Majster.AI — Tracker gotowości SaaS (żywa checklista)

Cel: jeden plik, który trzymasz w projekcie Majster, żeby śledzić co jest źle, czego brakuje, co trzeba weryfikować za każdym razem oraz żeby odznaczać elementy w miarę napraw.

Zasady: evidence-first, zero zgadywania. Jeśli czegoś nie zweryfikowano → oznacz jako `UNKNOWN` i dopisz, jakich dowodów brakuje.

0) Snapshot (uzupełniaj przy każdej aktualizacji)

- Data:
- Źródło dowodów:
- Screenshoty: (lista)
- Testowane URL-e:
- GitHub PR/commit:
- Vercel deployment:
- Tester:
- Wynik: PASS / FAIL

1) Executive Summary (dla laika)

Ten tracker pokazuje, co aktualnie blokuje Majster przed byciem prawdziwym SaaS (a nie demem), oraz powtarzalne testy, które muszą przechodzić po każdej zmianie.

Element oznaczasz jako DONE dopiero wtedy, gdy dołączysz dowód (URL + screenshot/log/wynik testu).

2) Aktualne findings (z ostatnich screenshotów, które podałeś)

Referencje dowodów

- `S-2026-02-17-0828`: ekran Ustawień (Ustawienia → Język / Prywatność i dane)

Tabela findings (aktualizuj status w miarę napraw)

	Obszar	Severity	Problem	Dowód	Status	Naprawa (krótko)	Weryfikacja (wymagany dowód)
01	i18n	P0	Przełącznik języka jest, ale brak realnych języków (wygląda, że tylko PL).	`S-2026-02-17-0828`	TODO	Podłączyć provider i18n + paczki językowe (PL/EN/UK). Przełącznik ma realnie zmieniać tekst UI.	Screenshot pokazujący opcje EN + UK oraz zmian tekstów UI na 3 stronach

	Obszar	Severity	Problem	Dowód	Status	Naprawa (krótko)	Weryfikacja (wymagany dowód)
02	Legal/Privacy UX	P1	Przyciski prywatności/prawne widoczne dla użytkownika w Ustawieniach (Centrum RODO, Polityka Prywatności, Cookies, Regulamin, Umowa DPA). To zwykle jest OK jako *tylko podgląd*, ale edycja musi być wyłącznie dla admina.	`S-2026-02-17-0828`	TODO	Zostawić użytkownikowi możliwość podglądu, ale dopilnować poprawności treści i tego, że edycja jest tylko w panelu Owner/Admin (CMS).	Potwierdzić, że user nie m edycji. Potwierdzić, że treści stron są poprawne.
03	Produkt	P1	Ustawienia pokazują tylko podstawowe sekcje; trzeba zweryfikować brakujące kluczowe ustawienia SaaS (bezpieczeństwo konta, sesje, klucze API, powiadomienia, zespół).	`S-2026-02-17-0828`	TODO	Dodać brakujące strony ustawień albo ukryć zakładki do czasu wdrożenia.	Screenshot pełnej architektury informacji (IA Ustawień albo usunięcie martwych zakładek.

> UWAGA: Część wcześniejszych problemów (np. bloki „REKLAMA”, deployment protection na Vercel, bazowy URL w sitemap) była widoczna w starszych screenach. Zostają w globalnej checkliście poniżej, bo muszą być weryfikowane przy każdym release. Jeśli już są naprawione — oznacz DONE i dołącz dowód.

3) Definicja: „SaaS, nie demo”

Majster jest SaaS-ready tylko wtedy, gdy wszystkie elementy P0 poniżej są DONE z dowodami, a każdy release przechodzi Regression Matrix (Sekcja 7).

Baseline SaaS = publiczny dostęp + prawdziwe auth + realna ochrona danych + stabilny deploy + poprawna legalka + monitoring + backupy + powtarzalne QA.

4) Blokery P0 (muszą być DONE zanim nazwiesz to SaaS)

4A) Dostęp & Deploy (Vercel)

☐ P0-A1 Publiczny dostęp działa (brak ściany Vercel-auth dla zwykłych userów).

