Externals-Checkliste — 4-Wochen-Sprint

Stand: 2026-06-12 (aktualisiert nach Scope-Schnitt 11.06. — siehe `SCOPE-V1-CUTS.md`) · Abgeglichen mit `.env.example` + allen v1-Phasen. Spalte „Wer" im Team-Meeting ausfüllen. **Kategorie A heute anstoßen — das sind Wartezeiten, keine Arbeit.**

> ***Durch den Scope-Schnitt entfallen/entschärft:*** *A2 nur noch Calendar-Scope (Gmail raus) · A3 Apple-Konto ruht (kein App-Store in v1/v2 — PWA-only, → v3) · A4 Google Play → v3 · A7 Microsoft Entra → v2 · B3 HalloPetra → v2 · B7 FCM/APNs* ***entfällt*** *(PWA → Web-Push/VAPID) · AlephAlpha (B6-Teil) → v2 · Memberspot/Boobora → v2.* ***AD-6 (Mailjet) + AD-7 (mCaptcha) sind GELOCKT*** *(Boilerplate-verdrahtet).* ***NEU: E6 AVV + Auskunfts-Vorlage (Anwalt).***

A — Lange Vorlaufzeit (HEUTE anstoßen, sonst reißt Woche 3–4)

#	Was	Wofür (Phase)	Vorlauf / Risiko	Wer
A1	**KWP (✅ entschärft, 12.06.):** Hersteller richtet Zugang ein, verfügbar ~**19.07.** (nach Launch → P10 = erstes v2-Modul). **Jetzt erledigen:** (a) Callback-URLs zurückmelden: `https://app.hivegrid.de/api/apps/kwp/oauth/callback` + `https://staging-app.hivegrid.de/api/apps/kwp/oauth/callback` (PKCE), (b) **kwp-bnWin.net auf 8.1 N3** bei Geerkens-IT aktualisieren	v2-P10	🟢 kein Sprint-Risiko mehr; Antwort-Mail diese Woche	
A2	**Google Cloud:** OAuth-App + **nur Calendar-API**-Scope-Verifizierung (Gmail-Scopes entfallen — Postfach-Sync → v2)	P16 Kalender (nur Google; Outlook → v2)	🟠 Review Tage–Wochen; Testmodus mit Workspace-Konten als Brücke	
~~A3~~	~~Apple Developer~~	**v3** (kein App-Store in v1/v2 — PWA-only, AD-17)	Konto vorhanden, ruht — keine Aktion	—
~~A4~~	~~Google Play Console~~	**v3** (kein App-Store in v1/v2 — PWA-only)	ruht bis native App (v3)	—
A5	**Stripe-Konto + Live-Verifizierung** (Geschäftsdaten, Bankkonto, ggf. Webseite-Anforderungen)	P20	🟠 Tage; Test-Mode reicht für Entwicklung, Live für Go-Live	
A6	**Sende-Domain einrichten:** SPF/DKIM/DMARC für Mailjet + **Domain-Warm-up** beginnen	P1 (notify), P2 (Einladungen), P14 (Marketing!)	🟠 DNS sofort; Reputation/Warm-up braucht Laufzeit — je früher, desto besser für Zustellbarkeit	
~~A7~~	~~Microsoft Entra (Outlook/Graph)~~	v2 (Outlook-Kalender + Postfach-Sync → v2)	→ v2-Vorbereitung	—

B — Konten/Keys anlegen (Tag 1–3, kurzer Vorlauf)

#	Was	Wofür	Hinweis	Wer
B1	**Mailjet**-Konto + API-Keys	P1/P2/P3/P14	✅ Boilerplate bereits verdrahtet (`MAILJET_*`) → **AD-6 heute formal locken**	
B2	**AirCall**-Konto + API/Sandbox + Webhooks	P15	Sandbox reicht bis W3	

