agentize.eu PoC — Vibe-Coding Context & Constraints

Ez a dokumentum a kódolási session-ök előtt olvasandó. Minden üzleti döntés és constraint egy helyen.

AMIT ÉPÍTÜNK — Egy mondatban

Enterprise AI platform PoC: Teams/Telegram chatbot → LangGraph agent → többpontos jóváhagyás → PDF output, az ügyfél Azure-jében, EU Data Zone Standard-ban.

MEGVÁLTOZTATHATATLAN DÖNTÉSEK

Ezek nem vitathatók, a csapat (HIGHNESS + Péter) és a Gábor-féle stratégiai tanácsok alapján lezárultak:

#	Döntés	Miért
1	**LangGraph** (NEM LangChain chains)	GA, production-ready, ~400 cég használja. Architekturálisan különböző.
2	**Nincs AI Search / RAG a PoC-ban**	User input-ból dolgozunk, nem dokumentum-RAG-ból. Legnagyobb költségtétel ($245/hó) kiesik.
3	**Sweden Central, Data Zone Standard**	EU adatrezidencia garancia. Nem alkuképes autóipari ügyfelek számára.
4	**Bot Framework** (Teams SDK)	Multi-channel (Teams + Telegram). 3 versengő SDK van — ez a stabil.
5	**Nem Managed Application**	PoC-ban sima resource group + RBAC. Deny Assignment blokkolta volna az AI Foundry-t.
6	**PDF az elsődleges output**	A jelenlegi outputok PDF-ben készülnek, ez nem változik.
7	**Többpontos jóváhagyás** (nem hallucináció framework)	Folyamatos interakció + review + final approval. Nem kell confidence scoring / golden dataset.
8	**EU AI Act jelölés**	"AI által generált tartalom" — 2025 feb óta kötelező. Minden output-on.
9	**Cosmos DB (MongoDB API)**	Kompatibilis a meglévő kódbázissal. Serverless a PoC-ban.
10	**Token költség → agent vendor**	A platform infra fix, az LLM fogyasztás az agent vendor dolga.

NINCS BENNE A PoC-BAN

Ha a vibe-coder bármelyiket el akarná kezdeni, ÁLLÍTSD MEG:

- ❌ Azure AI Search / RAG pipeline
- ❌ Private Link hardening (7 pontos checklist)
- ❌ TISAX / ISO dokumentáció
- ❌ Hallucináció framework (confidence scoring, golden dataset, refusal on low score)
- ❌ React Tab szerkesztő
- ❌ SharePoint mentés (Graph API)
- ❌ Multi-tenancy
- ❌ Metered billing / Marketplace integráció
- ❌ Managed Application wrapper
- ❌ Azure Lighthouse
- ❌ Partner Dashboard
- ❌ AKS migráció