Weryfikacja: otwórz produkcyjny URL w incognito na urządzeniu, które nie jest zalogowane do Vercel; dołącz screenshot.

☐ P0-A2 Preview jest chronione, Production jest publiczne (rekomendowane).

Weryfikacja: screenshoty ustawień Vercel: Deployment Protection.

☐ P0-A3 Canonical URL + sitemap używają poprawnej domeny produkcyjnej (nie losowego hasha deploya).

Weryfikacja: otwórz `/sitemap.xml` i potwierdź, że URL-e używają domeny produkcyjnej; dołącz screenshot + fragment odpowiedzi.

☐ P0-A4 Zero wycieków sekretów do klienta (w frontend tylko publiczne `VITE_*`).

Weryfikacja: sprawdź output buildu albo listę env var; potwierdź, że nie ma sekretów serwerowych.

4B) Auth & Role (Supabase)

☐ P0-B1 Auth end-to-end działa: rejestracja, logowanie, wylogowanie, reset hasła.

Weryfikacja: screenshoty + dowód maila (albo logi Supabase).

☐ P0-B2 Separacja Owner/Admin jest realna (nie tylko UI):

• user nie ma dostępu do tras admina

• trasy admina mają server-side checki autoryzacji

Weryfikacja: spróbuj wejść na `/admin` jako zwykły user; dołącz dowód.

☐ P0-B3 RLS włączone na wszystkich tabelach + poprawne polityki dla każdej roli.

Weryfikacja: screenshoty polityk Supabase + test: user A nie może czytać danych usera B.

☐ P0-B4 Buckety Storage są chronione (brak public read/write jeśli nie planowane).

Weryfikacja: polityki Supabase Storage + test dostępu.

4C) Bezpieczeństwo danych & zgodność

☐ P0-C1 GDPR/RODO basics: polityka prywatności, cookies, regulamin są poprawne i podpięte do właściwych tras.

Weryfikacja: otwórz każdą stronę i potwierdź poprawną treść.

☐ P0-C2 Zgody cookies realnie działają (zapisują zgodę, blokują nie-niezbędne do akceptacji).

Weryfikacja: dowód network/storage + screenshoty.

☐ P0-C3 Procesy praw użytkownika: eksport danych, usunięcie konta/danych (minimum: flow istnieje).

Weryfikacja: screenshot flow + dowód z logów backend.

4D) Niezawodność

☐ P0-D1 Monitoring: śledzenie błędów (Sentry lub równoważne) aktywne na produkcji.

Weryfikacja: testowy błąd pojawia się w dashboardzie.

☐ P0-D2 Backup & recovery: zaplanowane backupy Supabase i udokumentowana procedura restore.

Weryfikacja: screenshot konfiguracji backupu + link do runbooka w repo.

5) Utwardzanie P1 (powinno być DONE dla jakości „MVP+”)

5A) i18n zrobione poprawnie (PL/EN/UK)

☐ Wszystkie widoczne stringi UI są w plikach tłumaczeń (brak raw keys).

☐ Przełącznik języka zapamiętuje wybór (localStorage/profil) i po odświeżeniu działa.

☐ Format dat/liczb/walut zgodny z locale.

☐ Migracja UA→UK zakończona (jeśli dotyczy).

☐ Admin może edytować statyczne treści legal/marketing per język (CMS).

5B) UX polish

☐ Brak nachodzenia pływających przycisków na mobile (chat/CTA).

☐ Skeletony / empty states / error states na każdej liście.

☐ Touch targets ≥ 44px; działa nawigacja klawiaturą.

☐ Accessibility: etykiety, ARIA, kontrast, focus (WCAG AA).

5C) Performance

☐ Lighthouse: zebrany baseline Performance/SEO/Best Practices/Accessibility.

☐ Bundle size monitorowany; brak oczywistego bloatu.

☐ Poprawne nagłówki cache dla assetów statycznych.

