurücksetzen"-Funktion pro Sektion
- „Default-Set für meine Rolle anwenden"-Funktion

Operationen

- Toggle pro Kanal pro Event
- Priority-Threshold setzen
- Bulk-Operationen (Master-Toggles, Reset)
- Speichern explizit oder auto-save (Designer-Wahl, technisch beides praktikabel)

Default-Sets

Beim Onboarding seedet das System ein Preference-Set abhängig von der primären Rolle:

- **Vertriebler:** In-App + Push für Lead/Deal-Events; Email für Daily-Digest (Phase 2)
- **Projektleiter:** In-App + Push für Projekt-/Task-Events; Email für Termin-Erinnerungen
- **Monteur:** In-App + Push für Task-Zuweisungen, Plantafel-Änderungen, Acceptance-Anforderungen; Email aus Default
- **Büro/Backoffice:** Alle Kanäle für Eingang-Events (Lead, Mail, Form); reduziert für interne Events
- **GF:** Daily-Digest per Email; Push für Eskalationen (`high` / `urgent`)
- **Marketing:** Email für Kampagnen-Status; In-App für Lead-Events

LP-3, AV #3: Defaults sind deklarative Templates, keine Hardcode.

Klartext-Hinweise

- Master-Toggle „Alle Email aus": *„Du erhältst keine Email-Notifications mehr — auch nicht für neue Event-Typen, die wir später hinzufügen. Wichtige Sicherheits-Mails (Login, Passwort) bleiben immer aktiv."*
- Push deaktiviert auf Geräte-Ebene: Banner *„Push ist auf diesem Gerät deaktiviert. Toggles oben sind ohne Wirkung. [Geräte-Einstellungen]"*
- Reset auf Default: *„Bist du sicher? Deine bisherigen Einstellungen werden verworfen."*

Block F — Ruhezeiten

Routen-Spezifikation `/settings/notifications/quiet-hours`

Zu zeigende Daten

- Liste der konfigurierten Ruhezeiten
- Pro Ruhezeit: Wochentag(e), Start-Zeit, End-Zeit, Toggle aktiv, Urgent-Override-Toggle

Benötigte UI-Elemente

- Anlage-Funktion mit Wochentag-Picker (Multi-Select inkl. Quick-Wahl „Wochentags" / „Wochenende" / „Täglich")
- Time-Picker für Start + End
- Toggle „Auch ‚Urgent'-Notifications zurückhalten" (Default aus — Urgent kommt durch)
- Edit-Funktion pro Eintrag
- Lösch-Funktion
- Master-Toggle „Ruhezeiten aktiv" (für Urlaub aussetzbar)

Default-Sets

- Default-Ruhezeit beim Onboarding für Mobile-Push: **22:00–07:00 täglich** + **Wochenende ganztägig** mit Urgent-Override AUS
- User kann Default annehmen, anpassen oder deaktivieren

Wirkungs-Logik

- Wenn Notification außerhalb Ruhezeit ankommt → normaler Versand
- Wenn Notification innerhalb Ruhezeit:
- In-App: immer geliefert (sichtbar im Center, kein Pop-up/Sound)
- Email: gequeued bis Ruhezeit-Ende — Versand am ersten erlaubten Zeitpunkt (Bundle dabei aktiv)
- Push: gequeued bis Ruhezeit-Ende — Versand mit aktualisiertem Bundle-Count

- Urgent-Override = aus (Default Urgent-aktiv): Urgent-Notification trotz Ruhezeit sofort
- Urgent-Override = aktiv: auch Urgent-Notifications werden zurückgehalten

Klartext-Hinweise

- Bei Anlage: *„Während der Ruhezeit bekommst du keine Push und keine Mails — Benachrichtigungen werden gesammelt zugestellt, sobald die Ruhezeit endet. [Urgent-Override]"*
- Bei Urgent-Override-AUS-Bestätigung: *„Auch dringende Benachrichtigungen kommen erst nach der Ruhezeit an — sicher?"*
- Konflikt mehrere Ruhezeiten überlappen: *„Diese Ruhezeit überschneidet sich mit ‚X' — beide bleiben aktiv (Vereinigung der Zeitfenster)."*

Block G — Anti-Spam-Bündelung (Lücke L-17)