ARCHITEKTÚRA QUICK REFERENCE

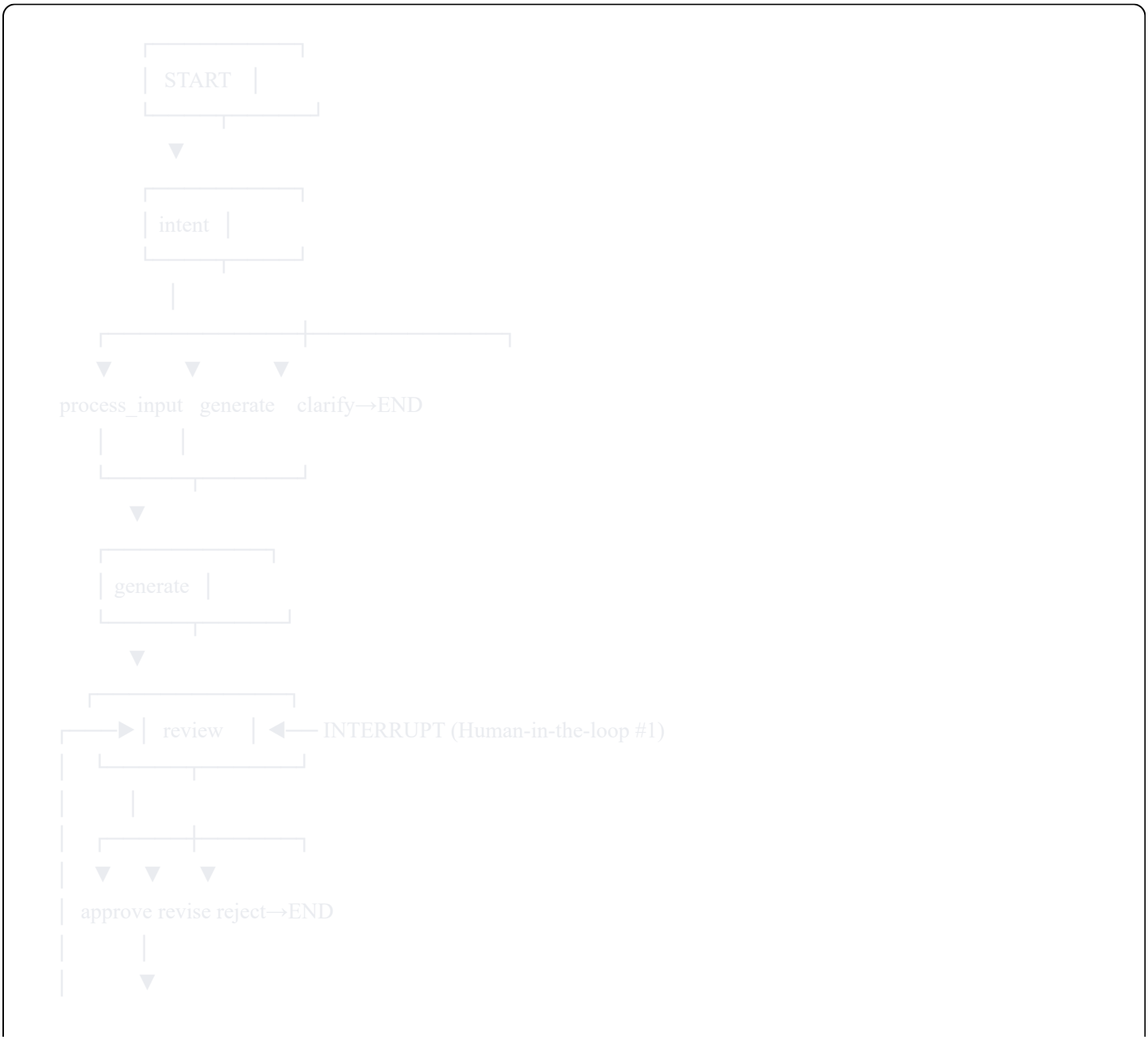
```
User (Teams/Telegram)
  → Azure Bot Service
  → FastAPI (Container App, minReplicas:1)
  → LangGraph Agent Graph:
      intent → process_input → generate(AI Foundry) → review(HITL#1) → [revise loop] → approve(HITL#2) →
output(PDF) → audit(Cosmos)
  → PDF → Blob Storage → SAS URL → User
```

