mVISZ-EIVOK-Kiber-AI konf délután 2026

OTP előadás: Felelős és biztonságos AI implementáció alaplépései

OTP Bank

2026. május 14.

Előadó: Nagy Zsombor, OTP Bank Nyt. Innovation Tribe, AI Office CoE

Agenda

1. Külső szabályozások, kontextus
2. Egy bank miért és hogyan használ AI-t
3. Példa esetek
4. Mellékletek

Szabályozói események és a rájuk adott intézkedések

Tevékenységünk célja, hogy a Bank megfeleljen a mesterséges intelligenciára vonatkozó harmonizált szabályok megállapításáról szóló (EU) 2024/1689 Rendeletnek („EU AI Act").

Kérdés: Hogyan használja az „AI" megoldásokat egy pénzintézet?
Válasz: Szabályosan és komplexen!!

2023.07.	2023.	2024.08.	2025. 02.-tól	2025. 03.31.	2025.08.02.; 2026.08.02.
MNB GTMI vizsgálat	MNB észrevételek és elvárt intézkedések megküldése	EU AI Act hatályba lépése	EU AI Act Tiltott AI megoldások lekapcsolása	Intézkedések végrehajtása és ellenőrzéseken megfelelés	Kapcsolódó szabályzatok frissítése; EU AI ACT további rendelkezések

- **Eszközökkel**
- **Folyamatokkal**
- **Szabályozással**
- **Képzéssel**

Agenda

1. Külső szabályozások, kontextus
2. **Egy bank miért és hogyan használ AI-t**
3. Példa esetek
4. Mellékletek

Használjuk, de mire?

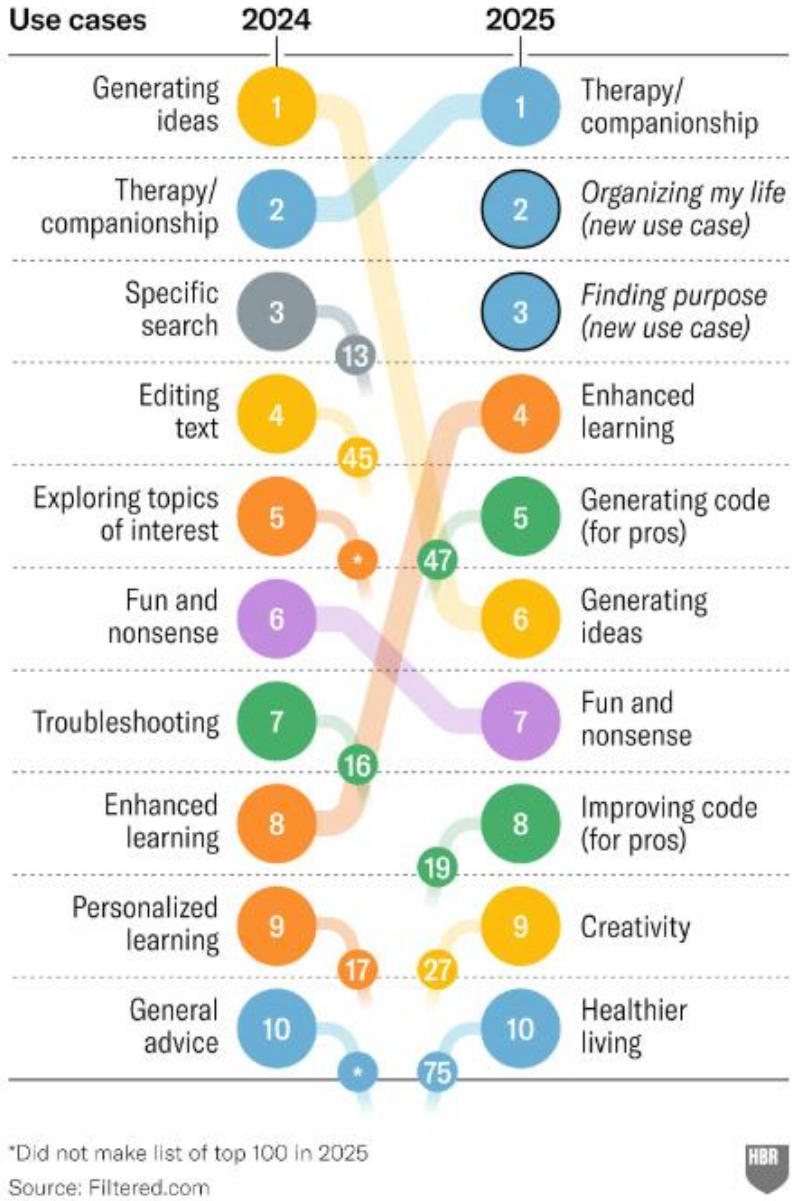
Magánszemélyként

Top 10 Gen AI Use Cases

The top 10 gen AI use cases in 2025 indicate a shift from technical to emotional applications, and in particular, growth in areas such as therapy, personal productivity, and personal development.