Bündelungs-Regeln

- Bei mehreren Notifications gleichen `event_type_group` an gleichen User innerhalb **5 Minuten** (Default, Tenant-Admin-konfigurierbar pro Event-Group):
- Kein einzelner Versand pro Push/Email
- Stattdessen: NotificationBundle wird angelegt/erweitert
- In-App: jede Einzel-Notification bleibt einzeln sichtbar (Wahrheit), aber Real-time-Toast/Badge nur einmal
- Push: ein Push pro Bundle mit `count` + Summary
- Email: ein Mail pro Bundle nach Bundle-Window-Ende
- Bündelungs-Fenster läuft sliding: bei jedem neuen Event innerhalb 5 Min wird Counter erhöht; nach 5 Min ohne neuen Event wird Bundle geschlossen und ggf. nachgereicht falls Push noch nicht raus war
- Maximaler Bundle-Inhalt: 100 Events; danach neue Bundle-Instanz

Bündelungs-Beispiel

- 23 neue Leads in 4 Min → 1 Push: *„23 neue Leads in den letzten 5 Minuten. [Lead-Inbox öffnen]"*
- 7 Tasks in 5 Min an Monteur zugewiesen → 1 Push: *„7 neue Aufgaben — [Aufgaben öffnen]"*
- 50 Chat-Messages in 5 Min im Projekt-Channel → 1 Push: *„50 neue Nachrichten in ‚Müller Heizung'"*

Bündelungs-Ausschlüsse

- `priority = urgent` → nie gebündelt, sofort versendet
- `event_type` mit `bundle_disabled = true` (z.B. Login-Sicherheits-Warnungen, 2FA-Codes-Notifications)
- Direkt-Mention im Chat (`@user`) → nie gebündelt mit anderen Mentions

Tenant-Admin-Setting

- `/admin/notifications/templates` (Phase 1: read-only Anzeige) zeigt Bundle-Window pro Event-Group
- Phase 2: Tenant-Admin kann Bundle-Window pro Event-Group ändern (z.B. längere Bündelung für interne Eskalationen)

Klartext-Hinweise

- Push-Body: *„23 neue Leads in den letzten 5 Min — [Inbox öffnen]"* statt 23 einzelne Pushes
- Email-Subject: *„HiveGrid: 23 neue Leads"* statt 23 einzelne Mails
- In Notification-Center bei Bundle-Eintrag: *„23 Events gebündelt — [Alle anzeigen]"*

Block H — Mobile-Device-Registrierung

Routen-Spezifikation `/settings/notifications/devices`

Zu zeigende Daten

- Liste aller registrierten Devices des Users
- Pro Device: `device_label`, `device_kind` (iOS/Android), `os_version`, `app_version`, `registered_at`, `last_seen_at`
- Status-Marker: `aktiv` / `inaktiv > 30 Tage` / `revoked`

Benötigte UI-Elemente

- Listen-Anzeige
- Pro Device: Test-Push-Funktion, Umbenennen, Revoke-Funktion
- Globaler „Alle Devices abmelden"-Button
- Hinweis bei keinem Device: *„Noch kein Mobile-Device verbunden — installiere die HiveGrid-App und logge dich ein, um Push-Notifications zu erhalten. [App-Store-Link]"*

Operationen

- Test-Push (sendet Klartext-Test: *„Test-Push von HiveGrid"*)
- Device umbenennen
- Device revoken (Push-Token wird entwertet, Eintrag bleibt mit `revoked_at`)
- Bulk-Revoke

Registrierungs-Flow (aus Mobile-App)

1. User loggt sich in Capacitor-App ein (Modul 36)
2. App fragt OS-Push-Permission ab
3. Bei Erlaubt: App holt FCM-/APNs-Token, sendet via `/api/v1/notifications/mobile-device` (Self-Scope, kein API-Key nötig — eingeloggter User)
4. Server prüft: Token bereits registriert? → Update `last_seen_at`. Sonst: neue NotificationDevice-Entity
5. Test-Push optional vom Server, um Token-Validität zu bestätigen

Token-Invalidierungs-Handling

- Bei Push-Versand-Fehler `InvalidToken` von APNs/FCM → Device wird automatisch revoked
- Bei User-Logout: Device wird revoked
- Bei Tenant-Wechsel: Device bleibt aktiv für aktuellen Tenant (User kann mehrere Tenants haben — Push pro Tenant)
- Bei User-Deaktivierung im Tenant: Device-Beziehung zu diesem Tenant gelöscht, kein Push mehr

Permissions

- Self-Scope: User sieht und verwaltet nur eigene Devices
- Tenant-Admin sieht **keine** User-Devices anderer User (Privacy)