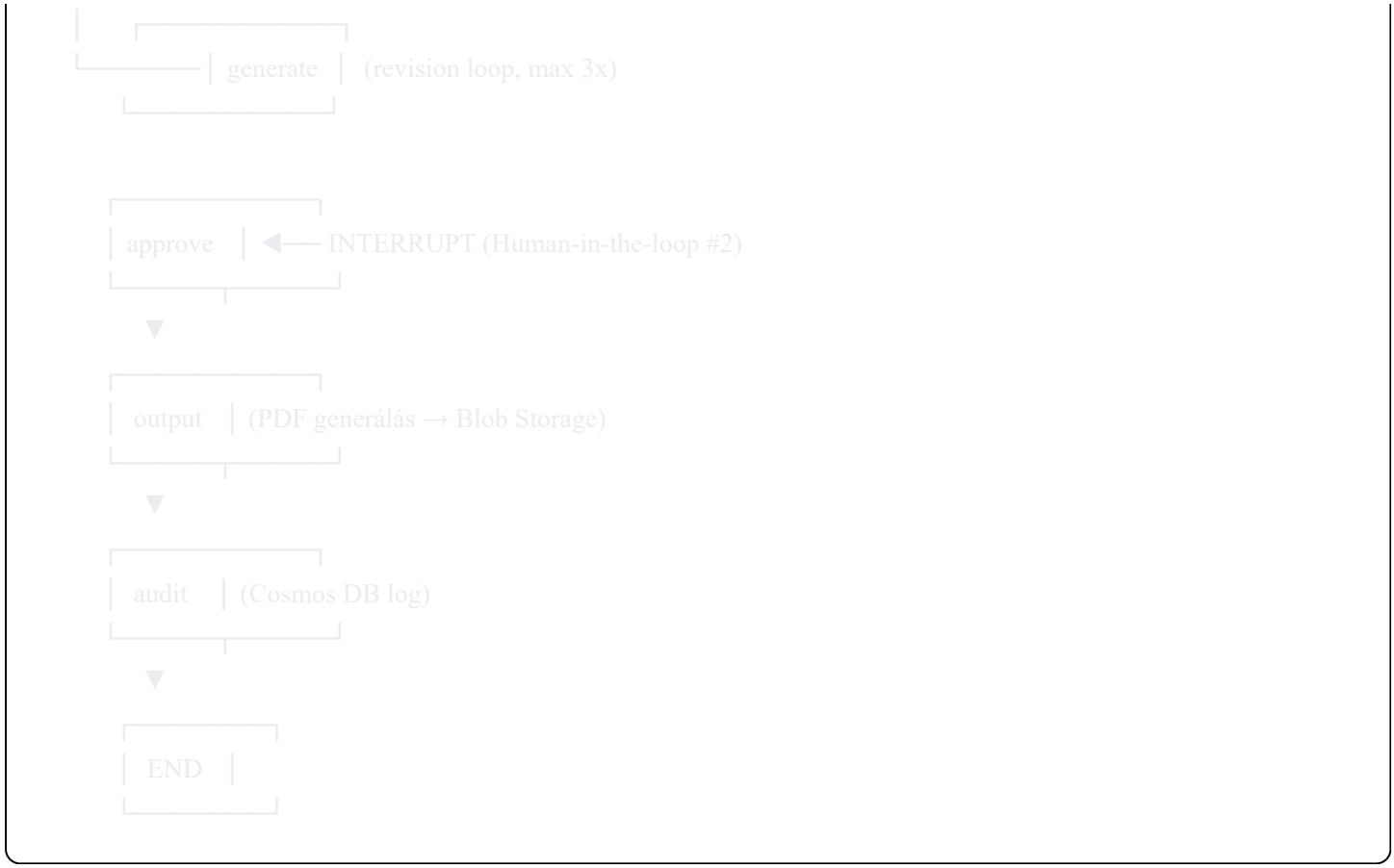
Tech Stack

Kategória	Technológia	Verzió/Megjegyzés
Orchestráció	LangGraph	0.3.x, GA
Backend	FastAPI + uvicorn	Python 3.12
Bot	Bot Framework (botbuilder-core)	4.16.x
LLM	Azure AI Foundry	Mistral Large VAGY GPT-4o, Data Zone Standard
DB	Cosmos DB (MongoDB API)	Serverless, motor async driver

Kategória	Technológia	Verzió/Megjegyzés
Storage	Azure Blob Storage	PDF output, SAS URL-lel
PDF	WeasyPrint	Jinja2 template → HTML → PDF
Secrets	Azure Key Vault	RBAC auth
Monitoring	Application Insights	PII masking kötelező
Identity	Microsoft Entra ID	SSO/OBO, App Registration
Deploy	Azure Container Apps	minReplicas: 1, VNET
CI/CD	GitHub Actions	Build → ACR → Container App

