

01 · Data model — Supabase

Project kbmvtawsdhmzjnsnazar (NIE Experts Site, eu-west-1). Verified live 2026-06-30. Postgres public: **14 tables + 2 views**. All timestamps `timestamp tz`. Access is **service-role only** (app/n8n use the service key, which bypasses RLS) — see Security.

Entity map

orders (Stripe checkout) —< practices (one per person) —< tokens
(Fase-2 magic link)

upsell_items

practice_satisfaction_events

affiliates —< affiliate_commissions

lifecycle status

affiliate_clicks (by referral_code)

admins · event_log · agent_events · processed_events · signup_attempts · kpi_snapshots · partner_appointments(view) · agent_practice_v(view)

orders.id and practices.order_id are both **Stripe checkout session ids** (cs_...). No DB-level FK between them (see AUDIT-FINDINGS H7).

Core tables

orders — purchase / checkout intent

id text **PK** (Stripe session id) · tier tier_t · amount_eur · payer_email · payer_whatsapp · persons · status text (free-text, def pending) · tier_label · consulenza_flag · appuntamento_flag · appointment_qty · client_id · notion_page_id/notion_synced_at · stripe_sessions jsonb · reminders_sent · phase1_sent_at · contacts_collected · created_at/updated_at. Trigger set_updated_at.

practices — core entity (one NIE case per person)

id uuid **PK** · order_id text (→orders, no FK) · full_name/gmail/whatsapp_intl (PII, NOT NULL) · situation situation_t · urgency/urgency_weeks · tier tier_t · status status_t (def created). Flags: is_head_of_household, priority_appt_flag, consultation_flag, drive_access_active(def true), refund_eligible. Drive: drive_*_file_id, drive_*_folder_id, share_permission_id, share_status. Lifecycle ts: docs_delivered_at, guide_shared_at, outcome_at, escalated_at, id_doc_purged_at... Review engine: dissatisfaction_score(def 0), objection_count, dissatisfaction_tags text[], review_hard_blocked, review_block_reason, review_eligible, review_requested, review_completed, rejection_count. id_doc_url (PII, purged by W21) · notion_page_id · language. Trigger set_updated_at.

tokens — single-use Fase-2 access

token uuid **PK** · practice_id →practices CASCADE · used/used_at · expires_at(def now()+14d) · attempts(def 0) · max_attempts(def 5). Minted W02 → consumed W03 (NIE_LIB-TokenConsume) → re-minted W05 on contact correction.

upsell_items

id uuid **PK** · practice_id →practices CASCADE · type upsell_t · stripe_payment_id **UNIQUE** · people · created_at.

practice_satisfaction_events — review-engine stream (append-only)

id uuid **PK** · practice_id →practices CASCADE · event_type · weight int · note · source(def agent). **RLS DISABLED** (D2). Written by log_satisfaction_event().

Affiliate tables

affiliates

id uuid PK · email **UNIQUE** · referral_code **UNIQUE** · status(pending/approved/rejected) · stripe_account_id · stripe_payouts_enabled(def false) · country(def IT) · magic_link_jti · last_magic_link_at · approved_at.

affiliate_commissions

id uuid PK · affiliate_id →affiliates · order_id text **UNIQUE** (→orders, no FK) · product · amount_eur · status(def pending) · paid_at · stripe_transfer_id · customer_name. CHECK status ∈ {pending, approved, paying, paid, refunded, clawed_back}. Amounts: digital €5 / expert €10 / concierge-plus €20.

affiliate_clicks

id uuid PK · referral_code · created_at. Joins affiliates by value (no FK).

Supporting

- **admins** — magic-link admin accounts (email **UNIQUE**, magic_link_jti); gates payout-approval page.
- **agent_events** — outbound queue for the WhatsApp/automation agent (event, practice_id no FK, payload jsonb, delivery_status).
- **event_log** — workflow/audit log (workflow, level, event, order_id, practice_id, message, detail jsonb).
- **processed_events** — idempotency ledger (event_id PK, source event_source_t).
- **signup_attempts** — affiliate-signup rate-limit (hashed IP).
- **kpi_snapshots** — daily KPI rollup, one row per snapshot_date (PK), ~40 metrics. Written by W13.

Views

- **agent_practice_v** — agent projection of practices (id→practice_id, English-izes situation). Read model for the automation agent.
- **partner_appointments** — partner slice where tier='concierge' OR priority_appt_flag (name, situation, appointment date/url, partner_notes).

Enums (exact)

Type	Values
tier_t	digital, expert, concierge
situation_t	studente, lavoratore, in_cerca_di_lavoro, situazione_specifica
status_t	created, phase2_sent, docs_pending, docs_delivered, guide_shared, appointment_booked, nie_obtained, nie_rejected, error_email, error_whatsapp, disputed, abandoned, contact_corrected, archived, refunded, awaiting_outcome, presumed_obtained, nie_rejected_consultation_done, closed, pdf_generation_failed
upsell_t	appointment, consultation
event_source_t	stripe, tally, whatsapp, calcom, resend, drive

Functions & triggers

- set_updated_at() — BEFORE UPDATE on orders, practices, kpi_snapshots.
- log_satisfaction_event(p_practice_id, p_event_type, p_note, p_source) → records/weights a satisfaction event, updates dissatisfaction_score/tags, applies hard-block rules, returns (dissatisfaction_score, review_hard_blocked, review_eligible, escalate). Core of the review-gating engine (feeds W20; called by agent tool W22).

Security model

- **RLS enabled on 13 tables but ZERO policies** → anon/authenticated = deny-all. App/n8n use the **service-role key** (bypasses RLS). Implication: whole posture depends on the service key never leaking; an anon key would silently get nothing. No defense-in-depth layer.
- `practice_satisfaction_events` has **RLS disabled** (inconsistent — D2).
- Views run definer-rights and **expose practices PII** without own RLS — never grant to public roles.
- Hardening: AUDIT-FINDINGS H1, D2, H6, H7.