Themes

- PERSONAL AND PROFESSIONAL SUPPORT
- CONTENT CREATION AND EDITING
- LEARNING AND EDUCATION
- TECHNICAL ASSISTANCE AND TROUBLESHOOTING
- CREATIVITY AND RECREATION
- RESEARCH, ANALYSIS, AND DECISION-MAKING



Forrás: https://hbr.org/data-visuals/2025/04/top-10-gen-al-use-cases

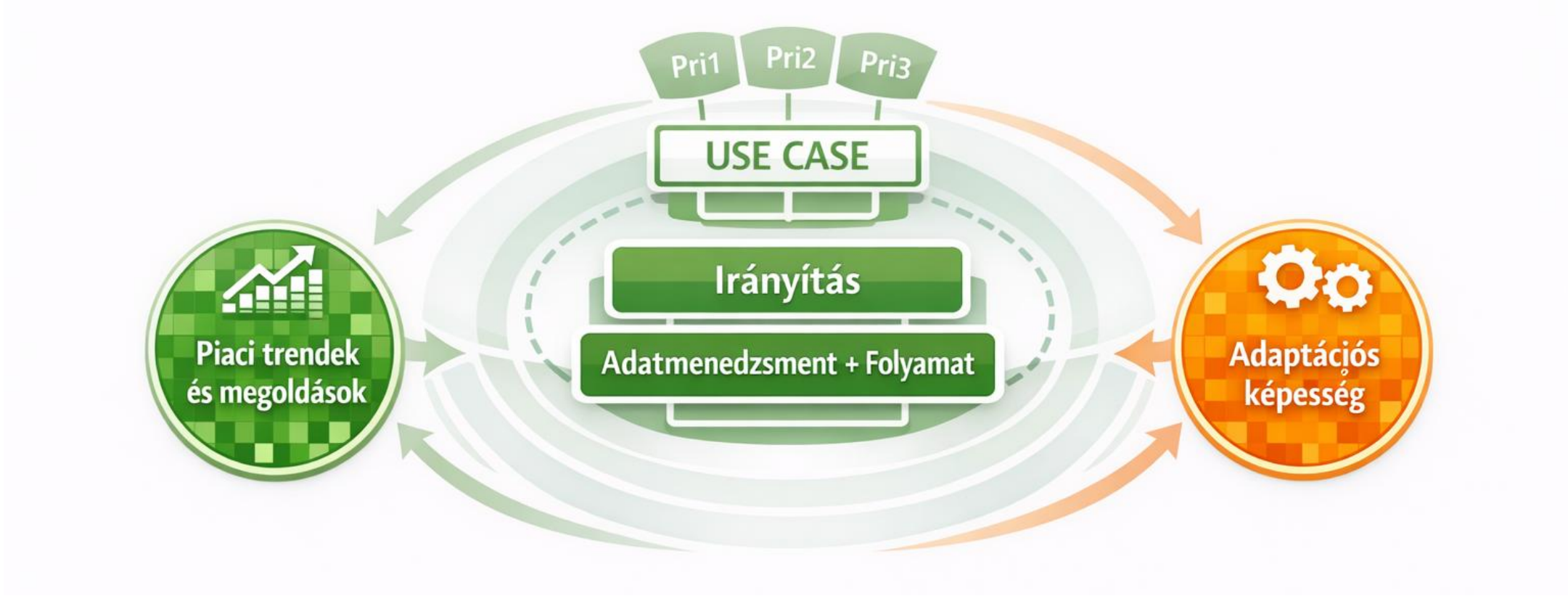
Tudjuk-e, hogy a szervezetünkben...

- ki,
- hol,
- mire és
- hogyan

használ AI-megoldást?

Tudjuk-e, hogyan teremt ez értéket a szervezet számára?

Folyamatos feladat – az irányítás folyamatos igazítása



Szervezeti keretek

Hozzáállás

Hogyan gondolkodik a szervezet erről a képességről?

Felelősség

Ki vállal felelősséget az AI által támogatott kimenetért?

Szerepek

Döntési és jóváhagyási
Szabályozói
Szakértői

Előfeltételek

Pl. adatok és folyamatok

Megbízható AI

EU etikus AI keretrendszer (EU Ethics Guideline for Trustworthy AI) szerint a megbízható MI-rendszernek három alapelvnek kell megfelelnie:

1. **Jogszerű**

2. **Etikus**

- Emberi autonómia tiszteletben tartása
- A kár megelőzése
- Méltányosság
- Megmagyarázhatóság - transzparencia

3. **Stabil**

7 etikai alapelv

Az emberi cselekvőképesség támogatása és emberi felügyelet	Az alapvető jogok, az emberi cselekvőképesség támogatása és az emberi felügyelet
Műszaki stabilitás és biztonság	A támadással szembeni ellenálló képesség és a védelem, a készenléti terv és általános biztonság, a pontosság, megbízhatóság és reprodukálhatóság
Adatvédelem és adatkezelés	A magánélet tiszteletben tartása, az adatok minősége és sértetlensége, valamint az adatokhoz való hozzáférés
Átláthatóság	A nyomonkövethetőség, a megmagyarázhatóság és a tájékoztatás
Sokféleség, megkülönböztethetőség és méltányosság	A méltánytalan torzítás elkerülése, a hozzáférhetőség és az egyetemes tervezés, valamint az érdekeltek részvétele
Környezeti és társadalmi jólét	A fenntarthatóság és a környezetbarát jelleg, a társadalmi hatás, a társadalom és a demokrácia
Elszámoltathatóság	Az ellenőrizhetőség, a hátrányos hatás minimalizálása és jelentése, a kompromisszumok és a jogorvoslat

Agenda

1. Külső szabályozások, kontextus
2. Egy bank miért és hogyan használ AI-t
3. **Példa esetek**
4. Mellékletek

Az adat- és technológiai időszakok megértése

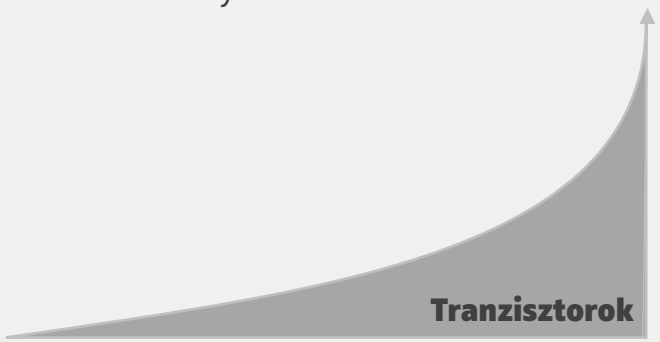
Az adatmenedzsment fejlődésének üteme elmarad az adatmennyiség növekedésének ütemétől

Moore Törvény ideje

Számítási kapacitás

A győztesek (mint az IBM, HP) a nagyobb teljesítményű szerverekkel és számítógépekkel növelték előnyüket, amelyek gyorsabban hajtották végre a tranzakciókat, és elindítottak minket az adatrobbanás felé.