LANGGRAPH GRÁF STRUKTÚRA





ADAPTIVE CARD FLOW

1. User ír → Bot válaszol "⏳"

2. [REVIEW CARD] ← Human-in-the-loop #1
   - ✅ Jóváhagyom" → APPROVAL CARD
   - 🖍️ Szerkesztés" + feedback → újra REVIEW CARD (max 3x)
   - 🗑️ Elvetés" → END

3. [APPROVAL CARD] ← Human-in-the-loop #2 (KÖTELEZŐ)
   - ✅ Ellenőriztem és jóváhagyom" → PDF generálás → RESULT CARD
   - ↩️ Vissza" → REVIEW CARD

4. [RESULT CARD]
   - 📥 PDF letöltés" (SAS URL, 24h érvényes)

COSMOS DB COLLECTIONS

Collection	Tartalom	Partition Key	TTL
conversations	Chat session-ök	conversation_id	90 nap

Collection	Tartalom	Partition Key	TTL
agent_state	LangGraph checkpoints	thread_id	—
generated_documents	Generált TWI doksik	tenant_id	—
audit_log	Minden esemény	tenant_id	—

KÖLTSÉGMODELL (Revised — AI Search NÉLKÜL)

Komponens	Havi költség
Container Apps (1 app, minReplicas:1)	~$40-55
Cosmos DB (serverless)	~$10-30
Blob Storage (LRS)	~$3
Key Vault	~$1
Private Endpoints (×3-4)	~$22-30
App Insights	~$5-15
Bot Service (S1)	~$0 (included)
Platform infra összesen	**~$80-135/hó**
AI Foundry token cost (változó)	→ Agent vendor fizeti

Sales price target: 2.5-3x markup → ~$300-400/hó alap

ENTRA ID APP REGISTRATION CHECKLIST

Az Azure Bot Service-hez szükséges:

- ☐ Entra ID → App Registrations → New Registration
- ☐ Name: "agentize-poc-bot"
- ☐ Supported account types: **Single tenant** (PoC-ban)
- ☐ Redirect URI: nem kell (Bot Framework kezeli)
- ☐ Client secret generálás → Key Vault-ba mentés
- ☐ API permissions: Microsoft Graph → User.Read (delegated)
- ☐ Bot Service resource-ban: msaAppId = App Registration client ID

KNOWN RISKS & WORKAROUNDS

Rizikó	Valószínűség	Workaround
AI Foundry kapacitás Sweden Central-ban	Közepes	Első nap tesztelni. Fallback: Germany West Central
Teams App sideload tiltva az org-ban	Alacsony	Admin engedély kérés, vagy Telegram-on demózni
WeasyPrint rendszerfüggőségek Docker-ben	Alacsony	Dockerfile-ban telepítve (pango, harfbuzz, gdk-pixbuf)
Cosmos DB serverless cold start	Alacsony	Első query lassabb (~1-2 sec), utána OK
Bot Framework token refresh	Alacsony	Adapter automatikusan kezeli
Adaptive Card méretkorlát	Közepes	Draft szöveg max 2000 karakter a card-ban, teljes szöveg a PDF-ben

---

REFERENCE DOKUMENTUMOK

A PoC a következő dokumentumokon alapul (a projekt repository-ban találhatók):

1. **architektura_terv_2_0.md** — Teljes architektúra terv (5 réteg, MVP definíció, TISAX lefedettseg, TCO)
2. **revised_architecture_v2.md** — Counter-proposal, TISAX gap analysis, security hardening
3. **assessment_hu.md** — Kritikai értékelés, 47 kockázat, Managed App probléma
4. **platform_pivot_elemzes_hu.md** — Platform pivot stratégia (HU), marketplace mechanika, DACH GTM
5. **Agentize_eu_Platform_Pivot...md** — Platform pivot stratégia (EN), moduláris árazás, AI training expansion
6. **Péter email feedback** — AI Search kiejtés, nincs RAG, PDF kell, Telegram támogatás, hallucináció kezelés = workflow

---

Utolsó frissítés: 2026-02-26