5D) Higiena bezpieczeństwa

☐ Audyt zależności (`npm audit` / Snyk/Trivy) przejrzany; krytyczne CVE naprawione.

☐ Brak wrażliwych logów (CodeQL high rozwiązane albo uzasadnione).

☐ Rate limiting / anti-abuse na formularzach i endpointach auth (minimum).

6) Kompletność produktu (co ma większość „prawdziwych SaaS”)

Dla każdego elementu ustaw: `DONE / TODO / NOT PLANNED` i link do roadmapy lub issue.

6A) Konto

☐ Profil (imię, firma, VAT/NIP, adres)

☐ Bezpieczeństwo: zmiana hasła, sesje/urządzenia, MFA (później)

☐ Preferencje powiadomień (email/push)

☐ Usuń konto (z potwierdzeniem + zasadami retencji)

6B) Zespół / multi-tenant (jeśli planowane)

☐ Workspaces/Teams

☐ Zaproszenia, role, uprawnienia

☐ Billing per workspace

6C) Billing (jeśli planowane)

☐ Strona planów, checkout, faktury, anuluj/wznów

☐ Trial, grace periods

☐ Webhooki i entitlement checks

6D) Panel Admin/Owner (musi być realny)

☐ Zarządzanie treściami stałymi (strony prawne, copy, tłumaczenia)

☐ Diagnostyka (logi, eventy błędów, zgłoszenia użytkowników)

☐ Feature flags

☐ Anti-abuse (rate limits, bany)

7) Macierz testów regresji (musi przechodzić po każdej zmianie)

7A) „Critical path” manual smoke (10 minut)

1. [ ] Landing ładuje się (mobile + desktop)
2. [ ] Sign up → weryfikacja maila (jeśli włączone) → login
3. [ ] Dodaj klienta
4. [ ] Dodaj projekt
5. [ ] Utwórz ofertę (manual)
6. [ ] Utwórz ofertę (AI assistant) — jeśli włączone
7. [ ] Wygeneruj PDF + pobierz
8. [ ] Logout → login ponownie
9. [ ] Ustawienia otwierają się; linki prawne otwierają poprawne strony
10. [ ] Strona 404 działa; powrót do aplikacji

Dowód: 5 screenshotów + 1 krótki screen recording (idealnie).

7B) Automaty (CI)

☐ lint

☐ unit tests

☐ integration tests (Supabase mock albo test project)

☐ e2e (Playwright) — minimum: login + create project

☐ SAST (CodeQL) baseline

☐ dependency scan baseline

Reguła: No Green, No Finish.

8) Wzorzec „world-class SaaS” dla UI legal/privacy (benchmark)

Typowe w dojrzałym SaaS:

• Użytkownicy muszą mieć możliwość PODGLĄDU polityki prywatności, cookies, regulaminu. To normalne w Ustawieniach albo w stopce.

• Użytkownicy nie powinni mieć możliwości EDYCJI tych dokumentów. Edycja powinna być tylko w Owner/Admin (CMS).

• „RODO Center / Privacy Center” dla praw użytkownika (download/delete) jest częste, ale akcje muszą być kontrolowane i logowane.

Czyli problemem nie jest to, że linki są widoczne — problemem jest:

1) Czy te strony są poprawne i podpięte do właściwych tras?

2) Czy jakiekolwiek capability admin-only jest widoczne dla zwykłego usera?

3) Czy operacje praw użytkownika są zaimplementowane bezpiecznie?

9) Routing narzędzi (jak wykonujemy fixy)

• Claude Opus 4.6 → decyzje architektoniczne, audyty, walidacja roadmapy, rozumowanie cross-system.

• Claude Sonnet 4.5 → wykonanie, wąsko-zakresowe wdrożenia, weryfikacja CI.

• Prompty do narzędzi: tylko po angielsku (mniej tokenów, mniejsza niejednoznaczność).

10) Change log (dopisywać na końcu)

• YYYY-MM-DD: …