1971
Moore törvénye



Metcalfe Törvény ideje

Hálózatok és kapcsolatok

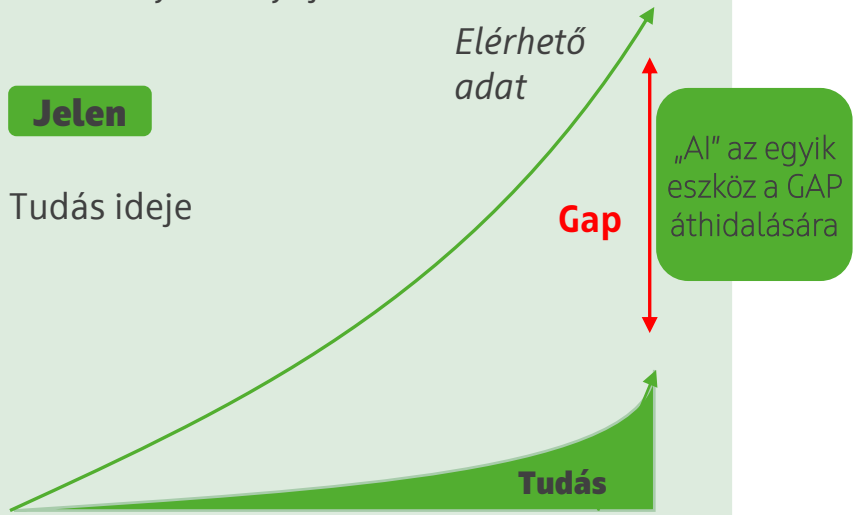
E korszak győztesei (mint a Google, az Amazon, a Netflix, a Facebook) azzal nyertek, hogy erős digitális súlypontokat hoztak létre felhasználóik és ügyfeleik számára. Kapcsolódtak ügyfeleik életének számos aspektusához.

1995
Metcalfe törvénye

Tudás, ismeret ideje

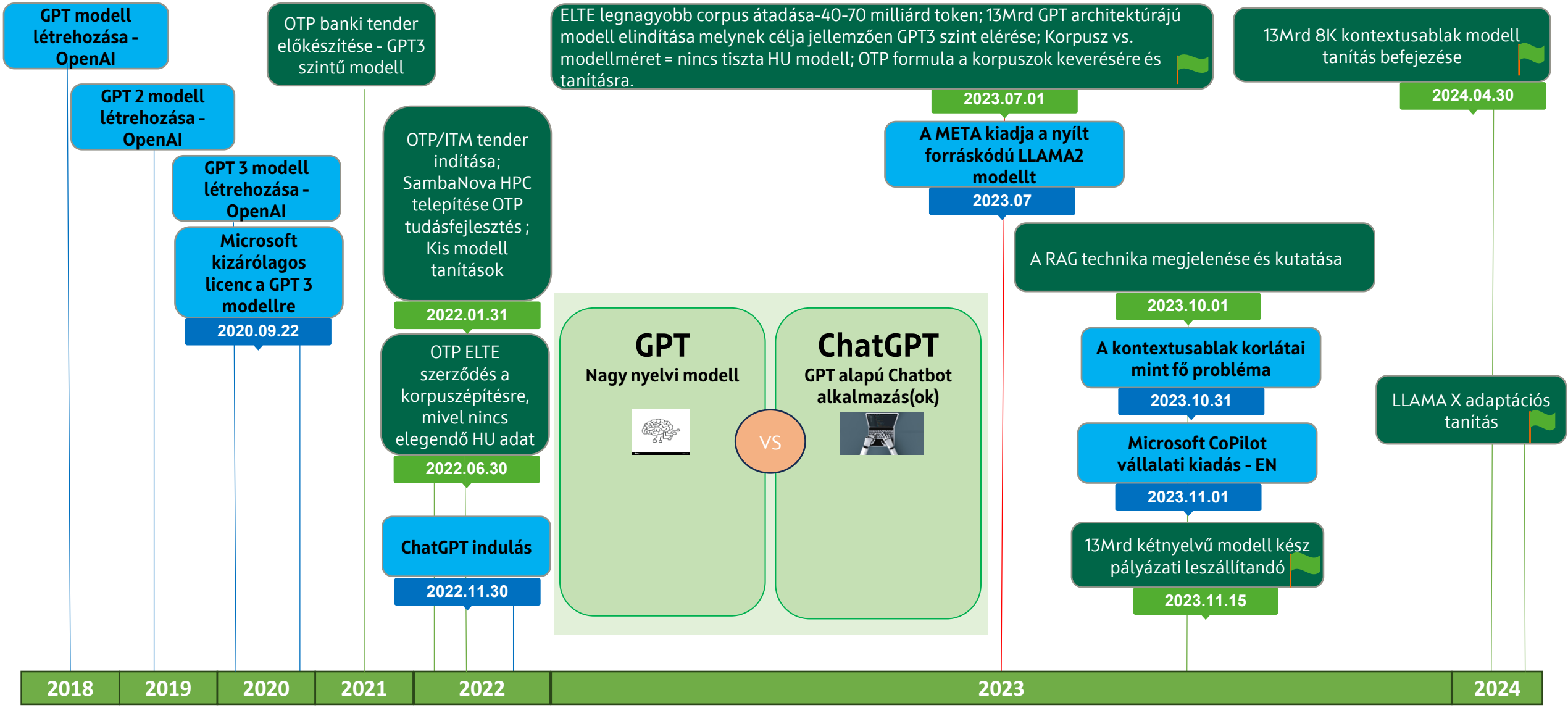
Az adatok és az MI hasznosítása

Azok a vállalatok lesznek a győztesek, amelyek kihasználják adataikat és információikat, hogy agilisak és előrelátóak legyenek, és kiváló termékeket és élményeket nyújtsanak.