~~B3~~	~~HalloPetra~~	v2 (M105 → v2)	→ v2	—
B4	**PandaDoc** und/oder **DocuSign** Konto + API (Sandbox)	P16 Signatur	einen Provider für Launch wählen, zweiter später	
B5	**Hetzner-Projekt `HiveGrid` anlegen** (Infra-ADR-009): S3-Object-Storage-Bucket + Token, Storage Box (Backups) · **DEK-Master-Key** in Coolify-Secrets (AD-8 revidiert: app-seitige Envelope-Encryption, kein Cloud-KMS) · ⚠ `SCALEWAY_*`-Env-Vars der Boilerplate auf Hetzner-Endpoint umziehen (S3-API identisch)	P4 (Storage), P5/P17 (DEK), Prod-Compute	🟢 Stunden — Muster im Infra-Repo	
B6	**Mistral** (La Plateforme) API-Key — **Primär-LLM** (Infra-Wechsel: Scaleway Generative APIs entfallen; zweiter EU-Provider + Whisper → v2)	P13	✅ in `.env.example` vorgesehen	
~~B7~~	~~FCM/APNs~~	**entfällt** (PWA → Web-Push/VAPID, kein FCM/APNs-Konto nötig)	v2: VAPID-Keys selbst generieren, notify()-Push-Kanal aktivieren	—
B8	**Geo-IP-Dienst** (ipapi.is / ipstack) API-Key	P2 (Session-Standortanzeige)	✅ in Boilerplate; EU-Konformität kurz prüfen oder Feature stubben	
B9	**HaveIBeenPwned** k-Anonymity (frei) bzw. API-Key	P2 (Breach-Check)	k-Anonymity-Endpoint ist kostenlos/ohne Key	
B10	**Subframe**-Workspace + Lizenzen für Designer + Devs	Designer-Track ab W1	sofort, sonst steht D0	

C — Eigene Infra provisionieren (Ops, Woche 1–2)

#	Was	Wofür	Deadline	Wer
C1	**Meilisearch: läuft bereits zentral auf `node1`** (Infra-ADR-008) — nur **scoped Key minten** (`indexes: ["hivegrid-*"]`, Muster: Boilerplate-Key vom 06.06.; `MEILI_API_KEY`, nicht Master-Key!)	P11 (AD-5)	🟢 5 Minuten statt Setup	
C2	**mCaptcha: läuft bereits zentral** auf `captcha.saas-ctrl.com` (Infra-ADR-013) — nur ENV anbinden + Sitekey anlegen (AD-7 ✓)	P2 Login, P16 Public-Forms/Booking	🟢 anbinden statt aufsetzen	
C3	**Hosting/Deploy (Infra-ADR-009/010, ersetzt Fly/Scaleway — `fly.toml` entfernt, `deployment-region-provider-pinning.md` stale!):** Staging auf `staging-1` via zentrale **Coolify**-Control-Plane (Muster: Boilerplate läuft dort mit 8 Apps) · Prod = Hetzner-Projekt `HiveGrid` (`hivegrid-db` / `-app` / `-worker` / `-lb`) · Registry = Gitea, build-once/promote (Infra-ADR-005). **Staging (User-Entscheidung 12.06., revidiert): ÖFFENTLICH** auf `staging-app.hivegrid.de` + `staging-api.hivegrid.de` (beide unter dem `*.hivegrid.de`-Wildcard-Zertifikat, kein VPN). **Pflicht-Härtung dafür:** (a) **NUR synthetische Daten** — niemals echte Kunden-/Geerkens-Daten auf Staging (DSGVO; Demo-Seeds reichen), (b) eigene Secrets/Keys je Umgebung (Stripe Test-Mode, eigene OAuth-Apps, eigene Webhook-Secrets), (c) Webhooks auf staging-api mit HMAC-Signaturpflicht + Rate-Limit, (d) `X-Robots-Tag: noindex` + robots.txt deny, (e) Login wie Prod (TOTP), optional IP-Allowlist nachrüstbar. OAuth-Callbacks: Staging-Redirect-URIs (`staging-app.…`) bei KWP/Google mitregistrieren	ab W1 (CI/Gates brauchen Staging!)	Mitte W1	
C4	**Postgres + Redis: Coolify-managed** (Staging auf `staging-1`, Prod auf `hivegrid-db` — Muster: mITapp/Boilerplate; PgBouncer auf staging-1 vorhanden, siehe `docs/ops/pgbouncer.md`)	alles	Mitte W1	
C5	**Domains/DNS + TLS (Cloudflare — `hivegrid.de`-Zone existiert bereits!):** `app.hivegrid.de` + `admin.hivegrid.de` (Host-Routing + Cookie-Domain-Trennung!) + `staging-app.hivegrid.de` + `staging-api.hivegrid.de` (öffentlich, siehe C3) — ein `*.hivegrid.de`-Wildcard deckt alle. Portal/Forms/Booking/Help/API sind **Pfade** unter app.* gemäß `INTEGRATION-CONTRACTS.md` §6 (korrigiert 12.06.)	P1 URL-Schemata, P19 Admin, C3 Staging	W1	