Klartext-Hinweise

- Device inaktiv > 30 Tage: *„Dieses Gerät hat sich seit X Tagen nicht gemeldet. [Revoken]"*
- Test-Push fehlgeschlagen: *„Push-Test fehlgeschlagen — möglicherweise wurden Push-Berechtigungen am Gerät widerrufen. [Geräte-Einstellungen]"*
- Push-Quota erschöpft (extremer Edge-Case): *„Versand-Limit erreicht — versuche es in einer Stunde erneut."*

Block I — Event-Typen-Katalog

> ***Dies ist ein Auszug. Vollständiger Katalog entsteht modulweise mit Modul-Specs.***

Lead-Events (Modul 2)

`event_type`	Default In-App	Default Email	Default Push	Bundle-Group
`lead.created`	ja	nein	rolle-abhängig	`lead.created`
`lead.assigned_to_me`	ja	rolle-abhängig	ja	`lead.assigned`
`lead.unassigned`	ja	nein	nein	`lead.assigned`
`lead.responded`	ja	nein	nein	(nie gebündelt)
`lead.spam_marked`	ja	nein	nein	`lead.spam`
`lead.source_paused` (Anomalie)	ja	ja	ja (urgent)	(nie gebündelt)

Deal-Events (Modul 3)

- `deal.assigned_to_me`, `deal.stage_changed`, `deal.won`, `deal.lost`, `deal.stuck` (Eskalation)

Projekt-/Task-Events (Modul 4, 26)

- `project.assigned_to_me`, `project.stage_changed`, `project.acceptance_requested`
- `task.assigned_to_me`, `task.due_soon`, `task.overdue`, `task.completed_by_other`

Termin-Events (Modul 6, 25)

- `appointment.scheduled`, `appointment.reminder_24h`, `appointment.reminder_1h`, `appointment.cancelled`, `appointment.rescheduled`

Chat-Events (Modul 13)

- `chat.mention` (Direkt-Mention `@user`), `chat.dm_received`, `chat.thread_reply`

Email-/Telefonie-Events (Modul 9, 12)

- `email.received_personal`, `email.bounce`, `call.missed`, `call.voicemail`

Automation-Events (Modul 17)

- `automation.execution_failed`, `automation.dry_run_completed`, `automation.rate_limit_hit`

Auth-/Sicherheits-Events (Modul 27)

- `auth.new_device_login` (high), `auth.password_changed` (high), `auth.2fa_disabled` (urgent)
- Diese sind **bundle_disabled** und **immer-aktiv** (kein Opt-Out)

Customer-Portal-Events (Modul 15)

- `portal.user.commented`, `portal.user.approved`, `portal.user.uploaded_file`

KWP-/Integration-Events (Modul 19, 33a)

- `kwp.sync_failed`, `kwp.schema_drift_detected`, `integration.disconnected`

System/Admin-Events

- `tenant.frozen`, `tenant.past_due` (urgent), `subscription.payment_failed`, `audit.export_completed`

Block J — Versand-Pipeline

Architektur (Stichworte)

- **Producer:** alle Module rufen `notificationService.send({ recipientUserId, eventType, subject, ... })` auf
- **Resolver:** lädt User-Preferences und Quiet-Hours, entscheidet pro Kanal Send/Skip
- **Bundle-Manager:** prüft offenes Bundle für Recipient + Event-Group, hängt an oder erstellt neu
- **Queue:** BullMQ (oder gleichwertig — Implementation-Detail) mit Worker pro Kanal
- **Senders:**
- In-App: schreibt `Notification`-Row + sendet SSE-Event
- Email: render Template mit i18n + Branding, sendet via Sending-Domain (Modul 9)
- Push: ruft Novu-API mit gerendertem Payload pro aktivem Device
- **Status-Tracker:** schreibt `delivery_status` zurück bei Erfolg/Fehler
- **Retry-Logik:** 3x mit Backoff bei transienten Fehlern (SMTP-Timeout, FCM-503); kein Retry bei Permanent-Fehlern (InvalidToken, Hard-Bounce)
- **Audit:** Versand wird **nicht** ins Modul-21-Audit geloggt (zu hohe Frequenz; eigenes Versand-Log in `delivery_status` reicht). Ausnahme: Versand-Fehler `urgent` werden auditiert.