Az LLM-MI projektet befolyásoló külső és belső tényezők

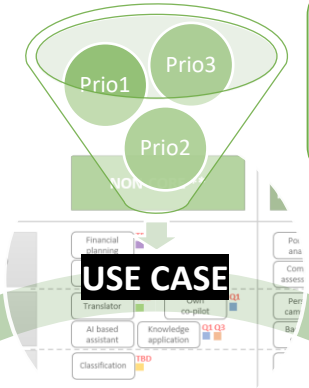
A K+F irányok megértéséhez elemeznünk kell az iparági eredményeket, mérföldköveket



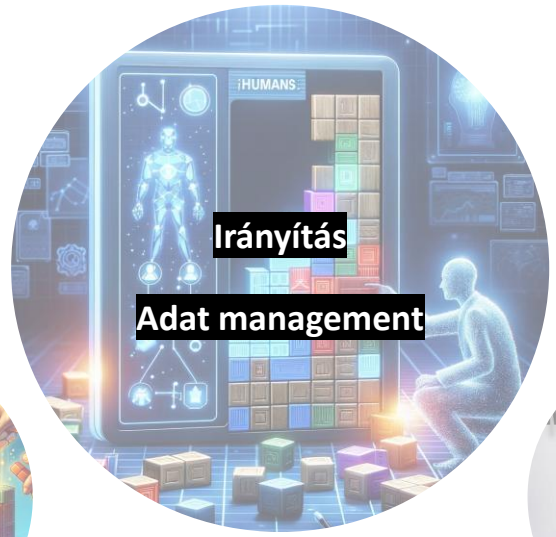
Folytonos a körforgás

Megfelelő irányítása kiépítése a szervezetekben nagyon fontos (adat management, MI kompetencia).

- AI mint szolgáltatás.
- A piacra jutás ideje.
- A folyamatosan fejlesztett képességek kihasználása



- Alkalmazkodás és a globális trendek megértése, egyedi megoldások kutatása.
- Mintha "Tetrist" játszanánk magas szinten: a kockák nagyon gyorsan jönnek, vagy tartjuk a tempót, vagy veszítünk. És ez egyre gyorsabb lesz.
- Továbblépni: képesek vagyunk saját építő blokkokat gyártani



BUY or BUILD?

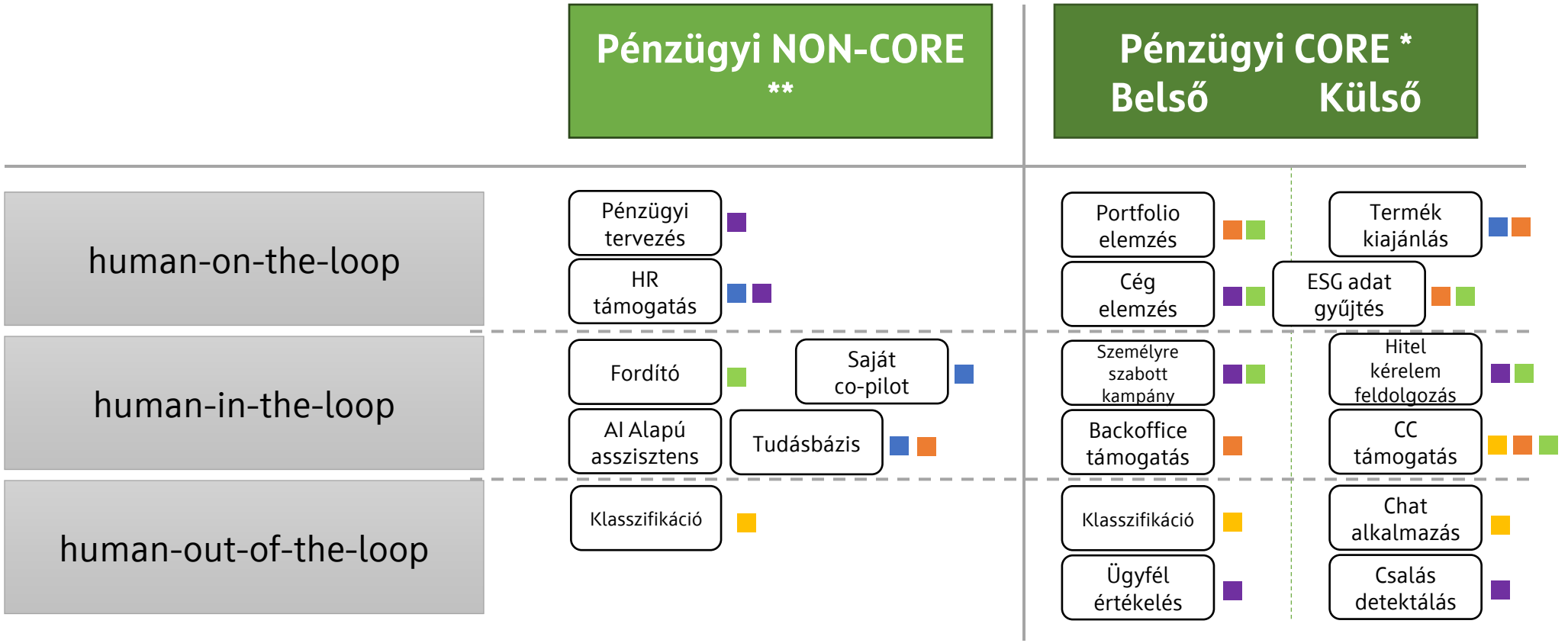
- Új megoldások: GPT, LLAMA, Phi, Copilot..
- Kontextusproblémák, GPU-kihasználás .
- RAG
- AI ≠ ChatGPT –mély megértés, tudás fejlesztés
- Felhő