C6	(Optional) **Authentik** für Admin-SSO (AD-3, optional)	P19	kann Fast-Follow sein	

D — Entscheidungen, die heute fallen können (Boilerplate hat sie quasi getroffen)

#	Entscheidung	Faktenlage	Aktion
D1	**AD-6 EU-Email-Provider**	Boilerplate ist auf **Mailjet** verdrahtet (Keys, Webhooks, Worker-Delivery) — Tendenz im ADR war ohnehin Mailjet	Heute locken: ADR-Eintrag auf `Accepted`, Konto anlegen (B1), Domain-Setup (A6)
D2	**AD-7 Captcha**	Boilerplate liefert **self-hosted mCaptcha** inkl. Infra-README — EU-perfekt (PoW, keine US-Firma)	Heute locken: ADR auf `Accepted`, Instanz aufsetzen (C2)
D3	**EU-Sterilisations-Zusatzfunde**	`.env.example` enthält noch **GA-Tracking** (`ANALYTICS_GA_TRACKING_ID`) + **ConvertKit** (US)	In P1-Scope aufnehmen: entfernen/ersetzen (Analytics → EU-Alternative oder raus)
D4	Signatur-Provider primär	PandaDoc **oder** DocuSign für Launch	im Team-Meeting wählen (B4)

E — Organisatorisch (Menschen & Termine)

#	Was	Wann	Wer
E1	**Noah: 4 Freitags-Slots** für Gate-Demos fest blocken (W1 CRM-Vorschau, W2 CRM, W3 Kette, W4 Voll-Walkthrough)	heute terminieren	
E2	~~KWP-Ansprechpartner identifizieren~~ ✅ läuft (KWP-Mail an Noah, 12.06.) · **NEU: Noah-Frage — gehört der Lagerist-Arbeitsplatz (M070) zum Validierungs-Versprechen?** (entscheidet, ob die M070-Dünnung hält)	bei Demo #1 (Fr W2)	
E3	Echte SHK-Beispieldaten von Geerkens für Seeds-Validierung (Pipelines, Custom-Felder, Rollen)	bis W2	
E4	Dev-Zuordnung Tracks A/B/C + Scope-Leiter-Abnahme	Team-Meeting	
~~E5~~	~~App-Store-Metadaten~~ → **v3** (kein App-Store in v1/v2 — PWA-only)	—	—
E6	**AVV-Vertragsvorlage (Auftragsverarbeitung, Art. 28) + DSGVO-Auskunfts-Vorlage** vom Anwalt — Launch-Pflicht für jeden Mandanten!	diese Woche beauftragen	

Merksatz fürs Meeting: Kategorie A sind **Wartezeiten** — jede Stunde Verzögerung beim Anstoßen wandert 1:1 ans Ende des Sprints. B+C sind Arbeit, die parallel läuft. D sind Geschenke der Boilerplate — einfach locken.