EU-Stack (LP-13)

- Email-Versand über EU-SMTP (Mailersend EU oder Resend EU oder selbst-gehostet auf Scaleway)
- Push über Novu (Self-Hosted auf Scaleway oder EU-Cloud); APNs/FCM sind Kanäle, dort unausweichlich aber nur Token + minimaler Payload (kein PII-Datenleck)
- Push-Payload: kein PII außer Subject-Name; Detail nur via Deeplink + App-Login

Failure-Handling

- Email-Hard-Bounce → User-Setting auf Email-aus für 7 Tage + Notification im Center
- Push-InvalidToken → Device revoked, kein Re-Try
- SSE-Disconnect → Polling-Fallback im Client

Block K — Permissions-Anwendung

Permission-IDs

Permission	Erlaubt
(Self-Scope)	Eigenes Notification-Center, eigene Präferenzen, eigene Ruhezeiten, eigene Devices — kein Permission-Bundle nötig
`notifications.admin`	Email-Templates lesen (P1), Test-Notifications senden, Bundle-Settings ändern (P2)

Bundle-Mapping (Variante 2)

Bundle	Atomare Permissions
`notifications.none`	(keine — Notifications laufen Self-Scope)
`notifications.admin`	`notifications.admin`

Anwendung in Routes

- `/notifications`, `/notifications/:id` → eingeloggter User (Self-Scope)
- `/settings/notifications/*` → eingeloggter User
- `/admin/notifications/*` → `tenant.admin` ODER `notifications.admin`
- `/api/v1/notifications/mobile-device` → eingeloggter User (Token-Reg ist Self-Scope)

Cross-User-Notifications

- User kann **nicht** direkt Notification an andere User senden — nur über Modul 17 (Automation Send-Notification-Action) oder explizite User-Interaktionen (z.B. Chat-Mention, Task-Zuweisung)
- Send-Notification-Action in Automation Engine erfordert `automation.write` und `automation.run`-Permissions auf das Automation-Subject

Klartext-Fehler

- Push registrieren ohne Login: 401 mit *„Bitte zuerst einloggen."*
- Test-Notification ohne Permission: nicht sichtbar
- Notification eines anderen Users öffnen: 404 (nicht 403, um Existenz nicht zu offenbaren)

Block L — Klartext-Hinweise

Im Notification-Center:
- Leerer Center: *„Keine Benachrichtigungen — sobald etwas Wichtiges passiert, erscheint es hier."*
- Email-Bounce: *„Emails an dich kommen aktuell nicht an — bitte Email-Adresse prüfen. [Profil]"*
- Push-Permission-Denied: *„Push ist auf diesem Gerät deaktiviert. [Geräte-Einstellungen]"*
- Bundle-Eintrag: *„23 neue Leads — [Alle anzeigen]"*

In Settings:
- Alle Email-aus: *„Du bekommst keine Email-Notifications mehr (außer Sicherheit). [Wieder aktivieren]"*
- Alle Push-aus: *„Du bekommst keine Push-Notifications mehr — Mobile-App-Benachrichtigungen sind komplett aus."*
- Ruhezeit-Konflikt: *„Diese Ruhezeit überschneidet sich mit ‚X' — Vereinigung der Fenster aktiv."*
- Default-Reset: *„Deine bisherigen Einstellungen werden auf den Standard für deine Rolle zurückgesetzt — sicher?"*

Beim Versand-Fehler:
- *„Tenant ‚X' ist im Frozen-Modus — Notifications werden nicht versendet."* (interne Log-Meldung, sichtbar in `delivery_status`)
- *„Empfänger-User wurde deaktiviert — Notification wurde nicht gesendet."*

Bei Anomalie:
- An Tenant-Admin (urgent, kein Bundle): *„Notification-Versand zeigt ungewöhnliches Aufkommen (5x normal). Bitte Automationen prüfen — möglicherweise Loop. [Automation-Studio]"*

Bei Push-Token-Revoke:
- *„Gerät ‚iPhone von Max' wurde abgemeldet — kein Push mehr an dieses Gerät."*

Bei Test-Push-Fehler:
- *„Push-Test fehlgeschlagen — möglicherweise wurden Push-Berechtigungen am Gerät widerrufen oder die App ist nicht installiert."*