MI szabályozások kialakulóban, fontos a felelős MI használat

A használati eseteket az emberi szerep, felelősség szerint is kategorizálhatjuk
Megoldandó feladatnak megfelelően válasszunk eszközt

otp Csoport

Kérdés: Mi is az „AI"? Mit akarunk megoldani?
Válasz: Sok féle működésű „AI"-nak definiálható megoldás létezik. Nem az AI a cél, csak egy eszköz.



* CORE - az ügyféllel kapcsolatos összes eset (belső - az OTP kezdeményezi a kapcsolatot; külső - az ügyfél kezdeményezi a kapcsolatot).
** NON – CORE – csak a belső használatot támogató funkciókat kell lefedni.

GPT *Hagyományos ML/DL*
HU-BERT *Egyéb LLM*
Llama 2

Miért érdemes finomhangolni, adaptálni LLM-eket?

Out of the Box modellek, szolgáltatások is jók, de egyedi igényekre nem mindig optimálisak

„Tőke, hitel" vajon hogyan helyezkedik el az LLM-ek mátrixában?

Megj.: nem releváns, hogy saját modell (OTP GPT3, vagy magyarra adaptált (LLAMA-GEMMA,stb.). Költség és üzemeltetési optimalizálási kérdés, (no meg security...)

Chat szándékfelismerés megoldás

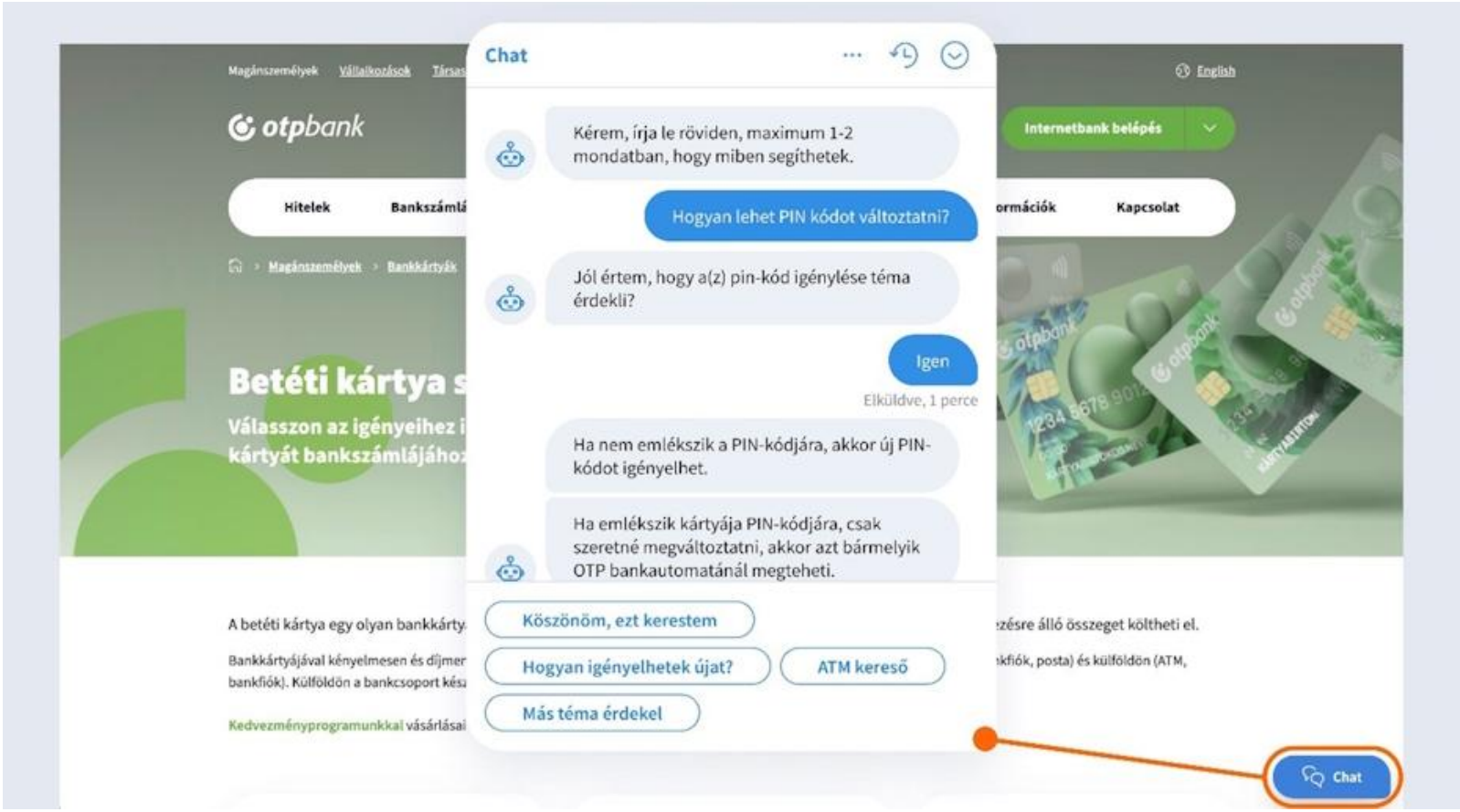
Nagyon kicsi, finomhangolt, optimalizált modell is elég, nem kell „ágyúval verébre”. Persze lesz evolúció.

Main topic (~15)

- Információbiztonság
- Digitális csatornák
- Biztosítás
- Számla
- Bankkártya
- Személyi kölcsön
- Folyószámlahitel
- Hitelkártya
- Áruhitel
- Ingatlanhitel
- OTP Diákhitel számla
- Hátralékos hitel / számla
- Videóbank szolgáltatás
- Megtakarítások
- Értékpapír
- Vállalkozói pénzügyek

Subtopic (~98)

- Külföldi kártyahasználat
- Bankkártya limit
- Kártya letiltása
- Lejárt/lejáró kártya
- Kártya igénylése, aktiválása
- Kártyás tranzakció információk
- Internetes vásárlás
- ATM bevont kártya
- Zárolás
- SMS szolgáltatás

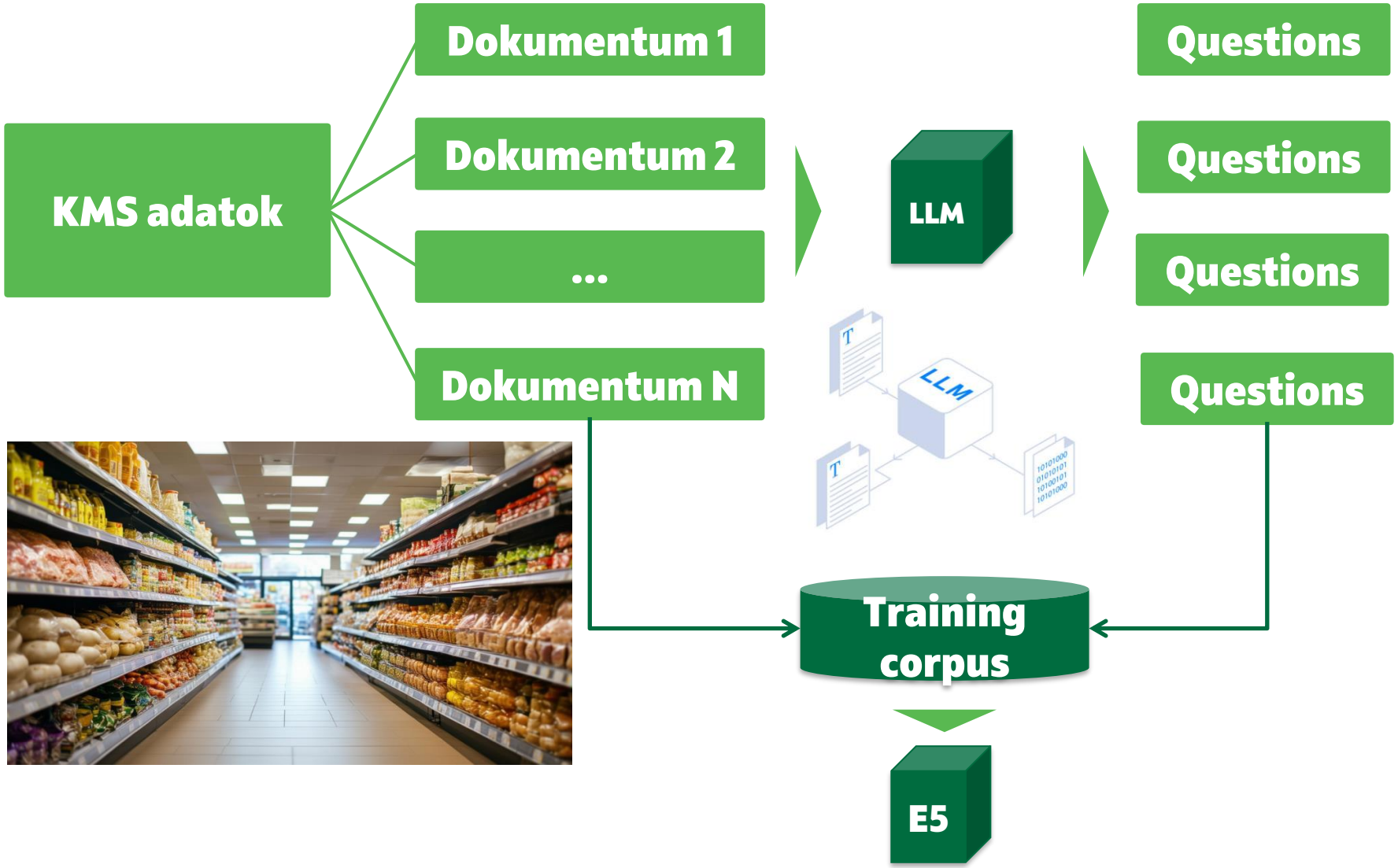


- **„mellébeszélés” 10%-kal csökkent**
- **Az ügyfél elégedettsége 15%-kal nőtt**
- **A tanító adatok gyűjtése kulcsfontosságú siker tényező**
- **Ugyanaz a probléma ugyanazt a modellt igényli (CC, KMS stb.)**
- **Minőségi(IT, Üzleti) követelmények kell támasztani a GenAI megoldásokhoz**

KMS- tudás management rendszer(ek)

Nagyon kicsi, finomhangolt, optimalizált modell is elég, nem kell „ágyúval verébre". Persze lesz evolúció.