Block M — Phase 2 / spätere Features

- **Daily-Digest-Email** (statt Einzel-Mails: tägliche Zusammenfassung aller Notifications mit Bundle-Logik über Tag)
- **Snooze-Funktion** (Notification verbergen für X Stunden, dann wieder im Center)
- **WhatsApp als Notification-Kanal** (Phase 2 Modul 11)
- **Tenant-Admin-konfigurierbare Bundle-Windows** pro Event-Group
- **Tenant-Admin-konfigurierbare Email-Templates** (mit Branding)
- **Notification-Schedule-Rules** (z.B. *„Lead-Notifications nur Mo-Fr 8-18"*)
- **Cross-Device-Read-Sync** (Mark-as-read auf Desktop schließt Push-Banner auf Mobile)
- **Notification-Anomalie-Detection-Auto-Pause** (KI erkennt Notification-Storms, pausiert Quelle, alarmiert Admin)
- **Silent-Push für Hintergrund-Sync** (Mobile-App syncronisiert Daten ohne sichtbare Notification)
- **Notification-Read-Receipts** in Chat (Modul 13 spezifisch)
- **Custom-Sound-Schemas pro Priority** (Mobile)
- **Notification-Pinning** (User pinnt Wichtiges oben im Center)
- **Auto-Cleanup** (Notifications älter als 90 Tage hard-gelöscht; Tenant-Admin-konfigurierbar)
- **Multi-Language-Email-Templates** (User-Sprache in `Contact.language` für Outbound; intern aus `User.language`)
- **Browser-Notification-Channel** (Web-Push-API als 4. Kanal — dort wo User keine Mobile-App hat)

Architektur-Vorschriften (Querschnitt)

- **AV #1, LP-10:** Klartext-Diagnostik überall (Bounce, Permission-Denied, Bundle-Hinweis, Versand-Fehler)
- **AV #5:** Self-Scope-Default — User sieht nur eigene Notifications/Devices
- **AV #6:** Versand-Status in `delivery_status`; Sicherheits-relevante Versand-Fehler werden ins Modul-21-Audit geloggt
- **AV #16:** Rate-Limiting + Anomalie-Detection für Notification-Versand (Schutz vor Loop-getriebenen Storms)
- **AV #20:** KI-Action-Boundary — KI darf Notifications senden nur über Automation-Action mit User-bestätigtem Trigger
- **LP-2:** Mobile-App ist Push-Konsument (Modul 36), nicht Producer — alle Producer sind Server-side
- **LP-8:** Apple-Compliance — Permission-Flow mit Pre-Prompt-Erklärung; keine Pricing-/Upgrade-Inhalte in Push
- **LP-12:** Email-/Push-Templates aus Locale-Files; Phase 1 nur DE
- **LP-13:** EU-Stack — SMTP über EU-Provider, Push-Provider Novu auf Scaleway
- **LP-3, AV #3:** Default-Preference-Sets pro Rolle als deklarative Templates

---

Detail-Spec-Status: DRAFT

Erste vollständige Detail-Spec für Modul 22. **Vor Bau:** Verifizierung mit Noah (zusammen mit Pflichtenheft-Sweep) und Modul 36 (Mobile-App) für Capacitor-Push-Flow-Detail. Bei Implementierung Novu-Konfiguration, Email-Sending-Domain (Modul 9-Integration) und APNs-/FCM-Credentials-Setup.

Offene Detail-Punkte (nicht-blockierend):
- Konkrete Default-Preference-Sets pro Rolle finalisieren (mit Noah am Geerkens-Use-Case)
- Bundle-Window-Default 5 Min validieren (ggf. event-group-spezifisch anders)

- Email-Template-Set Phase 1 (Welche Templates pflegen wir initial: Lead, Task, Termin, Sicherheit, Auth, Subscription, ...)
- Annahme: kein Notification-Auto-Cleanup in Phase 1 (90 Tage UI-Filter, aber DB-Eintrag bleibt) — Validation mit Noah ob Auto-Hard-Delete gewünscht
- Annahme: Versand-Erfolge nicht ins Modul-21-Audit (zu hohe Frequenz) — nur Sicherheits-relevante Failures
- Push-Provider Novu vs. Direct-APNs/FCM: Novu-Abstraktion ist Defaultwahl (siehe Codebase-Inventory) — bei Bau ggf. Re-Eval
- Browser-Push (Web-Push-API) Phase 1 oder Phase 2: Phase 2 angenommen (Mobile-App-First gemäß LP-2)

Abhängige Module:
- Modul 27 (Auth/Permissions) — Self-Scope, `notifications.admin`-Permission
- Modul 17 (Automation) — `send-notification`-Action
- Modul 36 (Mobile-App / Capacitor) — Push-Token-Registrierung, Permission-Flow
- Modul 9 (Email-Inbox) — Sending-Domain für Notification-Mails
- Modul 31 (Branding) — Logo + Primärfarbe für Email-Templates
- Modul 21 (Audit-Log) — Sicherheits-Versand-Failures
- Modul 30 (i18n) — Email-/Push-Template-Strings aus Locale
- Alle Producer-Module (1, 2, 3, 4, 6, 9, 12, 13, 15, 17, 19, 25, 26, 27) — als Notification-Quellen