otp Csoport



Iteratív keresés

92.5

Meta adatok felhasználása

81.9

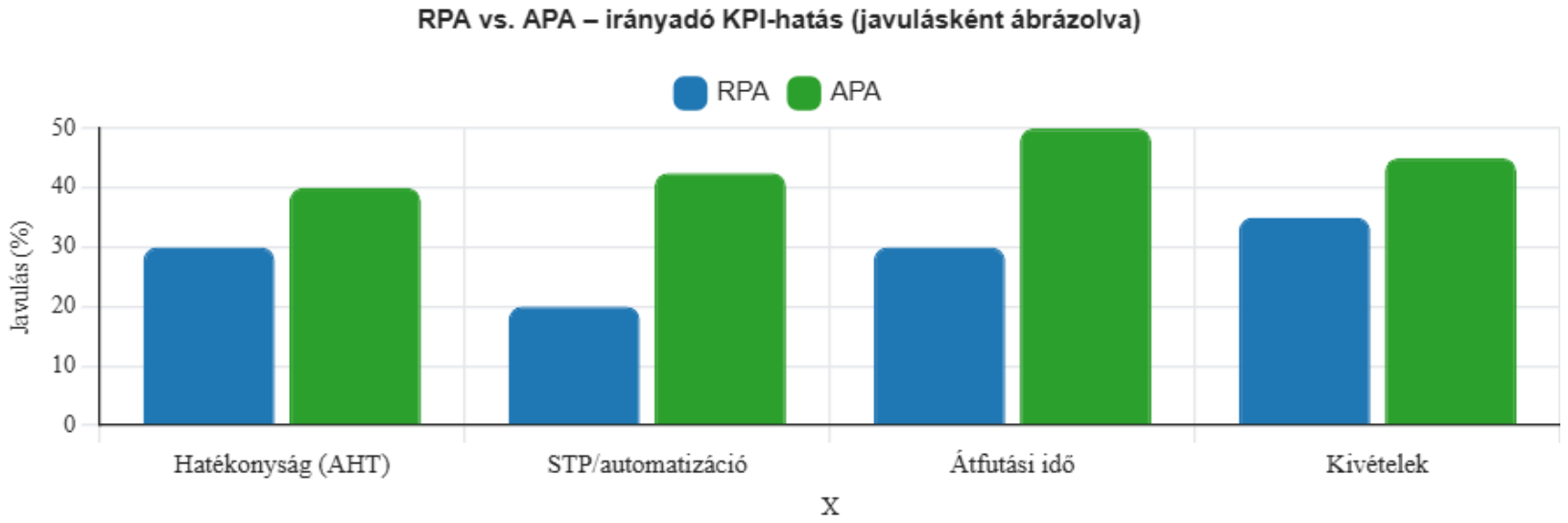
Modell finomhangolás

71.2

RPA vs APA

RPA = stabil költségcsökkentés; APA = komplexitás-kezelés + ügyfélélmény + bevétel.
„Stabil" → RPA; Változékony/ügyfélközeli → APA; Vegyes → hibrid

- RPA (Robotic Process Automation)Szabályalapú, determinisztikus „botok", amelyek UI-n/API-n ismétlődő, strukturált feladatokat hajtanak végre. Erős ott, ahol a folyamat stabil, standardizált, és az adatok strukturáltak.
- APA (Autonomous Process Automation)AI-val (ML/LLM/agentek) kiterjesztett automatizáció, amely képes nem szabványos bemenetek (pl. szöveg, dokumentumok) értelmezésére, változékony üzleti helyzetekhez alkalmazkodik, döntéseket hoz, és human-in-the-loop mellett vagy anélkül végrehajt. Cél: önműködőbb, tanuló végrehajtás, skálázható növekedési hatással.



KPI-k (irányadó tartományok):

a. Hatékonyság: AHT –20–40% (RPA), –30–50% (APA a teljes láncon).
b. STP/automatizáció: +10–30% (RPA), +25–60% (APA).Átfutási idő: –20–40% (RPA), –30–70% (APA).
c. Minőség/kivételek: hibaarány –20–50% (RPA), kivételarány –30–60% (APA).
d. Bevétel/élmény: NPS/CSAT ↑; upsell/cross-sell +5–15% (APA, agentikus ügyfélkiszolgálás).
e. Governance & megfelelés (banki):DORA-kompatibilis üzem: változás-/incidenskezelés, szolgáltatói függések, audit trail.AI/Data guardrail: PII-védelem, lineage, hozzáférés; model risk (eval metrikák, drift, bias/fairness).
f. Human oversight: HITL a material döntéseknél; go/no-go kapuk előre definiált küszöbökkel.

AI megoldások bevezetése (belső környezet) – kiberbiztonsági fókusz a kezdeten

Kezdő (2–6 hét) ellenőrzőpontok on-prem / privát cloud / belső hálózati integráció esetén

🗂️ Adatvédelem & adatosztályozás

- Milyen adat mehet be (PII, banktitok, IP) és milyen maszk/anon?
- Prompt/kimenet belső tárolása: retention, törlés, hozzáférési kontroll
- DLP szabályok: érzékeny adat kiszűrés promptban és válaszban

🔐 IAM, RBAC & privileged access

- SSO/MFA, csoport-alapú RBAC, least privilege
- Admin felületek: PIM/PAM, break-glass, audit trail
- Secrets: vault + rotáció + környezetenkénti elkülönítés

🧩 Modell, kód & supply chain (belső)

- Modellek/weights eredete, licenc, aláírás/ellenőrzés (SBOM/MBOM)
- Konténer image-ek: scan, provenance, policy enforcement
- Frissítések: jóváhagyás + változáskezelés (model versioning)

🧠 LLM-specifikus védelem (prompt/RAG)

- Prompt injection/jailbreak: guardrails, policy, input validálás
- RAG: permission-aware retrieval, forrás-hitelesség, dokumentum címkézés
- Kimenet: adat-kiszivárgás, hallucination risk, bizalmi jelölések

Belső AI megoldás

(LLM / ML / GenAI • belső hálózat • privát erőforrások)

Kezdő kiberbiztonsági kérdések

Cél: biztonságos pilot → kontrollált skálázás

🌐 Hálózat & futtatási környezet

- Szegmentáció (AI subnet), egress csak proxy-n át, allowlist
- Dev/Test/Prod elkülönítés, hardening, patching, endpoint védelem
- GPU/cluster hozzáférés: quota, izoláció, titkosítás nyugalomban

📈 Naplózás, SIEM & incidenskezelés

- Mit logolunk: prompt/válasz/tool-hívás (PII kezelése!)
- Detektálás: exfiltration, abuse, rendellenes tool-használat
- IR playbook: kulcsrotáció, modell rollback, feature flag / kill switch

🛠️ SDLC, tesztelés & red teaming

- Threat modeling a use case-re + adatfolyamokra
- Adversarial tesztek: prompt injection, data poisoning, RAG leak
- CI/CD: secret scanning, SAST/DAST, IaC policy, artifact signing

📜 Governance & belső kontrollok

- Use case kockázati besorolás, ownership (risk owner, approval)
- Szabályozók: adatkezelés, naplózás, hozzáférés, változáskezelés
- Kivételkezelés + kontrollmérések (KRI/KPI) a pilot alatt

Gyors start (belső): 1) adat + use case + integrációk feltérképezése 2) IAM + hálózat/egress 3) guardrails + RAG jogosultság 4) SIEM/IR minimum 5) pilot-korlátok + változáskezelés

Agenda

1. Külső szabályozások, kontextus
2. Életciklus feladatok, felelősségek
3. Következő lépések
4. **Mellékletek**

EU AI ACT

Főbb elvek.

Miről szól?

1. Európai értékek transzparens növelése, hangsúlyozva a mesterséges intelligencia etikus alkalmazását.
2. Folyamatok és szerepkörök meghatározásakor, valamint az egész életciklus során az MI rendszer minőségének érvényesítése.
3. Az EU-tagállamok közötti együttműködés és egyenlő versenyfeltételek elősegítése, valamint az uniós polgárok alapvető jogainak védelme a mesterséges intelligencia korában.

Mi a célja?

- Annak biztosítása, hogy az EU-ban forgalomba hozott és használt MI-rendszerek biztonságosak legyenek, és tiszteletben tartsák az alapvető jogokra és az EU-s értékekre vonatkozó hatályos jogszabályokat. A nem megfelelés akár 35 millió EUR közigazgatási bírságot is jelenthet!
- A jogbiztonság megteremtése a mesterséges intelligenciába történő beruházások és a mesterséges intelligenciát érintő innováció elősegítése érdekében.
- Az irányításnak és az MI-rendszerek tekintetében az alapvető jogokra és biztonsági követelményekre vonatkozó hatályos jogszabályok hatékony érvényesítésének a javítása.
- A jogszerű, biztonságos és megbízható MI-alkalmazások tekintetében az egységes piac kialakításának elősegítése és a piac széttöredezettségének megelőzése.

AI ACT kockázati besorolás

Elfogadhatatlan kockázatú, tiltott gyakorlatok

Tudatos észlelés, érzékelés nélküli, manipulatív rendszerek, jelentős társadalomformáló hatással bíró, vagy sebezhetőséget kihasználó megoldások, biometrikus jellemző alapján kategorizáló, illetve bizonyos azonosító rendszerek, amelyek sértik az egyének vagy bizonyos csoportok jogait, biztonságát

BETILTÁS, KIVEZETÉS

Nagy kockázatú rendszerek, erősen szabályozott feltételekkel

Alapjogokat érintő pl. foglalkoztatás, szolgáltatásokhoz történő hozzáférés, igazságszolgáltatás, határigazgatás, bűnüldözés

BIZTONSÁG, KOCKÁZATKEZELÉS, NYOMON KÖVETHETŐSÉG, ADATOK INTEGRITÁSA, EMBERI RÉSZVÉTEL

Korlátozott kockázatú rendszerek, átláthatóság biztosítása mellett

A transzparencia hiánya miatt hordoz kockázatot, ezért a tájékoztatáson nagy a hangsúly
pl. AI-jal folytatott chat, szintetikus médiatartalom, érzelemfelismerés

TÁJÉKOZTATÁS

Alacsony, minimális kockázatú rendszerek, magatartási kódex használatával

A legtöbb megoldás ilyen, amelyek bizonyos folyamatokat támogatnak.

SZAKMAI MEGFELELŐSÉG BIZTOSÍTÁSA

Potenciális szankció rendszer

Szankciórendszer

1

Jogsértés **(tiltott gyakorlatok)** miatt kiszabható pénzbírság nagyon magas, maximum

35 M€

VAGY

Vállalatok esetében az előző pénzügyi évben elért éves forgalom **7%-a**

2

Az AI Act egyéb követelményeinek megsértése (lista)

15 M€

VAGY

Vállalatok esetében az előző pénzügyi évben elért éves forgalom **3%-a**

3

A bejelentett szerveknek vagy nemzeti hatóságoknak **helytelen, hiányos vagy félrevezető információk** szolgáltatása

7,5 M€

VAGY

Vállalatok esetében az előző pénzügyi évben elért éves forgalom **1%-a**